Journal of Telecommunications and the Digital Economy

Volume 11, Number 4
December 2023

Published by
Telecommunications Association Inc.

ISSN 2203-1693

The *Journal of Telecommunications and the Digital Economy* is published by TelSoc four times a year, in March, June, September and December.

Journal of Telecommunications and the Digital Economy

Volume 11, Number 4
December 2023

Table of Contents

Discussion

Biography

Editorial Team

The *Journal* is published by the Telecommunications Association (TelSoc), a not-for-profit society registered as an incorporated association. It is the Australian telecommunication industry's oldest learned society. The *Journal* has been published (with various titles) since 1935.

Editorial

Regulation and Convergence

Leith H. Campbell
Managing Editor

Abstract: This editorial argues from content in this issue that telecommunications regulation has not kept pace with convergence of telecommunications and content providers. It suggests that the loose co-ordination between regulations and regulators for telecommunications services and digital platforms no longer makes technological sense within the converged architectures of 5G and 6G.

In addition, all the published papers, not just those relating to regulation, are briefly described. This issue also includes an obituary for John Burke, an influential member of this *Journal*'s Editorial Advisory Board.

Keywords: Editorial, Regulation, Convergence

Regulatory Proliferation

In this issue, we return again to the perennial topic of "telecommunications" regulation. (The quotation marks are deliberate, as you will see later.) We publish the Charles Todd Oration 2023, given by Rob Nicholls (2023), who looks, in part, at existing regulatory instruments and whether or not they are fit for current purposes. We also include a speech given to TelSoc earlier in the year by Cynthia Gebert (2023), the Telecommunications Industry Ombudsman (TIO); she argues for more direct regulation of telecommunications in relation to consumer issues. And we have a paper by Mark Gregory (2023), who considers that telecommunications should be included in the Australian critical infrastructure regime.

It is worthwhile first to survey the regulators that are currently concerned with telecommunications and its uses. In Australia, competition in telecommunications is regulated by the general competition regulator, the Australian Competition and Consumer Commission (ACCC), with special powers for regulating the telecommunications sector. As the TIO points out (Gebert, 2023, p. 139), technical regulation of telecommunications was put in

http://doi.org/10.18080/jtde.v11n4.914

the hands of the Australian Communications Authority, which eventually became part of the current Australian Communications and Media Authority (ACMA). As a "converged" regulator, with responsibility for broadcasting as well as telecommunications, the ACMA also regulates content (see, for example, ACMA, 2022). The ACMA may also be given additional powers "to combat misinformation and disinformation on digital platforms" (Australian Government, 2023). In addition to the TIO, which handles unresolved consumer complaints about telecommunications services, there is an eSafety Commission, which "helps remove serious online abuse, and illegal and restricted online content" ("What you can report", n.d.); and the Office of the Australian Information Commissioner, whose purpose is "to promote and uphold privacy and information access rights" (OAIC, n.d.). And there is regulation, still evolving, of "digital platforms" (Wilding, 2021).

It is likely that telecommunications will be brought under the critical infrastructure regime: the earlier exclusion of telecommunications from the regime has been called a "sweetheart deal" by the relevant Minister (Mizen *et al.*, 2023).

This proliferation of regulators — and regulations — comes about for several reasons. It may be a need for specific expertise and focus (e.g., competition policy). It may also come about from the ongoing identification of new requirements (e.g., online safety). It does suggest, however, that there is no overarching theory or practice on how or where regulation should reside or by whom it should be enforced. Dedicated expertise may well be required for detailed regulation, leading to a proliferation of regulators. At the very least, however, good co-ordination between regulatory regimes is important and will become more so as greater convergence between telecommunications and online service providers continues.

Convergence and Regulation

One heading that is notable — for a technologist, at least — in the TIO's speech is "The Lessons Telco Can Offer to Digital Platforms" (Gebert, 2023, p. 146). There is nothing wrong with this heading. It indicates the way the government thinks about the underlying issue: there are telecommunications operators ("Telco") and there are digital platforms; and each needs to be regulated in its own way.

From a technological point of view, however, the two topics are intimately interconnected. Digital platforms are only useful if they can be communicated with, by telecommunications; and a good deal of telecommunications traffic is directed to or from digital platforms. Telcos operate their own digital platforms and hope to profit from them. If content from some digital platform is to be restricted, the restrictions may well be implemented by a telco or an Internet Service Provider (ISP).

http://doi.org/10.18080/jtde.v11n4.914

With 5G, the interdependence between telcos and digital platforms becomes even stronger. In the 5G architecture (see, for example, Campbell (2021), Figure 2, p. 4, reporting on a speech to TelSoc by Bruce Davie), the 5G core network includes a variety of "clouds"; and all "clouds" are digital platforms, some or all of which are "digital platforms" in the sense used by government. 5G networks do not work without digital platforms. It will probably be a topic of future "technical" regulation as to how much the telco-deployed 5G core networks should be opened to third-party digital platforms.

There is a growing convergence between telecommunications and the services provided by digital platforms. To those who would argue for a continuing special case for telecommunications services, it should be pointed out that much voice and messaging traffic is now dependent on digital platforms (e.g. WhatsApp, Skype) – and the distinction will become every blurrier as 5G and 6G architectures become bedded down.

There is a need, then, to seriously consider further convergence of regulation. Just as a "converged" regulator once meant combining telecommunications and broadcasting, now a converged regulator should consider the whole picture of content, communication, carriage or complaint — even critical infrastructure — without historical boundaries getting in the way. It is absurd, for example, that content declared restricted or taken down on one digital platform should then become accessible on another platform. The solution, if there is an acceptable one, lies with both content and carriage working together.

While Rob Nicholls (2023) has argued that the regulatory instruments for future considerations are most likely already in place, the regulatory architecture needs more work to make it efficient and fit for purpose in the converged communications world.

Elsewhere in This Issue

In this issue, the two papers specifically concerned with regulation are Nicholls (2023), published in the Special Interest section, and Gebert (2023) in the Public Policy section. Readers should note that these papers, like all others, have been subject to peer review before publication.

There are three papers in the Digital Economy section. *Effect of Exchange Rates and Information and Communication Technology on Indonesia's Economic Growth* seeks to identify the effects of ICT on economic growth within a varying exchange-rate environment. *Strategies and Challenges of Unified Payment Interface* is concerned with the digital payments system in India. *AI Chatbot Innovation – Leading toward Consumer Satisfaction, Electronic Word of Mouth and Continuous Intention in Online Shopping* looks at interactions between consumers and chatbots.

http://doi.org/10.18080/jtde.v11n4.914

In the Telecommunications section, we publish six papers. *Building Trust in Telesurgery through Blockchain-Based Patient Consent and Surgeon Authentication* looks at how blockchain technology can be used to support consent in telesurgery. *SBM-SA: A Safety Beacon Message Separation Algorithm for Privacy Protection in Internet of Vehicles* is concerned with protecting privacy as motor vehicles communicate with one another. *Secure Data Sharing in a Cyber-Physical Cloud Environment* describes a secure data-sharing protocol. *CNN-based Occluded Person Re-identification in a Multi Camera Environment* considers the case of identifying a specific person in a video sequence. We also publish an *Interview with Teresa Corbin*, now Telstra's Chief Customer Advocate. Finally in the Telecommunications section, we have the paper by Mark Gregory (2023) on *An Analysis of the Optus National Outage and Recommendations for Enhanced Regulation*.

We also have one Discussion paper on *Digital Transformation, Social Innovation and the Not-For-Profit Sector in Australia*. This invites correspondence on the issues raised.

In the Biography, we publish an obituary for John Burke, *Vale John Burke (1942–2023)*, who contributed much to this *Journal*, to TelSoc (our publisher), and to Australian telecommunications.

References

ACMA [Australian Communications and Media Authority]. (2022). What audiences want – Audience expectations for content Safeguards: A position paper for professional content providers. ACMA, June 2022. Available at https://www.acma.gov.au/sites/default/files/2022-06/What%20audiences%20want%20-%20Audience%20expectations%20for%20content%20safeguards.pdf

Australian Government. (2023). Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—Fact sheet. Department of Infrastructure, Transport, Regional Development, Communications and the Arts, June 2023. Available at https://www.infrastructure.gov.au/sites/default/files/documents/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill-2023-factsheet-june2023.pdf

Campbell, L. H. (2021). The Broadband Futures Forum: The Rise of 5G and the NBN. *Journal of Telecommunications and the Digital Economy*, *9*(3), 1–11. https://doi.org/10.18080/jtde.v9n3.432

Gebert, C. (2023). Rebalancing Regulation in an Era of Distrust: Telecommunications Industry Ombudsman and Developing Consumer Regulation. *Journal of Telecommunications and the Digital Economy*, *11*(4), 137–149. https://doi.org/10.18080/jtde.v11n4.900

Gregory, M. A. (2023). An Analysis of the Optus National Outage and Recommendations for Enhanced Regulation. *Journal of Telecommunications and the Digital Economy*, 11(4), 185–198. https://doi.org/10.18080/jtde.v11n4.898

Mizen, R., Wiggins, J., & Ludlow, M. (2023, November 13). Telco boards hit with strict cybersecurity rules. *Australian Financial Review*, 13 November 2023. Available at https://www.afr.com/politics/federal/telco-boards-hit-with-strict-cybersecurity-rules-20231112-p5ejao

Nicholls, R. (2023). Regulating the New: Overland Telegraph to Generative AI: Charles Todd Oration 2023. *Journal of Telecommunications and the Digital Economy*, *11*(4), 1–12. https://doi.org/10.18080/jtde.v11n4.856

OAIC [Office of the Australian Information Commissioner]. (n.d.). What we do. Australian Government: Office of the Australian Information Commissioner. Available at https://www.oaic.gov.au/about-the-OAIC/what-we-do

"What you can report to eSafety". (n.d.). [Online] eSafety Commissioner. Available at https://www.esafety.gov.au/report/what-you-can-report-to-esafety

Wilding, D. (2021). Regulating News and Disinformation on Digital Platforms: Self-Regulation or Prevarication? *Journal of Telecommunications and the Digital Economy*, *9*(2), 11–46. https://doi.org/10.18080/jtde.v9n2.415

Regulating the New:

Overland Telegraph to Generative AI

Charles Todd Oration 2023

Rob Nicholls
UNSW Business School

Abstract: The Charles Todd Oration is an annual event run by TelSoc and is named for Charles Todd, the Postmaster-General of South Australia, who was responsible for completing the Overland Telegraph Line from Darwin to Adelaide in 1872. The 2023 Oration was delivered in Sydney on 12 October 2023 by the author, Rob Nicholls, and was introduced by Communications Minister Michelle Rowland MP. The Oration examined the challenge of novelty to regulators. It looked at history of regulating innovation, promotion of innovation in the context of consumer protection, how regulators can deal with innovation, and minimising consumer harm.

Keywords: competition, co-design, generative artificial intelligence, regulation, telecommunications

Introduction

This is a (close to) verbatim transcription of the Charles Todd Oration 2023.

I would like to start by acknowledging the traditional custodians of the land on which we meet, the Gadigal people of the Eora nation, and to pay my respects to elders past, present, and emerging. I would particularly like to pay my respects to all First Nations Peoples with us today.

Thanks, Minister, for your kind and generous introduction. Actually, I think that I am allowed to say "thanks, Michelle", given the amount of time that we worked together on telecommunications regulation at Gilbert + Tobin. I will be discussing some of the lessons learned there today.

My title for today is "Regulating the New: Overland Telegraph to Generative AI". Rather surprisingly, I will actually touch on generative artificial intelligence, rather than just using it

http://doi.org/10.18080/jtde.v11n4.856

to persuade you to come along today. I am going to look at this issue in four parts. The first is some history of the challenge of novelty for regulators (including when regulation was part of ownership). The second is the key issue of jointly promoting innovation and protecting consumers. I know, "stifling innovation" is the catch cry of regulatory submissions the world over. I should know, I have used it often enough on behalf of clients! However, I am going to try to come at the issue as dispassionately as I can. As an academic, I am supposed to be able to do that. The third issue is what principles can be used generally by regulators to deal with the new. The final part is to consider how regulation and regulators can ensure that these technologies are used in a way that harms consumers least. I will let you know now, just in case you worry about the time that I am taking, I will spend most of my time on issues one, two, and three.

Some History of the Challenge of Novelty for Regulators

For many years, the Commonwealth Postmaster General was the owner and regulator of communications services (Moyal, 1983). This flows from the Commonwealth's constitutional power. Section 51(v) of the *Constitution of Australia Act 1901* (Cth) gives the Australian Parliament power to legislate on "postal, telegraphic, telephonic, and other like services". Spectrum management also falls under that power. Last year, Minister Rowland gave her oration on the 150th anniversary of the Overland Telegraph for which we honour Todd today (Rowland, 2023). Importantly here, this was a quarter of a century before Federation.

The challenge was one of regulating, owning, and dominating the telegraphy space. Todd's vision may have been to link Australia and England, but he was the Postmaster General of the British Colony of South Australia (Livingston, 1997). To be fair, it was a self-governing and convict-free colony. However, Todd's task was to create an overland telegraph system in competition with the other Australian colonies (Courtenay, 2023). In particular, it was Queensland that wanted to direct traffic through Brisbane in competition with Todd's overland telegraph. Indeed, when Todd was running late and the submarine cable from Java had already landed at Darwin, the Queensland Superintendent of Telegraphs called for Todd's project to be scrapped, and for the line from Darwin to connect to the terminal at the remote Queensland town of Burketown (Puntis, 2008). Indeed, Burketown had been the original proposed termination. I should point out that the *Adelaide Evening Journal* on Saturday 24 August 1872 ("History of the Adelaide to London Telegraph," 1872), expressed undisguised glee in its history of the overland line in the role of South Australia compared with Queensland.

What I argue is that the Overland Telegraph was a state funded project leading, eventually, to becoming an asset of the Commonwealth.

http://doi.org/10.18080/jtde.v11n4.856

I think that it is also interesting to look at the replacement of the Overland Telegraph. Part of that interest is that it involves exclusive patents and a former Australian icon. The technology available in Australia for radio in the early 1920s used patents held by Amalgamated Wireless Australasia or AWA. For disclosure, I worked for AWA Communications about 30 years ago. These intellectual property rights were obtained as a result of the merger of the patent rights of the Marconi and Telefunken subsidiaries in Australia in 1913. In order to avoid Australia being, as Billy Hughes put it to the Imperial Conference in 1921, "at the end of the line", the Hughes administration entered into an agreement for the supply of communications services with AWA. As part of that arrangement, AWA was partially nationalised, with 50% plus one share under government control. However, the partial nationalisation was also controversial, in that the seven-member board of directors of the new AWA could be appointed on a 4:3 basis by the privately held part of AWA. Ultimately, this position was solved when, as Prime Minister, Billy Hughes took a seat on the board (Curnow, 1963, p. 88). That is a slightly different way in which a shareholder minister can express their statement of expectations.

The "single hop" link between Australia and the UK was delayed, partly due to British intransigence on the form of Imperial communications which, under the Norman scheme, was to use a series of relay stations to link the Empire. The Norman scheme was based on a report by Sir Henry Norman ("Relays in the Wireless Line," 1921, p. 5):

> *The Committee of the Imperial Conference today discussed a wireless proposal submitted by Sir Henry Norman. This provides for an Empire-wide scheme, enabling the Dominions and Britain to communicate with each other, but not directly. This plan provides for a two-thousand-mile radius, meaning that relays are necessary. Mr Hughes bitterly opposed this, demanding a direct exchange, if a scheme is to be attempted at all.*

This dispute was ultimately resolved in a variation to the agreement to build the wireless beam system in 1927.

There was a royalty flow described by Solicitor General Garran (Garran *et al.*, 1929, p. 80):

> *The company also agrees to make its patent rights available to the Commonwealth free of charge for the purpose of the manufacture or use of plant or apparatus to be manufactured and used exclusively by the Commonwealth. In return for these concessions the Commonwealth agrees to pay to the company 3d. per month in respect of every person licensed to listen in under the Wireless Telegraphy Act.*

Of course, the AWA wireless beam service was part of what became part of the Overseas Telecommunications Commission, later OTC, along with Cable and Wireless assets, in 1946. That is, regulating the new by nationalisation (Given, 2007).

Turning to more recent times, the deregulatory approach to telecommunications ran from 1992. It started with the "managed duopoly" of Telstra and Optus for fixed-line services and three GSM operators (Vodafone was the addition) in mobile. From 1997, the ACCC was tasked with delivering workable competition in an environment with many "natural monopolies" or

http://doi.org/10.18080/jtde.v11n4.856

bottlenecks. In 1997, telecommunications sector-specific competition law was introduced as Part XIB and Part XIC of what is now the *Competition and Consumer Act 2010* (Cth). The Telecommunications Act was designed to provide a "light touch" regulatory environment and provides for a high degree of self-regulation for the sector (Nicholls, 2017). It has a policy objective in section 4 to promote "the greatest practicable use of industry self-regulation". However, it had the "stick" that the regulator (the ACMA) can make binding codes or rules, if the self-regulatory regime does not deliver outcomes which are aligned with policy. This is known as co-regulation and I will discuss it further shortly.

The response to the "new" of deregulated telecommunications included two key concepts. The first is the "long-term interest of end-users" (LTIE). This is set out in section 152AB(2) of the *Competition and Consumer Act 2010* (Cth). The objectives of the LTIE are:

(a) the promotion of competition;

(b) achieving any-to-any connectivity; and

(c) encouraging economically efficient use of, and economically efficient investment in, infrastructure.

The ACCC has used a standard approach of regarding competition as the process of rivalry between firms, where each market participant is constrained in its price and output decisions by the activity of other market participants.

The second is the concept of access (Nicholls, 2014). There is a right of access to "declared" services and access must be provided on non-discriminatory terms and conditions. The ACCC is empowered to declare bottleneck services if declaration is in the LTIE.

However, this liberal co-regulatory market-based approach did not achieve the expected outcomes in the fixed sector. Instead, the national broadband network, described eloquently by Michelle in last year's oration was the outcome (Rowland, 2023). Three out of three for State ownership as a response to the new. I would have to note that national ownership can only be applied domestically.

So, we have had a look at the historical challenge of novelty for regulators. The next issue is promoting innovation and protecting consumers.

Promoting Innovation and Protecting Consumers

In any form of regulation there is a balance between promoting innovation and protecting consumers. Actually, it is often a balance between not stifling innovation and protecting consumers. I guess this is the stage at which to mention stifling of innovation (Lev Aretz & Strandburg, 2020). It is a phrase which appears mainly in regulatory submissions. It is also true that some of these were drafted by me for clients or reviewed by me at the ACCC. The

http://doi.org/10.18080/jtde.v11n4.856

problem in dismissing the risk of stifling innovation is a matter of information asymmetry. Is the regulator actually certain that the business is using a rhetorical tool or is it the final cry before exit? In either case, it is likely that this balance must be to minimise risk of harms to consumers — that is, regulatory intervention will have a consumer protection focus. Of course, I should mention that any decent submission will also hint darkly at "unintended consequences". Usually without specifying those consequences.

I will come to market-based and command and control regulation shortly. In either case, the regulatory implementation is likely to fall into one of a number of approaches. This is where there is a risk flowing from asking an academic to give an oration. A bit of "Regulation 101" is likely to be on the agenda (Baldwin *et al.*, 2011; Baldwin & Cave, 2020; Freiberg, 2017). One of my former colleagues asked me before the Oration whether Chat GPT had finished my speech yet. Here I will confess that I am using material that has already been presented to students! Some of the regulatory approaches are (Coglianese, 2017):

- **Outcome-Based Regulations**: Outcomes clearly defined in regulations (the "what") and the regulated parties determine the "how" (Haines & Gurney, 2003). Requires measurable and enforceable objectives.
- **Systems-Based Regulations**: Regulated parties have methods for assessing/managing prescribed risks, through process-oriented specifications for rules and system controls designed to meet goals (Behn *et al.*, 2022)
- **Standards and Guidelines**: Use of standards can complement legal instruments. But requires trustworthy standards bodies.
- **Regulatory co-design**: Opportunity to understand and focus on user needs. Requires stakeholders to be willing, trusted, and competent (Abbas *et al.*, 2021; Avram *et al.*, 2019; Banerjee *et al.*, 2021; Trischler *et al.*, 2018)

I like the idea of regulatory co-design, when it is done well. Essentially it helps to ensure that the regulatory approach keeps its focus on consumers, while being effective for the regulator and the regulated. It does take time. However, the time taken will assist in reducing the potential for whipsaw regulatory responses. Broadly, the degree of regulatory co-design is measured on a spectrum. The International Association for Public Participation or IAP2 has produced a model which maps out this spectrum (IAP2 Spectrum, 2023). For the consumer, the engagement sits on a scale, which ranges through:

Inform → consult → involve → collaborate → empower.

The role of the community in each of these ranges through:

Listen → contribute → participate → partner → decide.

Associated with both of these ranges is a set of goals as to why the participation is required and a set of promises as to how consumers will be involved. Regulatory co-design is effectively

http://doi.org/10.18080/jtde.v11n4.856

mandated in the energy sector in Australia (AER, 2023). It is just not part of the approach in the telecommunications sector. In my view, that is a missed opportunity.

As I mentioned, we currently have a telecommunications regulatory environment based on co-regulation. As a former regulator, co-regulation is neither fish nor fowl. From a regulatory enforcement perspective, self-regulation looks like the rules set for a club. As long as they are not detrimental to consumers and do not discourage entry, they can be safely ignored. Regulation flows from legislation and subordinate legislation and can be enforced. Co-regulation is often code for self-regulation, which is fine if it does not adversely affect consumers. When it is enforced regulation, there is often push-back from the regulated, arguing that the self-regulatory aspects are sufficient. This is part of the rationale behind the Telecommunications Industry Ombudsman, Cynthia Gebert, calling for direct regulation (Gebert, 2023) and Nerida O'Loughlin of the ACMA asking whether co-regulation has had its day (O'Loughlin, 2023).

In the context of dealing with the new, direct regulation is most likely. It seems to me that we need to have regulatory co-design as part of a regulatory regime that uses systematic regulation, which is outcomes-based. We do not have the option of national ownership. To provide improved consumer protection, I am not actually calling for a regulatory nirvana. Merely the application of well-understood tools.

Having looked at some of the issues in that joint task of promoting innovation and protecting consumers, I now turn to general regulatory principles in addressing the new.

General Regulatory Principles in Addressing the New

I want to briefly divert to discuss the issue of regulatory certainty. Mainly, because there is no such thing. The best that any regulator can offer is regulatory predictability, and this is probably the best that any regulated entity can expect. I say this in the context of "rule of law". Rule of law means that people in the same circumstances are treated by the law in the same way. That is, the operation of the law is predictable. It is not certain. Certainty is an ask that is never delivered. On the other hand, regulatory predictability leads to good outcomes for both the regulated and the regulator.

There is a tradition of considering regulatory systems in terms of either market-based or "command and control" (Cave, 2013). There are a few reasons why market-based approaches have been preferred in the last three decades. The most important of these is the issue of information asymmetry. Put simply, the regulated entity is likely to know far more than the regulator. Indeed, this is particularly the case in the telecommunications sector, where the

http://doi.org/10.18080/jtde.v11n4.856

ACCC uses recordkeeping rules, and other information provision requirements, to assist to understand how the sector functions.

So why would you choose either market-based or command-and-control regulatory approaches? And in the context of regulating the new, which is the right approach (Dunne, 2015)?

What are the reasons for market-based regulation? First, it's efficient. This is partly because businesses are allowed to choose the most cost-effective way to comply with the regulations. It has a high level of flexibility. Businesses can adjust their behaviour in response to changes in the market. After all, that is what business as usual is for businesses. I will also argue that market-based regulation can promote innovation. This is because businesses have a financial incentive to develop new technologies, if only to allow them to comply with regulations in a more cost-effective way.

On the other hand, there are some negatives to a market-based approach. The first is regulatory complexity. Market-based regulation can be complex to design and implement. Balancing fairness and effectiveness can create unintended consequences. Sorry, I couldn't help myself here! There are also equity issues. Market-based regulation can be inequitable because businesses that are able to afford to comply with the regulations will benefit at the expense of businesses that are not able to afford to comply. This compliance cost could well include external advisory costs. The last issue is effectiveness. Market-based regulation may not be effective in addressing all types of regulatory problem. This is particularly true of addressing externalities.

Well, why would you choose a command-and-control regulatory approach? There are three main arguments. The first is that it is effective. It has worked in the past. The second is simplicity. Command-and-control regulation is relatively easy to understand and enforce, because regulations are specific. The third is predictability. Businesses know what they need to do to comply with regulations, and consumers know that they are protected.

On the other hand, there are some downsides of command and control. Command-and-control regulation can have high compliance costs and these costs are passed on to consumers. Command-and-control regulation is inflexible. It restricts approaches to compliance. The third is most critical to this Oration. It adversely affects innovation. For once, I did not claim that it stifles innovation! However, businesses are less likely to invest in new technologies if they are required to comply with specific standards.

In the end, the decision is a balance between all of these factors. What is most important is that the regulatory approach is consistent and predictable. This means not changing the rules part way through.

http://doi.org/10.18080/jtde.v11n4.856

As I have mentioned, the telecommunications sector has primarily been characterised by market-based regulation with occasional nationalisation. This can be contrasted with broadcasting regulation, which has more command-and-control regulation on the basis that it is dealing with a social good.

As a generalisation, sectors characterised by dynamic efficiencies (rather than productive or allocative efficiencies) are best suited to market-based regulation (Decker, 2015). The rationale is that they tend to be more innovative.

In dealing with the new, I think that regulatory settings probably need to consider parallels with existing situations. However, there is a significant risk in getting it wrong by defining the problem too early. For example, I might have decided, acting reasonably, that in 2007 I would consider regulating MySpace. In that year it was registering 320,000 users a day, and had overtaken Yahoo! to become the most visited website in the United States. It was owned by News Corporation and looked like it was acquiring near monopoly market share. MySpace had eclipsed Friendster (yes, I really am that old!) and was not restricted to college students. Using a bit of network economics and knowledge of multi-sided markets, I might argue that the tipping point had occurred, and that News Corp's vertical and horizontal integration meant that MySpace was going to have monopoly characteristics. I should be thinking about providing access to MySpace in some regulatory way. Except, of course, that Facebook overtook MySpace in 2008 partly because of News Corp.

The logical approach to regulation of the new as the new is emerging is by using existing laws and regulations. We might fret about the market power of each of the big tech players. I am old-fashioned and still use the term GAFAM for Google, Apple, Facebook, Amazon, and Microsoft. Of course, Facebook is Meta and Google is Alphabet and Open AI should probably be in the mix (unlike X, formerly known as Twitter). But we have mechanisms for dealing with market power without new regulation. Australian competition law does not ban or break up monopolies. Nor does it prohibit monopoly rents. It does address misuse of market power and that, after all, is the likely problem. The misuse-of-market-power provisions were changed five years ago, partly to address changing business practices (Kemp, 2017). However, these have not been used by the ACCC in the GAFAM context.

Enough of general regulatory principles in addressing the new. My next and final area is how do we do it all in a way that protects consumers. I am also going to finally get to generative AI (Artificial Intelligence).

http://doi.org/10.18080/jtde.v11n4.856

Protecting Consumers

Ultimately, regulation is only required in order to protect some group which would be adversely affected in the absence of regulation. Usually, these are consumers. However, they may be small businesses and occasionally whole sectors, as in the News Media Bargaining Code (Nicholls, 2020, 2021).

A rush to regulation is required when there are no current tools that can be applied to a problem. The heart of the argument that I am making in this Oration is that the absence of regulatory tools is incredibly rare. I will take generative AI as an example. There are a few potential consumer harms, which flow from the use of generative AI using a chatbot interface, such as Chat GPT or Google Bard.

In relation to text, one key issue is transparency. This is less "why did the gen AI say this?" and more "what was the basis of the statement". In my view, this can be partly addressed by relying on the "Model Card" for the generative AI. Each of OpenAI (OpenAI, 2023), Google (Google, 2023), and Meta, for Llama 2 (Meta, 2023), publish a model card setting out some minimal information such as the model's:

(a) name and version;
(b) type;
(c) inputs and outputs;
(d) training data;
(e) evaluation metrics; and
(f) limitations and biases.

Why? Because the publication of the model card is at a minimum "conduct in trade or commerce" and might rise to be a "representation". It also sets a reasonable consumer expectation of the service. All can be dealt with under the Australian Consumer Law, which is Schedule 2 to the *Competition and Consumer Act 2010* (Cth) or the *Australian Securities and Investments Commission Act 2001* (Cth), if required. You will notice that I am comfortable with disclaimers as to the risk of hallucination. That is, there is no point trying to regulate that which cannot be changed.

On the other hand, the use of generative AI to produce images which are then used in bullying is not a matter where there should not be an immediate response. However, as has already been noted by the eSafety Commissioner, Julie Inman-Grant (Office of the eSafety Commissioner, 2023), the issue is not so much with the creation of the bullying material than with its publication on social media. Part of Meta's approach to free use of image-creating AI

http://doi.org/10.18080/jtde.v11n4.856

on its platforms is the reduction in potential harm. Taking down harmful material is easier when there is a mechanism for the creation of novel but harmless material.

I will note in passing that Google search appeared to have monopoly characteristics until Microsoft Bing Chat included access to GPT 4 at no additional cost, when the Open AI version costs $US20 per month. One source, Statistica (2023), suggests that Bing's share of search has risen from 6.8% in May to 9.2% in July as a result of this change. I should also note that other statistical sources are not as optimistic for Microsoft, despite its $US10 billion investment in Open AI.

Conclusions

I hope that I have done as I have promised. I have given a potted history of the challenge of novelty for regulators. I have discussed promoting innovation and protecting consumers. I have looked at how regulators can deal with the new. I ended by considering how regulation and regulators can ensure that novel technologies harm consumers least.

Acknowledgements

I would like to thank Jim Holmes and a former Gilbert + Tobin colleague, Elise Ball, from TelSoc for inviting me to give this year's Oration. Independent and academically rigorous contribution to regulatory debate is an essential feature of a well-functioning sector. I would also like to thank the Managing Editor of the *Journal of Telecommunications and the Digital Economy*, Leith Campbell. This journal, published by TelSoc, is a key source of peer reviewed literature on the technical, social, and regulatory challenges facing us in the telecommunications sector and the digital economy. Articles in this journal have influenced my regulatory thinking over time.

References

Abbas, R., Hamdoun, S., Abu-Ghazaleh, J., Chhetri, Ne., Chhetri, Na., & Michael, K. (2021). Co-Designing the Future With Public Interest Technology. *IEEE Technology and Society Magazine*, *40*(3), 10–15. https://doi.org/10.1109/MTS.2021.3101825

AER [Australian Energy Regulator]. (2023). Stakeholder Engagement. https://www.aer.gov.au/about-us/stakeholder-engagement

Avram, G., Ciolfi, L., Spedale, S., Roberts, D., & Petrelli, D. (2019). Co-design goes large. *Interactions*, *26*(5), 58–63. https://doi.org/10.1145/3348793

Baldwin, R., & Cave, M. (2020). *Taming the Corporation: How to Regulate for Success*. Oxford University Press (OUP).

Baldwin, R., Cave, M., & Lodge, M. (2011). *Understanding Regulation 2E: Theory, Strategy, and Practice*. Oxford University Press.

Banerjee, A., Lamrani, I., Michael, K., Bowman, D., & Gupta, S. K. S. (2021). *Socio-technical co-Design for accountable autonomous software*. AI Safety @ IJCAI [International Joint Conferences on Artificial Intelligence], Proceedings. Available at https://ceur-ws.org/Vol-2916/paper_22.pdf

Behn, M., Haselman, R., & Vig, V. (2022). The Limits of Model-Based Regulation. *The Journal of Finance*, *77*(3), 1635–1684. https://doi.org/10.1111/jofi.13124

Cave, M. (2013). Extending competition in network industries: Can input markets circumvent the need for an administered access regime? *Utilities Policy*, *27*, 82–92. https://doi.org/10.1016/j.jup.2013.09.006

Coglianese, C. (2017). The limits of performance-based regulation. *University of Michigan Journal of Law Reform*, *50*, 525–563.

Courtenay, A. (2023). *Mr Todd's Marvel: How One Man Telegraphed Australia to the Modern World*. Woodslane Press.

Curnow, R. (1963). The origins of Australian broadcasting. In Bedford, I., & Curnow, R., *Initiative and organization*. Melbourne: F. W. Cheshire.

Decker, C. (2015). *Modern Economic Regulation*. Cambridge University Press.

Dunne, N. (2015). *Competition Law and Economic Regulation: Making and Managing Markets*. Cambridge University Press.

Freiberg, A. (2017). *Regulation in Australia*. Federation Press.

Garran, R., Beasley, F. R., Groom, L. E., Gamble, J. F., Bean, E. L., Solomon, H. J., McIntyre, M. W. D., Zichy-Woinarski, J., Stow, F. L., & Gore, J. (1929). Review of Legislation, 1927. *Journal of Comparative Legislation and International Law*, *11*(2), 75–126.

Gebert, C. (2023, September 21). Rebalancing regulation in an era of distrust. https://www.tio.com.au/news/rebalancing-regulation-era-distrust

Given, J. (2007). Talking over Water: History, Wireless and the Telephone. *Media International Australia*, *125*(1), 46–56. https://doi.org/10.1177/1329878X0812500107

Google. (2023). PaLM 2 Technical Report. https://ai.google/static/documents/palm2techreport.pdf

Haines, F., & Gurney, D. (2003). The Shadows of the Law: Contemporary Approaches to Regulation and the Problem of Regulatory Conflict. *Law & Policy*, *25*(4), 353–380. Business Source Premier. https://doi.org/10.1111/j.0265-8240.2003.00154.x

History of the Adelaide to London Telegraph. (1872, August 24). *Adelaide Evening Journal*. https://trove.nla.gov.au/newspaper/article/196742551

IAP2 [International Association for Public Participation]. (2023). IAP2 Public Participation Spectrum. https://iap2.org.au/resources/spectrum/

Kemp, K. (2017). The Big Chill: A Comparative Analysis of Effects-Based Tests for Misuse of Market Power. *University of New South Wales Law Journal*, *40*, 493–536.

Lev Aretz, Y., & Strandburg, K. J. (2020). Regulation and Innovation: Approaching Market Failure from Both Sides. *Yale Journal on Regulation Bulletin*, *38*(1), 1–27.

Livingston, K. T. (1997). Charles Todd: Powerful communication technocrat in colonial and federating Australia. *Australian Journal of Communication*, *24*(3), 1–10.

Meta. (2023). Llama 2: Open Foundation and Fine-Tuned Chat Models. https://arxiv.org/abs/2307.09288

Moyal, A. (1983). Telecommunications in Australia: An Historical Perspective, 1854-1930. *Prometheus*, *1*(1), 23–41.

Nicholls, R. (2014). Structural Separation, Interconnection and Access. *Australian Journal of Competition and Consumer Law*, *2014*(22), 54–56.

Nicholls, R. (2017). The Australian Telecommunications Regulatory Environment: An overview. *Journal of Telecommunications and the Digital Economy*, *4*(4), 196–213. https://doi.org/10.18080/jtde.v4n4.76

Nicholls, R. (2020). When Code is Law: Bargains Between News Publishers and Platforms—Competition Policy International. *Competition Policy International*. https://www.competitionpolicyinternational.com/when-code-is-law-bargains-between-news-publishers-and-platforms/

Nicholls, R. (2021). Valuing News: The Australian News Media Bargaining Code. *InterMEDIA*, *49*(2), 20–25.

Office of the eSafety Commissioner. (2023, August 15). New industry recommendations to curb harms of generative AI. https://www.esafety.gov.au/newsroom/media-releases/new-industry-recommendations-to-curb-harms-of-generative-ai

O'Loughlin, N. (2023, August 15). Speech by Nerida O'Loughlin PSM, ACMA Chair, International Institute of Communications: Telecommunications and Media Forum 2023. https://www.acma.gov.au/publications/2023-08/speech/speech-nerida-oloughlin-psm-acma-chair-international-institute-communications-telecommunications-and-media-forum-2023

OpenAI. (2023). GPT-4 System Card. https://cdn.openai.com/papers/gpt-4-system-card.pdf

Puntis, P. (2008). *New technology, the "control crisis", and the government intervention: Lessons from telegraphy in the 1870s*. Communications Policy and Research Forum, Sydney, Australia.

Relays in the Wireless Line. (1921, July 19). *New Zealand Evening Post*, 5.

Rowland, M. (2023). 2022 Charles Todd Oration. *Journal of Telecommunications and the Digital Economy*, *11*(1), 18–28. https://doi.org/10.18080/jtde.v11n1.720

Statistica. (2023, September 20). Market share of leading desktop search engines worldwide from January 2015 to July 2023. https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/

Trischler, J., Kristensson, P., & Scott, D. (2018). Team diversity and its management in a co-design team. *Journal of Service Management*, *29*(1), 120–145. https://doi.org/10.1108/JOSM-10-2016-0283

Effect of Exchange Rates and Information and Communication Technology on Indonesia's Economic Growth

A Nonlinear Autoregressive Distributed Lag Approach

Wali Aya Rumbia
Department of Economics, Universitas Halu Oleo, Kendari, Indonesia

Asrul Jabani
Sekolah Tinggi Ilmu Ekonomi Enam-Enam, Kendari, Indonesia

Pasrun Adam
Sekolah Tinggi Ilmu Ekonomi Enam-Enam, Kendari, Indonesia

Bakhtiar Abbas
Sekolah Tinggi Ilmu Ekonomi Enam-Enam, Kendari, Indonesia

M. Nur
Sekolah Tinggi Ilmu Ekonomi Enam-Enam, Kendari, Indonesia

Yuwanda Purnamasari Pasrun
Department of Information System, Universitas Sembilanbelas November, Kolaka, Indonesia

Abstract: Foreign exchange rates as well as information and communication technology (ICT) are crucial in the global economy. Exchange rates affect trade balance, which influences gross domestic product (GDP) and economic growth. ICT also affects economic growth by reducing business transaction costs and increasing the income of investors and companies, stimulating national income and economic growth. This research examines the effect of exchange rate asymmetry and ICT on Indonesian economic growth, using annual time-series data on exchange rates, ICT usage (proxied by Internet, telephone, and mobile phone users), and economic growth (GDP from 1994 to 2018). The data were analyzed using a non-linear auto-regressive distributed lag model. The results show that the exchange rate exerts an asymmetric effect on long-term economic growth. ICT has short- and long-term positive effects on economic growth. According to the findings, the Indonesian government should stabilize the IDR/USD exchange rate through monetary policies to encourage economic growth. Monetary policy needs

http://doi.org/10.18080/jtde.v11n4.743

also to support IDR/USD exchange rate appreciation to enhance the trade balance, GDP, and economic growth. The economic growth of Indonesia, which is driven by ICT development, still needs to be sustained by the government initiating ICT development in cities and rural areas.

Keywords: Economic growth, exchange rate, exchange rate asymmetry, ICT, NARDL model.

Introduction

Foreign currency and information and communication technology (ICT) are vital in the world economy. By definition, foreign currency is an instrument of transactions in the real and financial trade sectors, meaning that the currency exchange rate is essential in trading transactions and activities (Sathiwitayakul & Prasongsukarn, 2011). In comparison, ICT is used for sending, storing, creating, sharing, or exchanging information by almost all companies to improve and promote product quality and sell goods and services. Also, consumers use ICT to find and purchase quality products and conduct transactions online (Farhadi *et al.*, 2012).

Economic growth could be significantly affected by ICT and exchange rates. The influence of exchange rates is reflected through the trade channel. According to the traditional theory, depreciation in a foreign currency exchange rate (appreciation in a domestic currency exchange rate) reduces the trade balance. Contrastingly, an increase in the trade balance increases economic growth (Kandil, 2004; Wang, 2009; Saidi *et al.*, 2020; Bao & Le, 2021). Furthermore, ICT affects economic growth through its application, facilitating investment by individuals and companies. It could reduce transaction and production costs, increasing the income earned by investors and companies (Ketteni *et al.*, 2014). Subsequently, such an increase ultimately boosts national income and economic growth (Nguyen *et al.*, 2020; Millia *et al.*, 2020; Rosnawintang *et al.*, 2021). In addition, ICT skills tend to positively affect entrepreneurial intentions (Sreejith & Sreejith, 2023). According to Virasa *et al.* (2022), the process of promoting entrepreneurial intentions leads to business activities, which contributes to job creation and economic development, such as growth (Virasa *et al.*, 2022).

Indonesia is a developing country that adheres to a floating exchange rate system. It adopts a monetary policy to develop the economy by stabilizing the domestic currency (IDR) exchange rate against foreign currencies, such as the US Dollar. This exchange rate stability is also intended to increase economic growth. However, the 1998 Asian financial crisis decreased the IDR/USD exchange rate to 10013.62 IDR per 1 USD from 2160.75 IDR per 1 USD in 1994. Similarly, economic growth declined to -13.6% from 7.3% in 1994 (Indonesia-Investments, 2021).

http://doi.org/10.18080/jtde.v11n4.743

The development of modern technology and information in Indonesia began with the launch of the Palapa satellite on July 8, 1976, from Cape Kennedy, USA. This satellite technology was then used to exchange data and information using the Internet and telephone, starting in 1988 (Prabowo & Gischa, 2021). The government issued rules to ensure the sustainable development and use of ICT by companies and the community (Zakaria, 2021). Subsequently, companies-built e-commerce using ICT to launch their business and increase their revenue with lower operating costs (Setiawan, 2017). However, ICT infrastructure has not been developed evenly, especially in rural areas, making most communities unable to access the Internet and telephone. Therefore, this study aimed to evaluate the two government policies regarding exchange rate stabilization and ICT development.

Extensive research has examined the impact of rates on economic growth in various countries. Examples include Elbadawi *et al.* (2012) in Sub-Saharan Africa, Wong (2013) in Malaysia, Saidi *et al.* (2015) in Indonesia, Lee & Yue (2017) in the US, Ribeiro *et al.* (2020) in 54 nations worldwide. The results showed that exchange rates affect economic growth. This is a symmetric effect in the economic literature (Shin *et al.*, 2014; Meo *et al.*, 2018; Saidi *et al.*, 2021; Abbasi & Iqbal, 2021). Research has also shown that exchange rates asymmetrically impacted economic growth. For instance, Bahmani-Oskooee & Mohammadian (2016) and Farouq & Sambo (2022) found that the exchange rates asymmetrically influenced economic growth. However, no research has shown the asymmetrical effect of the exchange rates on economic growth in Indonesia. Previous studies only examined the linear or symmetric effect of the exchange rate on economic growth. Saidi *et al.* (2015) and Yuliadi (2020) analyzed the effect of the exchange rate and other macroeconomic variables on Indonesia's economic growth using annual data from 2010 to 2016. A panel data model analysis showed that the exchange rate affects economic growth. In addition, Yussof & Febrina (2014) discussed the effect of the exchange rate on economic growth. The Vector Auto-Regression (VAR) analysis of the annual data for 1970–2009 showed that the exchange rate affects economic growth.

García-Muñiz & Vicente (2014) and Salahuddin & Alam (2016) showed that ICT affects economic growth. However, no previous research explored the asymmetric impact of exchange rates and ICT on Indonesia's economic growth. Therefore, this research investigates whether the exchange rates have an asymmetric effect on economic growth. Moreover, it examines the influence of ICT on Indonesia's economic growth using a Non-Linear Autoregressive Distributed Lag (NARDL) model. Therefore, these results could contribute to the literature on the influence of exchange rate asymmetry and ICT on economic growth using the NARDL model.

The second part of this paper reviews several empirical and theoretical studies consistent with this research, while the third describes the data and analysis methodology. The fourth part

http://doi.org/10.18080/jtde.v11n4.743

presents findings and discusses their analysis, while conclusions and recommendations are made in the fifth part.

Literature Review

Theory review

Theories explaining the relationship between exchange rates and economic growth through trading channels were stated in the introduction. This subsection presents the theory about the asymmetric relationship between the exchange rate and output. It was developed by Kandil & Mirzaie (2002) using the theory of rational expectations, as stated by Kandil (2008). In this theory, the exchange rate is divided into anticipated and unanticipated exchange rate components. Changes in the unanticipated component determine the asymmetrical effect of exchange rate on output, divided into two types. These are the effects of positive and negative exchange rate shocks, representing the depreciation and appreciation impacts of the domestic exchange rate, respectively. The positive shock effect decreases output or economic growth through the supply-side impact.

Theories about the relationship between ICT use and economic growth could be explained through Solow's and endogenous growth theories. According to Solow's growth theory, ICT use is an external factor that encourages economic growth (Solow, 1957). In contrast, the endogenous growth theory states ICT use is an internal factor as a production input that encourages economic growth (Mankiw, 2007). When ICT is considered a capital factor for improving production quality, it generates added value in increasing economic growth (Aghaei & Rezagholizadeh, 2017; Bahrini & Qaffas, 2019).

Empirical review

The literature shows that the exchange rates' impact on economic growth is both symmetrical and asymmetrical (Shin *et al.*, 2014; Meo *et al.*, 2018). Using annual time series data for the 1986–2010 period, Basirat et al. (2014) analyzed the effect of fluctuating currencies on economic growth in Iran, the Philippines, Colombia, and The Gambia. The panel data model results showed that economic growth was affected negatively by the exchange rate fluctuations. Furthermore, Habib *et al.* (2017) examined the influence of exchange rate movements on 150 nations' economic growth after the Bretton Woods period. The research used a dynamic panel model test against annual time series data during 1970–2010. The results showed that exchange-rate appreciation decreased economic growth. Ha & Hoang (2020) tested the effect of exchange rates on economic growth in Asian countries using annual panel data from 1994 to 2016. The Generalized Method of Moments (GMM) test showed that exchange rates and economic growth moved in the same direction. Moreover, Selimi & Selimi

http://doi.org/10.18080/jtde.v11n4.743

(2017) empirically assessed the exchange-rate impact on Macedonia's economic growth through a VAR review of quarterly data. The findings showed that economic growth was positively impacted by the exchange rates between the first quarters of 1998 and 2015.

Studies have also examined the asymmetrical impact of exchange rates on economic growth. For instance, Kandil (2008) analyzed the exchange rate's asymmetric influence on the economic growth of developing nations. The results showed that a depreciating currency exchange rate reduced output and economic growth. Similarly, Hussain et al. (2019) found that the domestic currency depreciation in Pakistan reduced GDP and economic growth. Wesseh & Lin (2018) reviewed the impact of exchange rates on Liberia's economic growth. The VAR analysis of yearly time series data during the 1980–2015 period showed that the exchange rates affected economic growth. Specifically, the depreciation of the Liberian currency against the US dollar reduced economic growth. Therefore, the exchange rates of the Liberian currency asymmetrically affected economic growth.

The effects of ICT on economic growth in several countries have been documented using panel data models. For instance, Amaghionyeodiwe & Annansingh-Jamieson (2017) analyzed the effect of ICT, particularly users of the Internet, mobile phones, and fixed subscriptions, on economic growth in the Caribbean nations. The research used a panel data model to analyze the yearly time series data from 1996 to 2013. The findings showed that ICT positively affected economic growth. Furthermore, Asongu & Odhiambo (2019) used panel data from 1980 to 2014 to examine the impact of ICT on economic growth in 25 of Africa's Sub-Saharan countries. The GMM method indicated that ICT positively impacted economic development. Similarly, Solomon & Klyton (2019) applied the GMM estimator to analyze the effect of digital technology use by individuals, businesses, and governments on economic growth in 39 African countries. The 2012–2016 panel data findings indicated that Internet use positively influenced economic growth. Habibi & Zahardast (2020) analyzed time-series data of 24 OECD and ten Middle-East nations from 2000 to 2017 to determine the contribution of ICT to economic growth. Data analysis using fixed-effect Ordinary Least Squares (OLS) and GMM methods indicated ICT positively affects economic growth. Therefore, the research recommended that the governments in OECD countries develop investment in ICT infrastructure to promote economic growth.

Arabi & Allah (2017) used an Auto-Regressive Distributed Lag (ARDL) model to investigate the impact of ICTs per 100 inhabitants, including fixed telephone lines, mobile phones, and Internet users, on Sudan's economic growth. The time-series data analysis between 1980 and 2024 indicated that ICT affected long- and short-term economic growth. In addition, García (2019) used 1990–2014 time-series data to analyze the effect of the Internet, mobile phone, computer, fibre optic, and Internet prices on Mexico's economic growth. Using a simultaneous

http://doi.org/10.18080/jtde.v11n4.743

equation model, the data analysis results showed that the Internet, cell phones, computers, and fibre optics positively impact economic growth. In contrast, Internet prices negatively influenced economic growth, meaning that the Mexican government should develop investment in ICT.

Data and Methodology

Data

This research employed annual time series data for Internet, telephone, and mobile users, as well as exchange rates and per capita GDP during the 1994–2018 period. IDR/USD exchange rates are a proxy for the exchange rates, while GDP per capita (measured in USD) is a proxy for economic growth (see Ramoni-Perazzi & Romero, 2022). The time-series data were obtained from the World Bank website. In the data analysis, the notations used are NET for Internet users, TEL for telephone users, MOB for mobile phone users, EXC for exchange rates, and GRO for economic growth. In this case, the EXC, NET, MOB, TEL, and GRO variables are in natural logarithmic forms.

Methodology

This research tested the long-term effect of positive shock (PEX) and negative shock (NEX) in exchange rates and ICT, comprising Internet, telephone, and mobile phone users, on economic growth in Indonesia. The test used the following co-integration regression model and the specifications of the long-term model used by Bahmani-Oskooee & Saha (2016) and Hussain *et al.* (2019).

$$GRO_t = C + \alpha PEX_t + \beta NEX_t + \gamma NET_t + \tau MOB_t + \delta TEL_t + \varepsilon_t \quad (1)$$

In equation (1), C, α, β, γ, τ and δ are the regression equation's parameters, assumed to be stable between 1994 and 2018. The parameters α, β, γ, τ and δ are also called long-run coefficients, while ε_t is an error or residual, identically distributed, independent and homoscedastic. Various empirical studies (Arfaoui, 2018; Jalil *et al.*, 2013) sometimes assume the error terms, ε_t, have equal, independent and normal distributions. Furthermore, PEX and NEX are partial-sum variables of positive and negative changes in the exchange rates, respectively. PEX and NEX state the IDR/USD exchange rate depreciation and appreciation variables, respectively (Bahmani-Oskooee & Saha, 2016). In line with this, Kandil (2008) named the term "the partial sum of positive and negative changes" with "positive and negative shocks in the exchange rate", respectively.

http://doi.org/10.18080/jtde.v11n4.743

The next equation defines PEX as a positive shock or exchange rate depreciation variable. In comparison, NEX is interpreted as a negative shock or an exchange rate appreciation variable. They are described in the following.

$$PEX_t = \sum_{i=1}^{t} \max\left[\Delta EXC_i, 0\right] = \sum_{i=1}^{t} \max\left[D(EXC_i), 0\right]$$

$$NEX_t = \sum_{i=1}^{t} \min\left[\Delta EXC_i, 0\right] = \sum_{i=1}^{t} \min\left[D(EXC_i), 0\right]$$

where $D(EXC_i) = \Delta EC_i = EXC_i - EXC_{i-1} = EXC - EXC(-1),\ i = 1, 2, \ldots, t$, is the change in the exchange rate.

All time-series data were transformed into a natural logarithmic form, and expressed with the notations NET, MOB, TEL, PEX, NEX, and GRO variables. This natural logarithm transformation is useful for eliminating multicollinearity between regressor variables (Nachrowi & Usman, 2006; Brooks, 2019).

The process of checking the multicollinearity assumption, according to the econometric literature, can be carried out by two methods, including (1) checking the correlation matrix among independent variables. When all correlations between two independent variables are less than or equal to 0.8, then there is no multicollinearity in the multiple regression (Gujarati & Porter, 2010). The other method (2) is checking the variance inflation factor (VIF) for each independent variable. When the VIF value for each independent variable is less than or equal to 10, there is no multicollinearity in the multiple regression (Cortinhas & Black, 2012). In this research, multicollinearity checking was conducted using the VIF values.

Equation (1) is a long-run model derived from the NARDL model when PEX, NEX, NET, MOB, TEL, and GRO are in equilibrium for the variable positive shock in exchange rates $PEX_t = PEX_{t-1} = \cdots = PEX_{t-q_1}$. The NARDL model with lag lengths $p,\ q_1,\ q_2,\ q_3$ and q_4, abbreviated as NARDL(p, q_1, q_2, q_3, q_4), are as follows (Shin *et al.*, 2014; Pesaran & Shin, 1999):

$$GRO_t = C_0 + \sum_{i=1}^{p} \theta_i GRO_{(t-i)} + \sum_{j=0}^{q_1} \left(\alpha_j PEX_{(t-j)} + \beta_j NEX_{(t-k)}\right) +$$

$$\sum_{k=0}^{q_2} \gamma_k NET_{(t-k)} + \sum_{l=0}^{q_3} \tau_l MOB_{(t-l)} + \sum_{m=0}^{q_4} \delta_m TEL_{(t-m)} + \varepsilon_{1t} \qquad (2)$$

where $C_0,\ \theta_i\ (i = 1, 2, \ldots, p),\ \alpha_j\ (j = 0, 1, \ldots, q_1),\ \beta_j\ (j = 0, 1, \ldots, q_1),\ \gamma_k\ (k = 0, 1, \ldots, q_2),\ \tau_l\ (l = 0, 1, \ldots, q_3)$ and $\delta_m\ (m = 0, 1, \ldots, q_4)$ are the parameters of the NARDL model.

In equilibrium, these parameters with those in equation (1) have a relationship:

$C = \frac{C_0}{1-\sum_{i=1}^{p}\theta_i}$, $\alpha = \frac{\sum_{j=0}^{q_1}\alpha_j}{1-\sum_{i=1}^{p}\theta_i}$, $\beta = \frac{\sum_{j=0}^{q_1}\beta_j}{1-\sum_{i=1}^{p}\theta_i}$, $\gamma = \frac{\sum_{k=0}^{q_2}\gamma_k}{1-\sum_{i=1}^{p}\theta_i}$, $\tau = \frac{\sum_{l=0}^{q_3}\tau_l}{1-\sum_{i=1}^{p}\theta_i}$, and $\delta = \frac{\sum_{m=0}^{q_4}\delta_m}{1-\sum_{i=1}^{p}\theta_i}$.

http://doi.org/10.18080/jtde.v11n4.743

Therefore, the model in equation (2) is also referred to as the long-term NARDL model (Ozturk & Acaravci, 2010). The residuals ε_{1t} are independent, identically distributed, and homoscedastic.

Several steps were taken to test the long- and short-term impacts of positive and negative shocks in exchange rates, the Internet, mobile, and telephone users on economic growth. The steps comprised testing variable stationarity, co-integration between variables, estimating model parameters, and the residual, and parameter stability requirements. It also examines the assumption of multicollinearity among independent variables.

The first step involved a stationarity test employing the Kwiatkowski, Phillips, Schmidt, and Shin (KPSS) test adopted from Kwiatkowski *et al.* (1992). The hypothesis formula used is H_0: time series is stationary, as opposed to H_1: time series is not stationary. The test criterion used was to accept hypothesis H_0 when the test statistic value is lower than its critical value at 1%, 5%, or 10% significance levels. The KPSS test developed by Kwiatkowski *et al.* (1992) tests the stationarity of a time series for a sample of 30 to 500 observations. The KPSS test is stronger than the Augmented Dickey-Fuller (ADF) test for a sample with 25 to 100 observations (Shin & Schmidt, 1992). Furthermore, Hornok & Larsson (2000) tested the strength of the KPSS test for a sample with 10 to 20 observations. The KPSS strength to test the stationarity of a time series with a small sample is in line with Kwiatkowski *et al.* (1992).

The next stage involved testing for co-integration between the Internet, telephone, mobile, positive and negative shock in exchange rates, and economic growth. The time-series data comprises three methods for testing cointegration, namely the Engle-Granger two-step, the ARDL Bound, and the Johansen tests. The Engle-Granger two-step test is applied to econometric models with a single equation, with all variables stationary at first differences and integrated with order 1, I(1). The co-integration test is accomplished by evaluating equation (1) and constructing (generating) its time-series residuals. When these time-series residuals are stationary at the level (a "level" in a time series refers to the overall value of a given variable over a period of time) or integrated of order 0, I(0), then all independent variables (PEX, NEX, NET, MOB, TEL) are co-integrated and have a long-term relationship with the dependent variable (Brook, 2019; Hill *et al.*, 2011). ARDL Bound cointegration test is also applied to a single equation, namely the ARDL equation. In this co-integration test, the stationarity of the variables involved in the model vary (Pesaran *et al.*, 2001). The Johansen co-integration test, which is applied to a system of equations, is generally used in Vector Autoregressive (VAR) models (Brook, 2019). This research used the NARDL co-integration test to determine the integration order of each variable and the number of equations in the model.

http://doi.org/10.18080/jtde.v11n4.743

The NARDL co-integration test follows the same procedures as the ARDL-bound co-integration test (Pesaran *et al.*, 2001). All the regressors of the NARDL model must be processed I(0) or I(1) to test the co-integration, meaning they must be stationary at the level of first difference. A dependent variable could be processed I(0) (Sam *et al.*, 2019). The NARDL model for testing cointegration could be:

$$D(GRO_t) = C_0 + \sum_{i=1}^{p-1} \theta_i D(GRO_{(t-i)}) + \sum_{j=0}^{q_1-1}\left(\alpha_j D(PEX_{(t-j)}) + \beta_j D(NEX_{(t-k)})\right) + \sum_{k=0}^{q_2-1} \gamma_k D(NET_{(t-k)}) + \sum_{l=0}^{q_3-1} \tau_l D(MOB_{(t-l)}) + \sum_{m=0}^{q_4-1} \delta_m D(TEL_{(t-m)}) + \theta_1 GRO_{t-1} + \theta_2 PEX_{t-1} + \theta_3 NEX_{t-1} + \theta_4 NET_{t-1} + \theta_5 MOB_{t-1} + \theta_6 TEL_{(t-1)} + \varepsilon_{2t} \quad (3)$$

where θ_i $(i = 1, 2, 3, 4, 5, 6)$ is the regression parameter and ε_{2t} is the residual. Testing was performed on the co-integration between a positive and negative shock in the exchange rate, the Internet, mobile, telephone, and economic growth in equation (3). The formulated hypothesis used is $H_0: \theta_1 = \theta_2 = \theta_3 = \theta_4 = \theta_5 = \theta_6 = 0$, where all time-series are not co-integrated, versus $H_1: \theta_1 \neq \theta_2 \neq \theta_3 \neq \theta_4 \neq \theta_5 \neq \theta_6 \neq 0$, with all time-series co-integrated. Hypothesis testing used the F-statistic or Wald-statistic, where the criterion rejected the H_0 hypothesis when the statistic test of upper bound I(1) exceeded the critical value at the 1%, 5%, or 10% significance levels.

The next stage involved estimating the equation (1) long- and short-term coefficients of the error correction model (ECM-ARDL) in equation (4). The ECM-ARDL model modifies equation (2) (Heij *et al.*, 2004):

$$D(GRO_t) = \alpha_0 D(PEX_t) + \beta_0 D(NEX_t) + \gamma_0 D(NET_t) + \tau_0 D(MOB_t) + \delta_0 D(TEL_t) + \pi EC_{t-1} + \sum_{i=1}^{p-1} \theta_i^* D(GRO_{(t-i)}) + \sum_{j=1}^{q_1-1}\left(\alpha_j^* D(PEX_{(t-j)}) + \beta_j^* D(NEX_{(t-j)})\right) + \sum_{k=1}^{q_2-1} \gamma_k^* D\left(NET_{(t-k)}\right) + \sum_{l=1}^{q_3-1} \tau_l^* D(MOB_{(t-l)}) + \sum_{m=1}^{q_4-1} \delta_m^* D(TEL_{(t-l)}) + \varepsilon_{2t} \quad (4)$$

where θ_i^* $(i = 1, 2, \dots, p-1)$, α_j^* $(j = 1, 2, \dots, q_1 - 1)$, β_j^* $(k = 1, 2, \dots, q_1 - 1)$, $\gamma_k^*(k = 1, 2, \dots, q_2 - 1)$, τ_l^* $(l = 1, 2, \dots, q_3 - 1)$ and δ_m^* $(m = 1, 2, \dots, q_4 - 1)$ are the parameters. EC_{t-1} is an error correction variable at time (t-1) that satisfies equation (5):

$$EC_{t-1} = GRO_{t-1} - C - \alpha PEX_{t-1} - \beta NEX_{t-1} - \gamma NET_{t-1} - \tau MOB_{t-1} - \delta TEL_{t-1} \quad (5)$$

http://doi.org/10.18080/jtde.v11n4.743

When, in equation (1), $\alpha \neq \beta$, the test decision is a long-term asymmetric effect of exchange rates on economic growth. Conversely, when, in equation (4), $\alpha_0 \neq \beta_0$ and $\alpha_j^* \neq \beta_j^*$ $(j = 1, 2, \ldots, q_1 - 1)$, the exchange rates asymmetrically affect economic growth in the short term. Equation (4) involves D(PEX), D(NEX), D(NET), D(MOB), and D(TEL) as the regressor or the first difference between PEX, NEX, NET, MOB, and TEL variables. This transformation is useful for eliminating multicollinearity between regressor variables (Koop, 2006; Gujarati & Porter, 2009; Shin *et al.*, 2014).

The validity of the parameter estimation results in equations (1) and (2) was determined by testing the normality, independence, and residual homoscedasticity. The tests used are Breusch-Pagan-Godfrey (BPG), Breusch-Godfrey Serial Correlation LM (BGSCLM), and Jarque Berra (JB). Furthermore, the stability of equations (1) and (2) regression parameters was tested using the CUSUM and CUSUM Square tests (Brown *et al.*, 1975). This research also determined the assumption of multicollinearity in equation (1).

To determine whether the variables PEX, NEX, NET, MOB, and TEL are exogenous (not endogenous) variables, the endogeneity test was conducted using the J-statistic test, also called the Durbin-Wu-Hausman test. The J-statistic has a Chi-squared distribution with degrees of freedom equal to the number of regressors in the regression equation. The regression parameter estimation method relating to the endogeneity test is the two-stage least square (TSLS) or generalized method of moments (GMM). The hypothesis formulation in the J-statistic test is H_o: PEX, NEX, NET, MOB, and TEL are exogenous to GRO; the alternative hypothesis is H_1: PEX, NEX, NET, MOB, and TEL are endogenous (See Davidson & Mackinnon, 1993; IHS-Markit, 2017).

Results and Discussion

Results

Table 1. Results of the KPSS Test

Variable	Level		First Difference		Result of stationary test
	Intercept	Intercept and trend	Intercept	Intercept and trend	
NET	0.690411**	0.177996**	0.552795	0.173604**	I(0)
TEL	0.414131	0.153211**	0.479141**	0.123060***	I(1)
MOB	0.693124**	0.201750**	0.731584**	0.155055	I(0)
PEX	0.610564**	0.150519**	0.284331	0.125285***	I(0)
NEX	0.659491**	0.167369**	0.311768	0.500000*	I(0)
GRO	0.695133**	0.158790**	0.261538	0.066552	I(0)

Source: Research finding.
Note: *, **, *** significant at 1%, 5%, 10%.

In the ARDL bound cointegration test, one variable must be non-stationary at the second difference or process I(2). To ensure this, every variable's stationarity was first tested using

http://doi.org/10.18080/jtde.v11n4.743

the tests of KPSS, as shown in Table 1. The Internet, mobile, positive and negative shock in the exchange rate, and economic growth variables are stationary or integrated of order 0, I(0). In contrast, the telephone variable is stationary at the first difference or integrated of order 1, I(1).

This research used the NARDL model with a single equation comprising an integrated variable of order 1, I(1), and order 0, I(0). Therefore, the co-integration test between the independent and the dependent variables was carried out using the ARDL Bound co-integration test. The co-integration test determined the Internet, telephone, mobile, positive and negative shock in exchange rates, economic growth, and the NARDL model's lag length. From the Akaike information criterion (AIC), the lag lengths p=3 and $q_1 = q_2 = q_3 = q_4 = 2$ were obtained. Furthermore, the NARDL(3,2,2,2,2) bound model was used to test for co-integration. The calculation of the F-test statistic obtained the F-statistic value of 33.07, compared with the critical statistical value of upper bound I(1) of 5.76 at a significance level of 5%. That is, the F-statistic value is more than the F-critical value. Therefore, there is a long-term relationship between a positive and negative shock in exchange rates, the Internet, cell phones, and growth. The long- and short-term coefficients in equations (1) and (4) were estimated. Table 2 displays the estimates of these coefficients.

Table 2. Long-Run and Short-Run Coefficients Estimation

Independent variable	Coefficient	t-Statistic	P-value
A. Long-run coefficients, dependent variable: GRO			
PEX	-0.876911	-4.972667	0.0156
NEX	0.858269	1.645616	0.1984
NET	0.327650	2.602713	0.0802
MOB	0.416925	4.767840	0.0175
TEL	0.093102	3.365624	0.0436
Constant	27.21383	80.76889	0.0000
B. Short-run coefficients, dependent variable: D(GRO)			
D(GRO(-1))	-0.579886	-8.641749	0.0033
D(GRO(-2))	-0.037280	-3.645185	0.0356
D(PEX)	-0.773370	-85.39890	0.0000
D(PEX(-1))	-0.307685	-7.327401	0.0053
D(NEX)	-0.640108	-14.25579	0.0007
D(NEX(-1))	-1.083090	-10.14017	0.0020
D(NET)	0.247196	26.01943	0.0001
D(NET(-1))	0.083681	8.389286	0.0036
D(MOB)	-0.020380	-1.972867	0.1430
D(MOB(-1))	-0.043380	-4.463320	0.0209
D(TEL)	0.067156	13.46396	0.0009
D(TEL(-1))	0.024617	4.631077	0.0190
EC(-1)	-0.328114	-26.35249	0.0001

Source: Research finding.
Note: P-values of test statistics: BPG, BGSCLM, and JB are 0.38, 0.39, and 0.97, respectively

Table 2 shows a column containing the variable coefficients and their probability values. These coefficients show the multiplier of the independent variables, including positive and negative

http://doi.org/10.18080/jtde.v11n4.743

exchange rate shocks, Internet, mobile, and telephone, to the dependent variable, economic growth. Some coefficient signs are positive, while others are negative. If the probability value is less than 1%, 5%, or 10% significance level, the positive coefficient indicates the positive influence of the independent variable on the dependent variables. In this case, an increase in the value of the independent variable increases the dependent variable. In contrast, the negative coefficient indicates the negative effect of the independent variable on the dependent variables. This means that an increase in the independent variable reduces the value of the dependent variable.

Panel A shows that the PEX coefficient is negative and significant at the 5% significance level because p-value=0.0156<5%, while the NEX coefficient is positive and insignificant, because p-value=0.1984>5%. The significance of the PEX coefficient economically shows the long-term effect of a negative exchange rate shock on economic growth. Furthermore, the different signs and values of the two coefficients imply the long-term asymmetric effect of the exchange rate on economic growth. Therefore, an increase of positive shock in the IDR/USD exchange rate reduces economic growth in the long term. The domestic exchange rate depreciation lowers economic growth in the long run. In contrast, the coefficients for the Internet (NET), mobile (MOB), and telephone (TEL) variables are positive and significant at 10%, 5%, and 5%, respectively, implying the long-term impact of ICT on economic growth. Therefore, increased ICT use boosts economic growth in the long run. Panel B shows that positive (PEX) and negative (NEX) shocks in exchange rate coefficients at time lag 0 and 1, respectively, are different and significant at 1% in the short term. Therefore, economic growth was asymmetrically impacted by IDR/USD exchange rate in the short term. The coefficients for the NET, MOB, and TEL variables at time lag 0 and 1 are significant, except for the D(MOB) variable, indicating ICT's short-term impact on economic growth. Therefore, the exchange-rate asymmetry affects economic growth in the short and long term. Furthermore, ICT affects economic growth in the short and long term.

A model requirement test was conducted regarding the completeness of testing the effect of positive and negative exchange rate shocks, Internet, mobile, and telephone on economic growth. The NARDL(3, 2, 2, 2, 2) model residuals are homoscedastic, independent, and normally distributed. The CUSUM and CUSUM Square test trends are shown on the left and the right side of Figure 1, respectively. This trend curve is between the two 5% significance limit lines, implying the stability of the NARDL(3,2,2,2,2) model parameters. Therefore, the stability assumption of the NARDL(3,2,2,2,2) model parameters is fulfilled.

http://doi.org/10.18080/jtde.v11n4.743

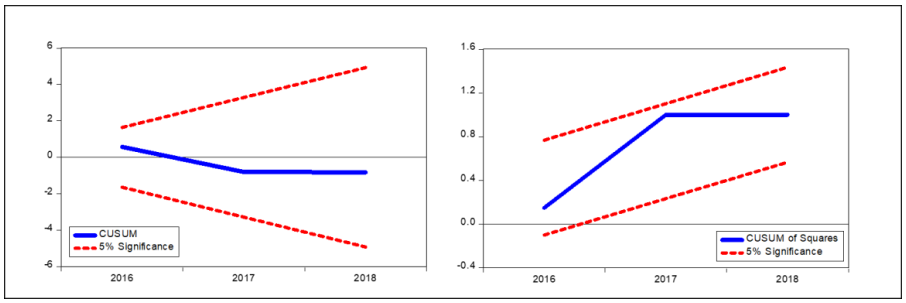


Figure 1. The CUSUM and CUSUM Square tests for NARDL(3,2,2,2,2) model parameters

The VIF for all independent variables (PEX, NEX, ITU, MOB, and TEL) is less than 10, as shown in Table 3. This indicates that there is no multicollinearity in model (1).

Table 3. VIF Estimation Results

Variable	VIF
PEX	9.00194
NEX	6.45138
ITU	7.38713
MOB	8.00801
TEL	3.431352

Discussion

This research revealed that the exchange rates asymmetrically affected long-term and short-term economic growth. A positive long-term increase in the IDR/USD rate negatively influences economic growth, characterized by a negative and significant positive shock coefficient value. Therefore, IDR depreciation reduced Indonesia's economic growth. A 1% increase in the IDR/USD exchange rate causes an 87.69% decrease in economic growth. This result is consistent with Kandil (2008), Bahmani-Oskooee & Mohammadian (2016), Wesseh & Lin (2018), and Hussain *et al.* (2019). This contradicts Yussof & Febrina (2014), Saidi *et al.* (2015) and Yuliardi (2020), which showed that the exchange rate affects Indonesia's economic growth symmetrically. Furthermore, these results support the theory on the effect of exchange rate asymmetry proposed by Kandil & Mirzaie (2002) and Kandil (2008). The theory states that unanticipated domestic exchange rate depreciation reduces economic growth.

This research found that ICT affected economic growth in the short and long run. The coefficients of the Internet, telephone, and mobile phone variables are significantly positive in the long term. The results imply that ICT positively influences economic growth. This confirms Amagiomyediwe & Annansingh-Jamieson (2017), Asongu & Odhiambo (2019), Solomon & Klyton (2019), Habibi & Zahardast (2020), Arabi & Allah (2017) and García (2019). The findings on the positive long-term influence of ICT on economic growth support Solow's and endogenous growth theories (Mankiw, 2007). This positive influence is an implication of the ICT development policy launched by the Indonesian government.

http://doi.org/10.18080/jtde.v11n4.743

Implications for practice and research

The findings showed that the Indonesian government should stabilize the IDR/USD exchange rate through monetary and fiscal policies to promote economic growth. The monetary and fiscal policies should support IDR/USD exchange rate appreciation to increase the trade balance, GDP, and economic growth. Monetary policy involves the process of decreasing the interest rates to a certain level without causing inflation to exceed the expected rate set by the Central Bank. Fiscal policy is the process of increasing exports and decreasing imports of goods. Indonesia's economic growth driven by ICT development still needs sustainability. Furthermore, the government should initiate ICT development in cities and rural areas. This development also involves the establishment of data and information-access speed.

The results are expected to contribute to empirical knowledge related to the asymmetric effect of exchange rates. It also shows an effect of ICT on economic growth and serves as a reference for future research.

Limitations and avenues for future research

This research was only conducted in Indonesia using IDR/USD as the currency exchange rate proxy. In the foreign exchange market in Indonesia, various currencies are traded in addition to the US dollar. Similarly, in international trade activities, currencies from other countries are often used instead of the US dollar, which have varying impacts on economic growth. Therefore, future investigation could be conducted in Indonesia and other countries on the use of different currency exchange rates or indices. Additionally, this research utilized telephone, Internet, and mobile phone users as proxies for ICT, which were examined using the analysis model. For future research, it is recommended to use an ICT index to avoid multicollinearity.

Conclusion and Recommendations

Foreign exchange rates and ICT play a vital role in the national economy. A currency forms a transaction instrument in international trade's real, service, and finance sectors. Furthermore, ICT is a means of communication between sellers and buyers in economic and business activities. This research aimed to determine the asymmetric effect of exchange rates and ICT on Indonesia's economic growth.

This research used yearly time-series data during the 1994–2018 period to test the asymmetric exchange rate and ICT's impacts on economic growth with the NARDL model. Furthermore, the ARDL bound co-integration test determined the long-term impact of positive and negative shocks in exchange rates and ICT on economic growth.

http://doi.org/10.18080/jtde.v11n4.743

The co-integration test showed that economic growth, positive and negative shocks in the exchange rate, and ICT were co-integrated. The long-term exchange rate positive shocks, Internet, mobile, and telephone coefficients are positive and significant. Therefore, the co-integration test shows a long-term effect of these variables on economic growth. The NARDL estimates showed that the exchange rates asymmetrically impact economic growth in the long term. Similarly, ICT affects economic growth. The ECM-NARDL estimates showed that exchange rates asymmetrically influenced short-term economic growth. ICT also affects economic growth in the short term, meaning that the exchange rate affects economic growth asymmetrically in the long and short term. Also, ICT affects economic growth in the long and short term. These findings could contribute to the economic literature and serve as input for the Indonesian government in monetary policy implementation and ICT development.

The findings imply that the Indonesian government must implement its monetary policy to stabilize the IDR exchange rate. Furthermore, ICT should be developed to respond to global advances and the increasing demand for its services.

The proxy for the exchange rate in this research was IDR/USD exchange rates. Therefore, future research could use a country's currency exchange rates against another foreign currency. Similarly, the ICT index could be used as a proxy for ICT, and there is a scope to research a wider area, such as ASEAN and Asia, by adding the government spending and inflation variables.

References

Abbasi, G. A., & Iqbal, D. J. (2021). The Asymmetric Impact of RER-misalignment on Economic Growth: An Application Hodrick-Prescott Filter Technique. *The Singapore Economic Review*. https://doi.org/10.1142/S0217590821500375

Aghaei, M., & Rezagholizadeh, M. (2017). The Impact of Information and Communication Technology (ICT) on Economic Growth in the OIC Countries. *Environmental & Socio-Economic Studies*, *17*, 255–276. https://doi.org/10.25167/ees.2017.42.7

Arfaoui, M. (2018). On The Spot-futures Relationship in Crude-refined Petroleum Prices: New Evidence from an ARDL Bound Testing Approach. *Journal of Commodity Markets*, *11*, 48–58. https://doi.org/10.1016/j.jcomm.2018.04.001

Amaghionyeodiwe, L., & Annansingh-Jamieson, F. (2017). An Investigation into the Impact of Mobile Technologies on Economic Growth and Employment in The Caribbean. *Athens Journal of Business & Econo*mics, *3*(3), 263–278. https://doi.org/10.30958/ajbe.3.3.3

Arabi, A. M. K., & Allah, B. A. W. (2017). The Impact of Information and Communication Technology (ICT) Development on Economic Growth in Sudan: An Application of ARDL Bounds Testing Approach. *Archives of Business Research*, *5*(3), 155–164. https://doi.org/10.14738/abr.53.2886

Asongu, S. A., & Odhiambo, N. M. (2019). Foreign Direct Investment, Information Technology, and Economic Growth Dynamics in Sub-Saharan Africa. *Telecommunications Policy*, *4*(1), 1–14.

Bahmani-Oskooee, M., & Saha, S. (2016). Do Exchange Rate Changes have Symmetric or Asymmetric Effects on Stock Prices? *Global Finance Journal*, *31*(C), 57–72. https://doi.org/10.1016/j.gfj.2016.06.005

Bahmani-Oskooee, M., & Mohammadian, A. (2016). The Asymmetric Effect of Exchange Rate on Domestic Production: Evidence from Nonlinear ARDL Approach. *Australian Economic Papers*, *55*(3), 181–191. https://doi.org/10.1111/1467-8454.12073

Bahrini, R., & Qaffas, A. A. (2019). Impact of Information and Communication Technology on Economic Growth: Evidence from Developing Countries. *Economies*, *7*, 1–13. https://doi.org/10.3390/economies7010021

Bao, H. H. G., & Le, H. P. (2021). Asymmetric Impact of Exchange Rate on Trade between Vietnam and Each of EU-27 Countries and the UK: Evidence from Nonlinear ARDL and The Role of Vehicle Currency. *Heliyon*, *7*(2021), e07344. https://doi.org/10.1016/j.heliyon.2021.e07344

Basirat, M., Nasirpour, A., & Jorjorzadeh, A. (2014). The Effect of Exchange Rate Fluctuation on Economic Growth Considering the Level of Development of Financial Markets in Selected Developing Countries. *Asian Economic and Financial Review*, *4*(4), 517–528.

Brooks, C. (2019). *Introductory Econometrics for Finance* (4th Ed.). New York: Cambridge University Press.

Brown, R. L., Durbin, J., & Evans, J. M. (1975). Techniques for Testing the Constancy of Regression Relationships over Time. *Journal of the Royal Statistical Society. Series B (Methodological)*, *37*(2), 149–192. https://doi.org/10.1111/j.2517-6161.1975.tb01532.x

Cortinhas., C., & Black, K. (2012). *Statistics for Business and Economics* (1st Ed.). Chichester United Kingdom: Wiley and Sons Ltd.

Davidson, R., & Mackinnon, J. G. (1993). *Estimation and Inference in Econometrics*. New York: Oxford University Press.

Elbadawi, I. A., Kaltani, L., & Soto, R. (2012). Aid, Real Exchange Rate Misalignment, and Economic Growth in Sub-Saharan Africa. *World Development*, *40*(4), 681–700. https://doi.org/10.1016/j.worlddev.2011.09.012

Farhadi, M., Ismail, R., & Fooladi, M. (2012). Information and Communication Technology Use and Economic Growth. *Plos One*, *7*(11), 1–7. https://doi.org/10.1371/journal.pone.0048903

Farouq, I. S., & Sambo, N. U. (2022). Real Exchange Rate and Economic Growth: The Interacting Role of Financial Development in Nigeria. *Iranian Economic Review*, *26*(4), 905–921. https://doi.orgh/10.22059/IER.2022.90664

Fred Economic Data. (2021). *Import Value (Goods): Total for Indonesia*. New York: Federal Research Bank of St Louis. https://fred.stlouisfed.org/series/XTIMVA01IDM667S

García-Muñiz, A. S., & Vicente, M. R. (2014). ICT Technologies in Europe: A Study of Technological Diffusion and Economic Growth under Network Theory.

Telecommunications Policy, *38*(4), 360–370. https://doi.org/10.1016/j.telpol.2013.12.003

Garcia, M. J. (2019). The Impact of Information and Communication Technology on Economic Growth in Mexico. *International Journal of Business and Social R*esearch, *9*(2), 11–22.

Gujarati, D. N., & Porter, D. C. (2009). *Basic Econometrics* (5th Ed.). New York: McGraw Hill.

Gujarati, D. N., & Porter, D. C. (2010). *Essential of Econometrics* (4th Ed.). New York: McGraw Hill.

Habib, M. M., Mileva, E., & Stracca, L. (2017). The Real Exchange Rate and Economic Growth: Revisiting the Case Using External Instruments. *Journal of International Money and Finance*, *73*(Part B), 386–398. https://doi.org/10.1016/j.jimonfin.2017.02.014

Habibi, F., & Zabardast, M. A. (2020). Digitalization, Education and Economic Growth: A Comparative Analysis of the Middle East and OECD Countries. *Technology in Society*, *63*, 1–9. https://doi.org/10.1016/j.techsoc.2020.101370

Ha, D. T-T., & Hoang, N. T. (2020). Exchange Rate Regime and Economic Growth in Asia: Convergence or Divergence. *Journal of Risk and Financial Man*agement, *13*(1), 1–15. https://doi.org/10.3390/jrfm13010009

Heij, C., De-Boer, P., Franses, P. H., Kloek, T., & Van-Dijk, H. K. (2004). *The Econometric Method with Applications in Business and Economics*. New York: Oxford University Press.

Hill, R. C., Griffiths, W. E., & Lim, G. C. (2011). *Principles of Econometrics*. Danvers, USA: John Wiley & Sons, Inc.

Hornok, A., & Larsson, R. (2000). The Finite Sample Distribution of The KPSS Test. *Econometrics Journal*, *3*, 108–121. https://doi.org/10.1111/1368-423X.00041

Hussain, I., Hussain, J., Khan, A. A., & Khan, Y. (2019). An Analysis of the Asymmetric Impact of Exchange Rate Changes on G.D.P. in Pakistan: Application of Nonlinear ARDL. *Economic Research-Ekonomska Istraživanja*, *32*(1), 3094–3111. https://doi.org/10.1080/1331677X.2019.1653213

Indonesia-Investments. (2021). The Indonesian Crisis Begins. Jogyakarta: Indonesia-Investments. https://www.indonesia-investments.com/culture/economy/Asian-financial-crisis/item246

IHS-Markit. (2017). *Eviews 10 User Guide*. Irvine: IHS Global Inc.

Jalil, A., Mahmood, T., & Idrees, M. (2013). Tourism–growth Nexus in Pakistan: Evidence from ARDL Bounds Tests. *Economic Modelling*, *35*, 185–191. https://doi.org/10.1016/j.econmod.2013.06.034

Kandil, M. (2004). Exchange Rate Fluctuations and Economic Activity in Developing Countries: Theory and Evidence. *Journal of Economic Development*, *29*(1), 85–108.

Kandil, M. (2008). The Asymmetric Effects of Exchange Rate Fluctuations on Output and Prices: Evidence from Developing Countries. *The Journal of International Trade & Economic Development: An International and Comparative Review*, *17*(2), 257–296. https://doi.org/10.1080/09638190701872772

Kandil, M., & Mirzaie, A. (2002). Exchange Rate Fluctuations and Disaggregated Economic Activity in The U.S.: Theory and Evidence. *Journal of International Money and Finance*, *1*, 1–31. https://doi.org/10.1016/S0261-5606(01)00016-X

Ketteni, E., Kottaridi, C., & Mamunea, T. P. (2014). Information and Communication Technology and Foreign Direct Investment: Interactions and Contributions to Economic Growth. *Empirical Economics*, *48*, 1525–1539. https://doi.org/10.1007/s00181-014-0839-1

Koop, G. (2006). *Analysis of Financial Data*. Chichester: John Wiley & Sons Ltd.

Kwiatkowski, D., Phillips, P. C. B., Schmidt, P., & Shin, Y. (1992). Testing the Null Hypothesis of Stationarity against the Alternative of a Unit Root. *Journal of Econometrics*, *54*, 159–178. https://doi.org/10.1016/0304-4076(92)90104-Y

Lee, J., & Yue, C. (2017). Impacts of the US Dollar (USD) Exchange Rate on Economic Growth and the United States Environment. *Energy Economics*, *64*, 170–176. https://doi.org/10.1016/j.eneco.2017.03.006

Mankiw, N. G. (2007). *Macroeconomics* (6th Edition). New York: Worth Publishers.

Meo, M. S., Chowdhury, M. A. F., Shaikh, G. M., Ali, M., & Sheikh, S. M. (2018). Asymmetric Impact of Oil Prices, Exchange Rate, and Inflation on Tourism Demand in Pakistan: New Evidence from Nonlinear ARDL. *Asia Pacific Journal of Tourism R*esearch, *23*(4), 408–422. https://doi.org/10.1080/10941665.2018.1445652

Millia, H., Adam, P., Saenong, Z., Balaka, M. Y, Pasrun, Y. P., Saidi, L. O., & Rumbia, W. A. (2020). The Influence of Crude Oil Prices Volatility, the Internet, and Exchange Rate on Indonesia's Number of Foreign Tourist Arrivals. *International Journal of Energy Economics and Policy*, *10*(6), 280–287. https://doi.org/10.32479/ijeep.10083

Nachrowi, N., & Usman, H. (2006). *Pendekatan Populer dan Praktis Ekonometrika untuk Analisis Ekonomi dan Keuangan*. Jakarta: Fakultas Ekonomi Universitas Indonesia.

Nguyen, T. T., Pham, T. A. T., & Tram, H. T. X. (2020). Role of Information and Communication Technologies and Innovation in Driving Carbon Emissions and Economic Growth in Selected G-20 Countries. *Journal of Environmental Management*, *261*, 1–10. https://doi.org/10.1016/j.jenvman.2020.110162

Ozturk, I., & Acaravci, A. (2010). The Causal Relationship between Energy Consumption and GDP in Albania, Bulgaria, Hungary, and Romania: ARDL Bound Testing Approach. *Applied Energy*, *87*, 1938–1943.

Pesaran, M. H., & Shin, Y. (1999). An Autoregressive Distributed Lag Modeling Approach to Cointegration Analysis. In S. Strom (eds), *Econometrics and Economic Theory in the 20th Century. The Ragnar Frisch Centennial Symposium* (pp. 371–413). Cambridge: Cambridge University Press.

Pesaran, M. H., Shin, Y., & Smith, R. J. (2001). Bounds Testing Approaches to the Analysis of Level Relationships. *Journal of Applied Econometrics*, *16*(3), 289–326. https://doi.org/10.1002/jae.616

Prabowo, G., & Gischa, S. (2021). Perkembangan Teknologi Informasi dan Komunikasi di Indonesia. Kompas.com. https://www.kompas.com/skola/read/2020/12/21/164007469/perkembangan-teknologi-informasi-dan-komunikasi-di-indonesia

Ramoni-Perazz, J., & Romero, H. (2022). Exchange Rate Volatility, Corruption, and Economic Growth. *Heliyon*, *8*(12), e12328. https://doi.org/10.1016/j.heliyon.2022.e12328

Ribeiro, R. S. M., McCombie, J. S. L., & Lima, G. T. (2020). Does Real Exchange Rate Undervaluation Promote Economic Growth? *Structural Change and Economic Dynamics*, *52*, 408–417. https://doi.org/10.1016/j.strueco.2019.02.005

Rosnawintang, R., Tajuddin, T., Adam, P., Pasrun, Y. P., & Saidi, L. O. (2021). Effects of Crude Oil Prices Volatility, the Internet, and Inflation on Economic Growth in ASEAN-5 Countries: A Panel Autoregressive Distributed Lag Approach. *International Journal of Energy Economics and Policy*, *11*(1), 15–21. https://doi.org/10.32479/ijeep.10395

Saidi, L. D, Kamaluddin, M., Rostin., Adam, P., & Cahyono, E. (2015). The Effect of The Interaction between US Dollar and Euro Exchange Rates on Indonesia's National Income. *WSEAS Transactions on Business and Ec*onomics, *12*, 131–137.

Saidi, L. O., Millia, H., Adam, P., Pasrun, Y. P., Munadi, L. O. M., & Sani, L. O. A. (2020). Effect of The Internet, Money Supply, and Volatility on Economic Growth in Indonesia. *International Journal of Advanced Science and Technology*, *29*(03), 5299–5310.

Saidi, L. O., Muthalib, A. A., Adam, P., Rumbia, W. A., & Sani, L. O. A. (2021). Exchange Rate, Exchange Rate Volatility, and Stock Prices: An Analysis of the Symmetric and Asymmetric Effect Using ARDL and NARDL Models. *Australasian Accounting, Business, and Finance Journal, 15*(4), 179–190. http://dx.doi.org/10.14453/aabfj.v15i4.11

Salahuddin, M., & Alam, K. (2016). Information and Communication Technology, Electricity Consumption and Economic Growth in OECD Countries: A Panel Data Analysis. *Electrical Power and Energy Sy*stems, *76*, 185–193. https://doi.org/10.1016/j.ijepes.2015.11.005

Sam, C. Y., McNown, R., & Goh, S. K. (2019). An Augmented Autoregressive Distributed Lag Bounds Test for Cointegration. *Economic Modelling*, *80*, 130–141. https://doi.org/10.1016/j.econmod.2018.11.001

Sathitwitayakul, T., & Prasongsukarn, K. (2011). Relativity of Economic Fundamentals and Fluctuation of Thai Currency: Spectra Analysis of Thai Baht REER (Real Effective Exchange Rate). *ABAC Journal*, *31*(1), 43–54.

Selimi, N., & Selimi, V. (2017). The Effect of Exchange Rate on Economic Growth in the Republic of Macedonia. *Eco Forum*, *6*(30), 50–55.

Setiawan, A. B. (2017). The Policy of Information and Communication Technologies Promotes the Formation of Future Business Models. *Jurnal Pekommas*, *2*(2), 193–204. https://doi.org/10.30818/jpkm.2017.2020210

Shin, Y., Yu, B. C., & Greenwood-Nimmo, M. (2014). Modeling Asymmetric Cointegration and Dynamic Multipliers in a Nonlinear ARDL Framework. In Sickels, R., & Horrace, W. (Eds), *Festschrift in Honor of Peter Schmidt: Econometric Methods and Applications* (pp. 281–314). New York: Springer.

Shin, Y., & Schmidt, P. (1992). The KPSS Stationarity Test is a Unit Root Test. *Economics Letters*, *38*, 387–392. https://doi.org/10.1016/0165-1765(92)90023-R

Solomon, E. M., & Klyton, A. (2019). The Impact of Digital Technology Usage on Economic Growth in Africa. *Utilities Policy*, *67*, 1–12. https://doi.org/10.1016/j.jup.2020.101104

Solow, R. M. (1957). Technical Change and the Aggregate Production Function. *The Review of Economics and Statistics, 39*(3), 312–320. https://doi.org/10.2307/1926047

Sreejith, P. M., & Sreejith, S. (2023). Exploring the Role of Cultural Capital, ICT Skills, and Entrepreneurial Self-efficacy in Shaping Entrepreneurial Intention among Women. *Journal of Telecommunications and Digital Economy*, *11*(2), 151–179. https://doi.org/10.18080/jtde.v11n2.711

Vinsensius, V., Assih, P., & Apriyanto, G. (2020). Signal of Rupiah Exchange Rate to US Dollar and Gross Domestic Product (GDP). *Journal of Auditing, Finance, and Forensic Accounting*, *8*(1), 1–10. https://doi.org/10.21107/jaffa.v8i1.5842

Virasa, T., Sukavejworakit, K., & Promsiri, T. (2022). Predicting entrepreneurial intention and economic development: A cross-national study of its policy implications for six ASEAN economies. *Heliyon, 8*(2022), e09435. https://doi.org/10.1016/j.heliyon.2022.e09435

Wang, P. (2009). *The Economics of Foreign Exchange Market and Global Finance* (2nd Ed.). Berlin: Springer-Verlag.

Wesseh, P. K., & Lin, B. (2018). There are Exchange Rate Fluctuations, Oil Price Shocks, and Economic Growth in a Small Net Importing Economy. *Energy*, *151*, 402–407. https://doi.org/10.1016/j.energy.2018.03.054

Wong, H. T. (2013). Real Exchange Rate Misalignment and Economic Growth in Malaysia. *Journal of Economic Studies*, *40*(3), 298–313. https://doi.org/10.1108/01443581311283934

Yuliadi, I. (2020). Determinant of Regional Economic Growth in Indonesia. *Jurnal Ekonomi & Studi Pembangunan*, *21*(1), 125–136. https://doi.org/10.18196/jesp.21.1.5035

Yussof, M. B., & Febrina, I. (2014). Trade Openness, Real Exchange Rate, Gross Domestic Investment, and Growth in Indonesia. *The Journal of Applied Economic Research*, *8*(1), 1–13. https://doi.org/10.1177/0973801013506398

Zakaria, R. (2021). Melihat Arah Kebijakan Teknologi Informasi dan Komunikasi di Indonesia. https://heylawedu.id/blog/melihat-arah-kebijakan-teknologi-informasi-dan-komunikasi-di-indonesia

Strategies and Challenges of Unified Payment Interface

Towards Facilitating a Digital Payments System in India

Athul Kuriakose
Sacred Heart College, Kochi, India

Sajoy P. B.
Sacred Heart College, Kochi, India

Abstract: The Indian economy is gradually curtailing its overdependence on currency-based transactions and thereby moving closer to digital and mobile-based payment transactions. The main objective of the paper is to provide an in-depth theoretical understanding of the Unified Payments Interface (UPI), its current pace of growth and the possible future penetration based on polynomial trendline projection, the possible challenges that limit future penetration, and the various strategies to overcome these challenges. The paper used the previous six years' UPI penetration statistics from 2016 to 2017 and established trends using polynomial trendline equation for the purpose of anticipating future penetration. The study also used statistics from published reports of the Reserve Bank of India (RBI) and the National Payment Corporation of India (NPCI) to draw meaningful conclusions on future UPI penetration. The study finds that the targeted one billion UPI transactions per day is achievable. The article contributes towards applied research by providing a decision-making tool to support policymakers, the government, and payment service providers, among others. Strategic applications of this research outcome include Unified Dispute and Issue Resolution processes, the RBI's lapse management, customer protection measures, UPI limit management, expansion of Internet user base and promoting digital financial inclusion in India.

Keywords: Unified Payments Interface, digital payments system, polynomial trendline projection

Introduction

India is the world leader in terms of the volume of digital transactions, with 48.6 billion in the year 2021, has surpassed China by almost three times and is higher than the combined volume of digital transactions of the US, UK, Canada, France and Germany (ACI Worldwide & Centre

http://doi.org/10.18080/jtde.v11n4.651

for Economics and Business Research (CEBR), 2022). India's real-time digital payment transactions volume stood at 31.3% of total payment transactions in the year 2021. The widespread adoption of digital payments in India benefited consumers and business entities, with an estimated cost savings of USD12.6 billion, which was almost .56% of the country's GDP in 2021 (Centre for Economics and Business Research (CEBR), 2022). The CEBR report forecast that the contribution of digital payments towards India's GDP could grow to US45.9 billion (1.12% of GDP) by 2026. India is the third fastest-growing real-time digital payments market in the world economy with a weighted average growth rate of 33.5% annually, behind Brazil (56.8%) and Oman (41%). The CEBR report also highlighted the role played by Unified Payments Interface (UPI) in facilitating the widespread acceptance of real-time digital payments among Indian users.

Although India is the global leader in real-time digital payments, the currency circulation in the Indian economy increased rapidly from USD199.12 billion (16.42lakh crore) (Gochhwal, 2017) during the time of demonetisation in November 2016 to USD366.70 billion (30.35lakh crore) (RBI, 2022) in October 2022. There was an increased penetration of 85% during the period. One of the main objectives of demonetisation was to reduce overdependence on paper currency in the Indian economy. However, the data released by the Reserve Bank of India (RBI) shows that dependence on paper currency is gradually increasing (RBI, 2022). Since overdependence on paper currency is not good for any economy, the RBI and the Indian Banking Association (IBA) jointly established the National Payment Corporation of India (NPCI) to promote digital payments in India. Since the introduction of the NPCI, the digital payments industry in India has undergone rapid growth during the last decade and continues this pace of penetration. As part of India's 'Digital India' campaign, the active Internet-enabled smartphone user base stands at 829 million (KPMG, 2021) and the total volume of digital transactions reached the benchmark level of 72 billion (RBI, 2022) with 64% of these transactions conducted through the UPI during the 2021–22 financial year. The high smartphone penetration in India is paving way for mobile-based payment systems. Since only 60% of India's population use smartphones and the currency circulation in India is still consistently increasing, there is still substantial room for further penetration of digital payments and the consequent achievement of digital financial inclusion.

The subsequent sections of this paper shed light on the available literatures relating to the role of UPI in facilitating the digital payments system in the Indian economy, the theoretical background and the possible penetration of UPI and other digital payment modes. The last section of the paper deals with the various strategies to overcome the possible challenges that need to be taken by the policymakers for achieving the targeted one billion UPI transactions per day by the 2026–27 financial year.

http://doi.org/10.18080/jtde.v11n4.651

Literature Review

The digital payments system's adoption of a cashless mode is yet to be widely and successfully adopted among consumers in emerging economies. Rahman *et al.*, (2020) find that Unified Theory of Acceptance and Use of Technology (UTAUT2) factors have significant influence on the adoption of cashless payments by consumers in developing economies. Shaikh *et al.* (2017) conceptualised a new mobile banking system called Mobile Based Payment System (MBPS) to overcome the challenges posed by the existing digital payment modes in developing economies, which include lack of convenience, scalability and usability. Pobee *et al.* (2023) studied the moderating effect of taxing the digital payments on the adoption of digital payments services in developing economies and found that taxing the digital payments services will negatively influence the adoption decision of consumers. The introduction of UPI fuelled acceleration and value addition to the existing digital payments sector of the Indian economy (Gochhwal, 2017). The UPI was introduced by NPCI and made publicly available through its indigenously developed BHIM (Bharat Interface for Money) UPI platform. The most widely used digital payment mode at the time of the introduction of UPI were e-wallets. The major drawback of digital or e-wallet-based digital payments was that one needed to add money to the wallet before making payments with no direct payments from the payer's bank account. The UPI-based payment technology primarily addressed this issue and allowed the payer to make payments directly from their bank account, thereby increasing competition in the digital payments industry to a cut-throat level (Bagla & Sancheti, 2018). The growth of UPI during its initial phase was moderate as there was only one NPCI-backed BHIM (a mobile-based UPI application) providing UPI services to banking customers in India. The entry of third-party application providers to the UPI ecosystem helped the rapid growth of UPI in India (Kumar *et al.*, 2022). UPI surpassed all other digital payment modes within three years of its official launch in terms of volume and value of transactions (Ahmed & Sur, 2023).

The existing literature on UPI focuses mainly on UPI theoretical background, various adoption determinants of UPI, customer satisfaction and use intention of UPI. Gochhwal (2017) studied the theoretical aspect of UPI and highlighted the convenience, cost-effectiveness and security of UPI as the key elements that drives users in adopting UPI. Kapur *et al.* (2020) developed a mathematical Bass model and empirically validated the model using the data collected from UPI users in India and found that word-of-mouth was the key determinant of UPI adoption in India. The UTAUT model and its extended versions are the most widely used models in the existing literature for measuring the adoption determinants of UPI (Mallik & Gupta, 2020). The study of Mallik & Gupta (2020) found that performance expectancy and perceived security were the major influencing factors when adopting UPI by customers. Fahad (2022) also studied the various determinants of UPI adoption in India and found that relative advantage,

http://doi.org/10.18080/jtde.v11n4.651

complexity and observability were the key determinants of UPI adoption. The relative advantage of UPI over digital wallets, Internet banking and other digital modes of payments attracts more customers towards UPI (Kuriakose *et al.*, 2022; Fahad, 2022).

While analysing the current literature on UPI, it is evident that it focuses only on the basic theoretical background and functioning of UPI, and its various factors of adoption and usage using various existing models. There is a gap in the existing literature with regards to the measurement of the future penetration level of UPI, identification of the various challenges that might prevent future penetration and the strategies that need to be adopted to overcome these challenges. Therefore, this study attempts to bridge this gap by incorporating a trendline equation using the polynomial trendline method for measuring future penetration of UPI. The study also proposes strategies to overcome the possible challenges that might limit the future penetration of UPI.

UPI Theoretical Background

UPI

"Unified Payment Interface (UPI) is a single-window mobile payment system introduced by the NPCI in 2016 to promote mobile-based payments in India. UPI allows the payer to make payment directly to the payee's UPI-linked bank account without providing any sensitive information about the payee such as bank account number, Indian Financial System Code (IFSC), account holder's name, and branch code" (Kuriakose *et al.*, 2022, p.2). UPI's single-window mobile platform allows the customer to add multiple bank accounts and thereby merge several banking features, seamless fund routing and merchant payments (National Payments Corporation of India, 2016). The customer needs to enter only the UPI-registered mobile number or the UPI ID or QR code of the recipient to send the money. There are currently 358 banks live on UPI in India and 52 banks and 22 third-party players are providing their own UPI applications for their customers (National Payments Corporation of India, 2022b). UPI applications provided by these banks and third-party players can be downloaded from the relevant app stores by the users. These applications are developed by Payment Service Providers (PSPs), which are considered important players in UPI's ecosystem. PSPs are the entities which are permitted to issue virtual addresses to the users and provide payment (credit/debit) services to individuals or entities, and are regulated by the RBI under the *Payments and Settlement Systems Act, 2007* (BHIM UPI, 2016). PSPs might be banks, mobile wallet providers, payment banks, or other third parties registered as PSPs in the RBI.

http://doi.org/10.18080/jtde.v11n4.651

Basic features and unique advantages of UPI

The need for a new digital payments system arises only when there are shortfalls in the existing digital payment modes. The introduction of UPI is also a result of such shortcomings in convenience, ease of use, usefulness and affordability of existing digital payment modes. NPCI successfully addressed such shortcomings through the introduction of UPI. The basic features of UPI make it simple and effective to make mobile-based digital payments and distinguishes itself from other payment modes. These features help to increase the UPI adoption level among customers:

- Functions in a mobile platform: Mobile phones are used as the primary device to initiate all payments through UPI. UPI-enabled mobile application is installed in the user's personal mobile phone and thereby can add more than one bank account in this application and can perform transactions from the required bank account as an option for the customer. Increased smartphone penetration in India helps UPI to expand its customer base.
- Multiple payment options available: UPI has the facility to offer multiple payment options compared to other digital payment modes. Customers can pay using multiple identifiers of the recipient such as the unique virtual address of the recipient, account number with IFSC code, mobile number and scanning QR code. This facility in UPI relieves customers from entering recipients' sensitive information when initiating transactions.
- One-click, two-factor authentication: UPI uses two-factor authentication to safeguard customers' interests and thereby avoid security threats. The first authentication is at the time of login to the app. It is either the fingerprint or face ID or password of the mobile phone. The second-factor authentication is the UPI pin at the time of making the payment. Since there is a two-factor authentication with UPI, it is considered to be the most secured digital payments platform compared to other digital payment modes.
- 'Push' and 'pull' based transactions enabled: UPI is the only mobile payment system that has the feature to initiate a transaction both from the side of the payer and the payee. A transaction that is initiated by the payer is called a push-based transaction and the transaction being initiated by the payee to request the payment from the payer is called a pull-based transaction.
- Merchant and end user-friendly: The UPI-based mobile payment system is highly merchant user-friendly as it allows the customer to make a payment by scanning the QR code displayed at the merchant shop, Internet, near field communication technology, Bluetooth, or any other standard protocol available in the UPI application.
- Involvement of PSPs: The UPI app that the end customer is using to make their UPI payments is developed and provided by PSPs. The PSPs might be a bank, a wallet provider,

http://doi.org/10.18080/jtde.v11n4.651

a payment bank, or any other third-party software provider. The PSPs are given the freedom to add more functionality in their app by the RBI and NPCI to meet the customer's growing needs. Since, there are more than 40 PSPs operating under the UPI ecosystem in India, they will try to add more improvements to attract more customers to their platforms.

UPI towards facilitating a digital payments system

The targeted volume of total retail digital payments transactions for the 2017–18 financial year set by India was 25 billion (Balakrishnan, 2017), and currently the total volume of UPI transactions alone recorded 45.96 billion for the 2021–22 financial year (National Payments Corporation of India, 2022c). UPI has become the frontrunner in the mobile and digital payments sector in India and has overtaken all other digital payment modes in terms of volume in just two and a half years since its launch. UPI recorded 6.58 billion transactions accounting for USD131 billion, averaging about 212 million transactions per day in the month of August 2022 (Kashyap, 2022). According to Kashyap (2022), the target volume of UPI transactions by the 2026–27 financial year is set at one billion transactions per day which is almost five times higher than current levels. UPI has surpassed all other digital payment modes such as Immediate Payment Service (IMPS), debit card payments, credit card payments, prepaid payment instruments (PPIs), and national electronic fund transfer (NEFT) in terms of volume and value of transactions. The total volume of UPI transactions grew from 17.9 million in the year 2016–17, the launching year, to 45.9 million transactions during the 2021–22 financial year. The total value of these transactions grew from USD.84 billion to USD1.014 trillion (National Payments Corporation of India, 2022c) and 314 banks are live on the UPI platform. Table 1 draws the meaningful conclusion that the number of UPI transactions grew at an average of 200% annually over the past four years.

Table 1. UPI growth statistics

Financial year	Volume of transactions (in millions)	Value of transactions (in billions)	No. of banks live on UPI
2016–17	17.90	69	44
2017–18	915.20	1,098	91
2018–19	5,353.40	8,770	142
2019–20	12,518.60	21,320	148
2020–21	22,330.70	41,040	216
2021–22	45,956.10	84,160	314

Source: National Payments Corporation of India, *Product Statistics* (2022c)

The pace of growth of UPI transactions when compared to other digital payment modes is substantially high. The penetration level of UPI in India is facilitating the overall growth of digital payments and thereby enriching the reach of digital financial inclusion in India. The growth statistics of UPI provided by the NPCI's Product Statistics report highlighted the active

http://doi.org/10.18080/jtde.v11n4.651

participation of banks when providing UPI services to its users (National Payments Corporation of India, 2022c). Banks are making increased efforts to expand the UPI services' reach to more targeted population. The participation of banks increased annually on an average of 52% over the past five years. The UPI holds 64% of the total volume of total digital payment transactions in India during the 2021–22 financial year (RBI, 2022). The penetration statistics of UPI from its month of launch shows UPI is the most influencing and facilitating digital payment mode in India's digital payments industry.

Methodology

The polynomial trendline equation method is a statistical method used to analyse and forecast trends in data that follow a nonlinear pattern. Polynomial trendline fits data to curves and these curves can be used to make projections and predictions about future values based on historical data points. It is widely used in existing studies to forecast projections of future penetration of various technologies and events based on previous years' data (Balakrishnan, 2017; Zhang & Jiang, 2021; Saksono & Fulazzaky, 2020). Balakrishnan (2017) adopted polynomial trendline equation to forecast the future penetration of digital payments in India and to check whether the targeted 25 billion retail digital payment transactions by 2017 are achievable. Other studies by Zhang & Jiang (2021) used a polynomial projection model to predict the future COVID-19 cases in China. Hence, polynomial trendline equation method is identified as the most suited method for projecting future penetration of UPI and other competing digital payment modes in India. Even though the pandemic played a crucial role in the increased penetration of UPI during the 2020–21 financial year, the growth rate of UPI during the post-pandemic period 2021–22 is more than that of the pandemic period of 2020–21. So, prediction using polynomial trendline equation is not affected by the growth of UPI during the pandemic period.

Results

Table 2 shows the pace of growth of UPI in terms of volume compared to other digital payment modes. The previous six years' performance of various types of digital payment modes such as IMPS, debit cards, credit cards, PPIs, NEFT, and NACH (National Automated Clearing House) are included in the table. The expected projection based on the polynomial trendline is also included in the table to understand whether the target of one billion UPI transactions per day can be achieved. The data shows that UPI surpassed all other digital payment modes within just three years of its official introduction. The weighted average growth rate of UPI comes to over 300% annually in terms of transactions. Since the published statistics on the number of UPI transactions is available on a monthly and yearly basis, the anticipated average future per-

http://doi.org/10.18080/jtde.v11n4.651

day UPI transaction is arrived at by converting the yearly data into per day data. As per the polynomial trendline projection, the expected UPI volume after five years will reach 450 billion transactions, and the per day transaction will be around 1.21 billion. So, the polynomial trendline projection indicates that the target of one billion UPI transactions per day can be attained within the targeted five years by maintaining the current pace and trend of growth.

Table 2. Item-based transaction matrix and future projections for the next five years (figures in million)

Serial No.	Financial year	IMPS	Debit card	Credit card	PPIs	NEFT	NACH	UPI
1	2016–17	506.7	2,399.3	1,087.1	1,963.7	1,622.1	2,057.3	17.9
2	2017–18	1,009.8	3,343.4	1,405.2	3,459	1,946.4	2,503.3	915.2
3	2018–19	1,752.9	4,414.3	1,762.6	4,604.3	2,318.9	3,035.2	5,353.4
4	2019–20	2,579.2	5,061.1	2,177.3	5,381.1	2,744.5	1,694.2	12,518.6
5	2020–21	3,278.3	4,014.6	1,764.1	4,974.3	3,092.8	2,611.1	22,330.7
6	2021–22	4,662.5	3,938.7	2,239.9	6,581.2	4,040.7	2,951.8	45,956.1
Trendline-based projection for the next five years								
7	2022–23	5,139.31	4,897.64	2,464.91	7,334.95	4,223.35	2,820.97	98,361.74
8	2023–24	5,951.05	5,193.57	2,672.2	8,146.67	4,679.28	2,919.68	147,448.16
9	2024–25	6,762.79	5,489.49	2,879.5	8,958.39	5,135.22	3,018.4	211,571.6
10	2025–26	7,574.52	5,785.42	3,086.8	9,770.11	5,591.16	3,117.11	318,612.38
11	2026–27	8,386.26	6,081.34	3,294.1	10,581.83	6,047.1	3,215.82	441,827.67

Source: Data are drawn from the RBI's Annual Reports from 2018–19 and 2021–22 (RBI 2021; RBI 2022)

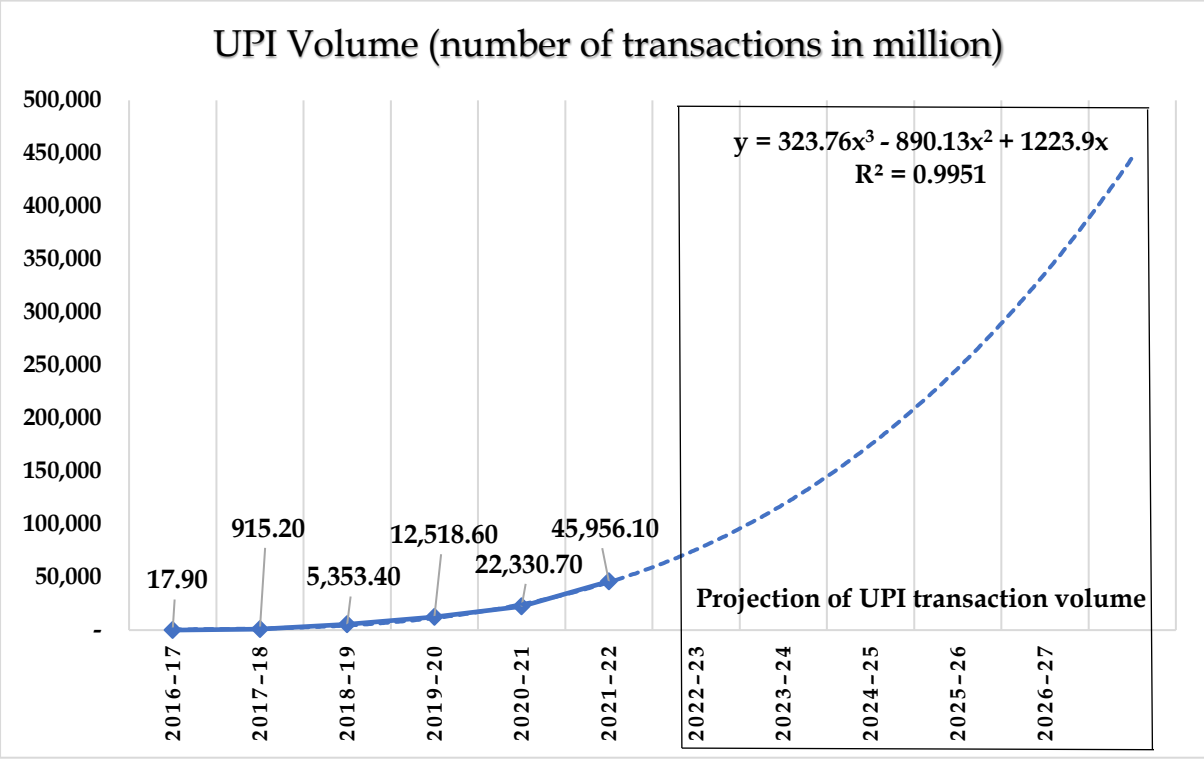


Figure 1. UPI transaction volume statistics with projections

Figure 1 shows the historical statistics of UPI volume penetration for the past six years and the trendline projection of UPI transaction volume for the next five financial years. The projections are based on the polynomial trendline equation as it is the trendline that best fits

http://doi.org/10.18080/jtde.v11n4.651

the projection with an R-square value of 0.9951. The results of the polynomial trendline projection show that the UPI volume will reach 450 billion transactions by the end of the 2026–27 financial year. The target of one billion transactions per day can be achieved within the next five years if UPI can maintain its current pace of penetration and through overcoming the challenges that limit the growth of UPI in future.

UPI growth during the pandemic period

The COVID-19 and associated lockdown paved way for the proliferation of online-based transactions (Donthu & Gustafsson, 2020) rather than offline transactions. The pandemic restricted people from direct contact with community and induced them to adopt digital payments (Allam, 2020). The major share of this opportunity was utilised by UPI payment applications, as it is the most advanced and convenient mode of mobile payment. The pace of growth of UPI in India during the pandemic was very high compared to other modes of digital payments. The main reasons for this rapid growth of UPI in terms of volume and value are ease of use of the UPI apps, cost and time effectiveness, promotional offers, and other rewards offered by various UPI apps due to heavy competition between them.

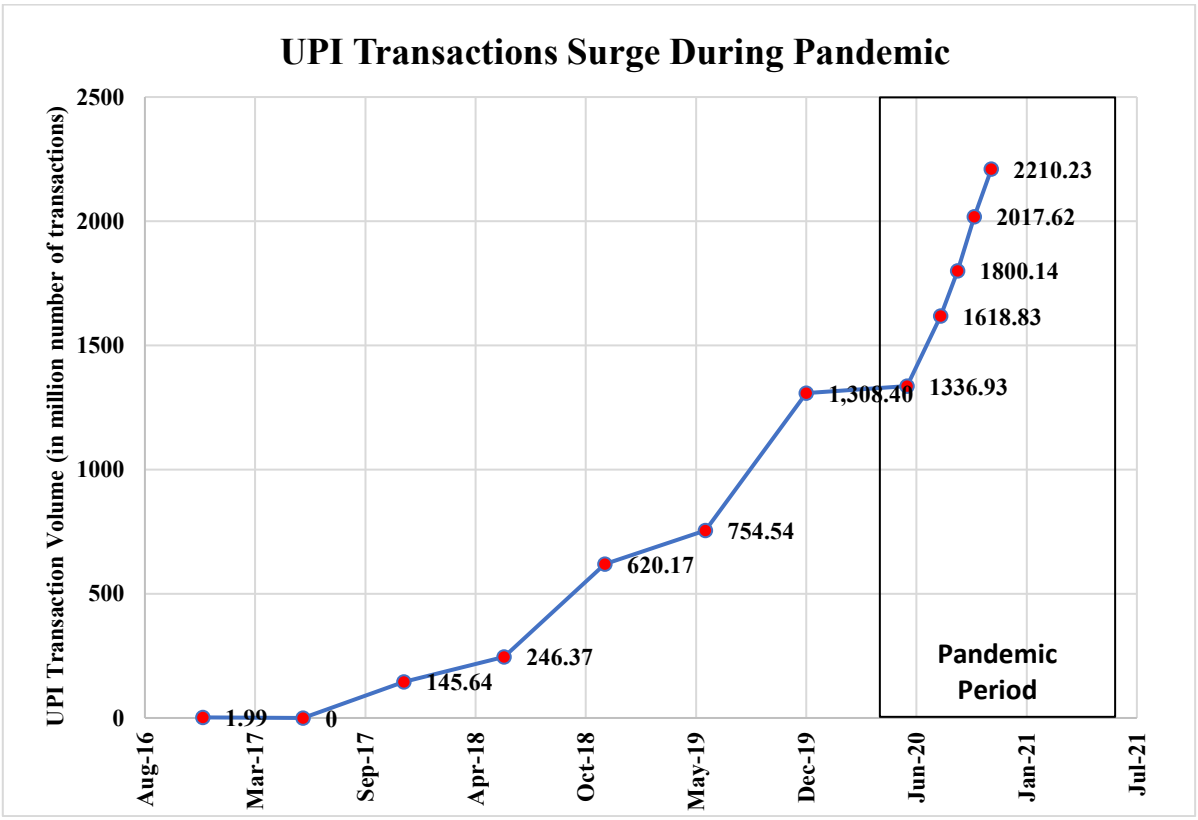


Figure 2. UPI transaction surge during pandemic period. Source: National Payments Corporation of India, *Product Statistics* (2022c)

UPI transactions more than doubled during the pandemic period from one billion in April 2020 to 2.23 billion in December 2020 (Figure 2). During this period, UPI transactions grew

http://doi.org/10.18080/jtde.v11n4.651

at an average 13.7% monthly. These figures shows that the acceptance and adoption of digital payment modes by users rose rapidly during the pandemic period and most users considered UPI as their primary digital payment mode. The pandemic added fuel to the pace of growth of UPI in India. Demonetisation of higher-value currencies also played a significant role along with the pandemic in boosting digital payments in India. But the statistics show that the growth rate of UPI after the pandemic period grew at a higher rate than the pandemic period. This shows that even though the COVID-19 pandemic accelerated the UPI penetration, the impact of the COVID-19 pandemic was limited on the overall penetration of UPI in India.

Discussion

Key strategies to strengthen UPI payments

Identifying the challenges faced by UPI when expanding its user base is important for PSPs when framing various strategies to overcome the challenges, which can be segregated into internal (infrastructural) challenges and external (accessibility) challenges. The PSPs should adopt specific strategies to tackle these internal and external challenges.

Strategies to overcome infrastructural challenges

UPI is facing the challenge of an increased failure rate on transactions initiated by customers. The technical glitches faced by both private and public sector banks in India are affecting the UPI-based payment transactions. There are several reasons that lead to the increased transaction failure due to technical glitches such as sudden increased penetration of UPI transaction volume over a short span of time, zero income generation to the bank as UPI charges no cost for making payments, lack of accountability for the failed transactions and the complexity of the UPI payment architecture (PWC, 2020). These challenges will bring down the pace of UPI penetration in India. So, it is desirable to adopt strategies to tackle these infrastructural challenges:

- Timely implementation of UDIR: Implementation of Unified Dispute and Issue Resolution (UDIR) for the purpose of resolving the complaints and redressals of customers regarding payment issues. UDIR is the concept introduced by the RBI in view of increased payment failure complaints received from payment customers. It is an automated single window redressal system specifically designed to resolve customers' UPI payment failure redressals. It was introduced by the RBI in the year 2020, but it lags in its timely implementation. So, the timely and strategic implementation of UDIR is necessary to tackle the infrastructural challenge of customer grievance redressal.
- The RBI's directions to examine the lapses: the RBI should periodically review the lapses by the participating banks in resolving the customer grievances related to UPI

http://doi.org/10.18080/jtde.v11n4.651

transactions. The RBI should also make the participating banks accountable for the payment failures due to technical glitches. This helps the RBI to identify the basic causes for these technical glitches and to fix these glitches permanently.

- Strengthening the guidelines for customer protection measures: the RBI should frame and periodically update the customer protection guidelines regarding payment grievances in line with safeguarding customers' interests. The guidelines should clearly undermine the limit of customers' liabilities in the event of unauthorised transactions or failed transactions. This helps to bring safety and protection to the minds of customers in delivering the UPI transactions and thereby increases the pace of UPI penetration.
- Increasing the transaction limit of UPI: The current UPI daily limit for UPI transactions is Indian Rupee (INR) 100,000 (limit changes with the participating banks) and up to 10 transactions per day. This limits the UPI usage among existing users and thereby compels them to adopt other payment mechanisms to transfer higher amounts than the limit. Through proper customer protection measures, it is advisable to increase the transaction limit of UPI payments to increase the extent of use.

Strategies to overcome accessibility challenges

India faces challenges in rural areas regarding Internet connectivity, digital infrastructure and digital literacy. In such areas it is difficult for a digital payments platform to grow as adequate Internet connectivity and digital education are necessary for building awareness of the UPI apps. PSPs should form appropriate strategies to tackle the accessibility challenges posed by UPI in its penetration:

- Promote Internet user base: The Internet user base of India stands at 43% of the total population (International Telecommunication Union, 2020) and is expected to reach 900 million users by the year 2025 (Internet And Mobile Association of India, 2019). The data shows more than half of the population is still out of the purview of Internet use. Since Internet participation by users is necessary for the growth of UPI, there should be proper infrastructural developments in rural areas for penetrating Internet users. The UPI user base can be improved from the existing level by promoting the Internet user base in India. Increased penetration of an Internet user base can help in increasing digital payments and thereby play a large role in helping the users to manage their personal finances and be financially included (RBI, 2020).
- Promote P2M payments: The peer to merchant (P2M) or person to merchant payments in terms of value of transactions was only 22% of total UPI transaction value (National Payments Corporation of India, 2022a) during the 2021–22 financial year. But the total volume of transactions of P2M and P2P is almost on par with each other. The statistics show users are reluctant to make high-value payments to the merchants on their

http://doi.org/10.18080/jtde.v11n4.651

purchases. So, the service providers should encourage the users to make P2M payments through more promotional and add-on benefits when making high-value UPI payments to merchants.

Practical Study Implications

The increased growth and penetration of UPI in India gives the clear indication that it emerged as a game changer in the digital payments industry. UPI had already surpassed all other digital payment modes in terms of volume and value of transactions in just two and a half years of its commencement by NPCI. UPI recorded 45.956 billion transactions worth USD1.014 trillion during the 2021–22 financial year, which is substantially ahead of its competitors such as debit cards, credit cards, PPIs, and IMPS. The polynomial trendline projection on the projected volume of UPI transactions for the next year shows that the India's targeted volume of one billion UPI transactions per day can be achieved by the 2026–27 financial year. This targeted volume can be achieved only if UPI can maintain its current pace of penetration. Only 31.3 % of total payments were in real-time digital mode during the 2021–22 financial year, and this shows that two-thirds of the entire transactions are done through cash payments. Most of the population is still out of the purview of UPI payments. So, there is substantial opportunity for UPI to expand its user base if it can successfully overcome the infrastructural and accessibility challenges. The tech giant Google's recommendation to the US Federal Reserve to draw lessons from India's successful performance of UPI is an example that the world is benchmarking UPI in the mobile payments industry. The exponential innovation, push and pull-based mobile transactions, multiple payment options, simplicity and security distinguish UPI from other payment modes. By implementing the strategies to overcome the challenges such as low penetration of UPI in P2M payments, challenges in Internet connectivity and lack of digital literacy, the UPI can achieve the targeted one billion transactions per day. The Indian economy can curtail its overdependence on currency transactions and thereby achieve the goal of a transparent economy through digital financial inclusion if the UPI can maintain its current pace of growth.

Conclusion

The main objective of the study was to have an in-depth theoretical understanding of UPI and its current pace of growth based on published UPI statistics by NPCI, and potential future penetration based on polynomial trendline projection. The study also discussed possible challenges that limit the future penetration of UPI, and the various strategies to overcome these challenges. The existing literatures concentrated mainly on the various adoption and usage determinants of UPI, and it helped the various PSPs in improving their UPI payment

http://doi.org/10.18080/jtde.v11n4.651

services. But when it comes to the projections based on the previous performance of UPI, the existing literature is lacking. The existing literature does not discuss the various challenges that limit the UPI growth rate and the various strategies that can be adopted to overcome these challenges.

This paper addresses this gap and introduces new tools for future UPI projection and provides various strategies for government and other PSPs in attaining their targeted one billion UPI transactions per day by the 2026–27 financial year. The polynomial trendline projection anticipates the targeted one billion UPI transactions can be achieved only through maintaining the current pace of growth. The current pace of growth can be maintained only through overcoming the infrastructural and accessibility challenges posed by UPI in India. The study put forward strategies to overcome infrastructural challenges which include timely implementation of UDIR, improvements in the current direction mechanism of the RBI in figuring out the lapses from the participating banks, periodic updating of guidelines for strengthening the customer protection, and increasing the transaction and daily limit of UPI. The study also provided strategies to overcome the accessibility challenges posed by UPI through increasing the Internet user base, especially in rural areas of the country and the need to promote P2M transactions. The adoption of these strategies by government and PSPs can improve the pace of growth of UPI in India and can achieve the targeted one billion UPI transactions by the 2026–27 financial year.

References

ACI Worldwide, & Centre for Economics and Business Research (CEBR). (2022). *Prime Time for Real-Time* (Issue April). https://www.aciworldwide.com/wp-content/uploads/2022/04/Prime-Time-for-Real-Time-Report-2022.pdf

Ahmed, S., & Sur, S. (2023). Change in the uses pattern of digital banking services by Indian rural MSMEs during demonetization and Covid-19 pandemic-related restrictions. *Vilakshan – XIMB Journal of Management*, *20*(1), 166–192. https://doi.org/10.1108/xjm-09-2020-0138

Allam, Z. (2020). The Forceful Reevaluation of Cash-Based Transactions by COVID-19 and Its Opportunities to Transition to Cashless Systems in Digital Urban Networks. In *Surveying the Covid-19 Pandemic and its Implications*. https://doi.org/10.1016/b978-0-12-824313-8.00008-5

Bagla, R. K., & Sancheti, V. (2018). Gaps in customer satisfaction with digital wallets: challenge for sustainability. *Journal of Management Development*, *37*(6), 442–451. https://doi.org/10.1108/JMD-04-2017-0144

Balakrishnan, M. (2017). Can India get to 25 billion retail digital transactions in 2017–18? *Journal of Payments Strategy & Systems*, *11*(3), 259–274.

BHIM UPI. (2016). *UPI Terms And Conditions*. https://www.bhimupi.org.in/terms-conditions#:~:text="Payment Service Provider" or ",and Settlement Systems Act%2C 2007.

Centre for Economics and Business Research (CEBR). (2022). *India Tops The World In Real-Time Payment Volumes In 2021*. https://cebr.com/reports/inc-42-india-tops-the-world-in-real-time-payment-volumes-in-2021/

Donthu, N., & Gustafsson, A. (2020). Effects of COVID-19 on business and research. *Journal of Business Research*, *117*(June), 284–289. https://doi.org/10.1016/j.jbusres.2020.06.008

Fahad, M. S. (2022). Exploring the determinants of adoption of Unified Payment Interface (UPI) in India: A study based on diffusion of innovation theory. *Digital Business*, *2*(2), 100040. https://doi.org/10.1016/j.digbus.2022.100040

Gochhwal, R. (2017). Unified payment interface-an advancement in payment systems. *American Journal of Industrial and Business Management*, *7*, 1174–1191. https://doi.org/10.4236/ajibm.2017.710084

International Telecommunication Union (ITU). (2020). *Individuals using the Internet (% of population) – India*. https://data.worldbank.org/indicator/IT.NET.USER. locations=IN

Internet And Mobile Association of India. (2019). Digital in India 2019. In *Nielsen*. https://cms.iamai.in/Content/ResearchPapers/2286f4d7-424f-4bde-be88-6415fe5021d5.pdf

Kapur, P. K., Sharma, H., Tandon, A., & Aggarwal, A. G. (2020). Studying BHIM app adoption using bass model: An Indian perspective. *International Journal of Mathematical, Engineering and Management Sciences, 5(1), 120–135*. https://doi.org/10.33889/IJMEMS.2020.5.1.011

Kashyap, H. (2022). UPI targeting 1 bn daily transactions in next 5 years: FM Nirmala Sitharaman. *Inc42 Daily Brief*. https://inc42.com/buzz/upi-targeting-1-bn-daily-transactions-next-5-years-fm-nirmala-sitharaman/#:~:text="UPI target is to cross, this number by around 394%25.

KPMG. (2021). *Contribution of Smartphones to DIGITAL GOVERNANCE IN INDIA A study by India Cellular & Electronics Association* (Issue July). https://icea.org.in/blog/wp-content/uploads/2022/06/ICEA-Digital-Governance-in-India-Report-2020.pdf

Kumar, A., Kar, S. K., & Bansal, R. (2022). The growth trajectory of UPI-based mobile payments in India: Enablers and inhibitors. *Indian Journal of Finance and Banking*, December, 45–59. https://doi.org/10.46281/ijfb.v11i1.1855

Kuriakose, A., P.B, S., & George, E. (2022). Modelling the consumer adoption intention towards unified payment interface (UPI): An extended UTAUT2 model with relative advantage, add-on services and promotional benefits. *2022 Interdisciplinary Research in Technology and Management (IRTM)*, 1–7. https://doi.org/10.1109/IRTM54583.2022.9791524

Mallik, P. K., & Gupta, D. (2020). A study on factors influencing consumer intention to use upi-based payment apps in Indian perspective. In *Information and Communication Technology for Intelligent Systems* (Vol. 2). https://doi.org/10.1007/978-981-15-7062-9_23

National Payments Corporation of India. (2016). *Unified Payments Interface (UPI) Product Overview*. https://www.npci.org.in/what-we-do/upi/product-overview#:~:text=Unified Payments Interface (UPI) is, merchant payments into one hood.

National Payments Corporation of India. (2022a). *UPI Ecosystem Statistics*. https://www.npci.org.in/what-we-do/upi/upi-ecosystem-statistics#innerTabThreeOct22

National Payments Corporation of India. (2022b). *UPI Live Members*. https://www.npci.org.in/what-we-do/upi/live-members

National Payments Corporation of India. (2022c). *UPI Product Statistics*. https://www.npci.org.in/what-we-do/upi/product-statistics

Pobee, F., Jibril, A. B., & Owusu-Oware, E. (2023). Does taxation of digital financial services adversely affect the financial inclusion agenda? Lessons from a developing country. *Digital Business*, *3*(2), 100066. https://doi.org/10.1016/j.digbus.2023.100066

PWC. (2020). *The remarkable rise of UPI in 2020* (Vol. 1, Issue December). https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/point-of-view/pov-downloads/the-remarkable-rise-of-upi-in-2020.pdf

Rahman, M., Ismail, I., & Bahri, S. (2020). Analysing consumer adoption of cashless payment in Malaysia. *Digital Business*, *1*(1), 100004. https://doi.org/10.1016/j.digbus.2021.100004

RBI. (2021). *Annual Report 2020–21*. https://m.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1293

RBI. (2022). *Annual Report 2021–22*. https://rbidocs.rbi.org.in/rdocs/AnnualReport/PDFs/9PAYMENTANDSETTLEMENT033C9414C22C4370AD16C837C55EDDC9.PDF

Reserve Bank of India. (2020). Assessment of the progress of digitisation from cash to electronic. In *RBI Occasional Paper*. https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=19417

Reserve Bank of India. (2022). *Money Supply for the fortnight ended October 21, 2022*. https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=54640

Saksono, T., & Fulazzaky, M. A. (2020). Predicting the accurate period of true dawn using a third-degree polynomial model. *NRIAG Journal of Astronomy and Geophysics*, *9*(1), 238–244. https://doi.org/10.1080/20909977.2020.1738106

Shaikh, A. A., Hanafizadeh, P., & Karjaluoto, H. (2017). Mobile banking and payment system: A conceptual standpoint. *International Journal of E-Business Research*, *13*(2), 14–27. https://doi.org/10.4018/IJEBR.2017040102

Zhang, J., & Jiang, Z. (2021). A new grey quadratic polynomial model and its application in the COVID-19 in China. *Scientific Reports*, *11*(1), 1–27. https://doi.org/10.1038/s41598-021-91970-1

Building Trust in Telesurgery through Blockchain-Based Patient Consent and Surgeon Authentication

Awwal Ishiaku
Innopolis University

Alexander Maloletov
Innopolis University

Abstract: Telesurgery, which enables remote surgical procedures, has the potential to revolutionize healthcare by improving access to specialized care and reducing costs. However, trust in telesurgery is a major concern for patients and healthcare providers. To address this issue, we propose a novel system for building trust in telesurgery through blockchain-based patient consent and surgeon authentication. Our system uses a smart contract on the blockchain to store patient consent and surgeon authentication data, which is securely verified by the telesurgery robot. We present a simulation of our system and evaluate its performance. Our results show that our system can authenticate surgeons and grant patient consent quickly and securely. This system has the potential to increase trust in telesurgery and promote its widespread adoption.

Keywords: Telesurgery, Security, Blockchain, Authentication.

Introduction

The field of healthcare has been revolutionized by recent advances in telemedicine and robotics, allowing for remote diagnosis, treatment, and surgery. Telesurgery is an emerging field that enables surgeons to perform operations remotely using robotic systems. However, telesurgery introduces several security and privacy challenges, including patient consent and surgeon authentication. We must ensure that the patient has given informed consent for the surgery and that the surgeon is authorized to perform the operation.

Blockchain technology has shown great potential in addressing these challenges, as it provides a secure and transparent platform for recording and verifying transactions. Smart contracts, which are self-executing agreements on the blockchain, can be used to automate the consent and authorization process, providing a tamper-proof and auditable record of the surgery.

http://doi.org/10.18080/jtde.v11n4.766

In this paper, we present a smart contract-based approach for patient consent and surgeon authentication in telesurgery. We propose a design for the smart contract that enables the patient to grant or revoke consent for the surgery and allows the surgeon to authenticate themselves using their address on the blockchain. We also describe the implementation of a remote-control architecture that ensures the surgeon is authorized before gaining control of the robot to perform the surgery. Finally, we evaluate the security and privacy of our system and compare it with existing approaches.

Smart contracts introduce a transformative approach to addressing informed patient consent by automating the consent process, creating immutable and transparent records, enforcing conditional execution, and ensuring real-time verification. These smart contracts enable what we refer to as "compliance by design". In practical terms, smart contracts actively enforce the rules and conditions defined within them, such as automating the consent and authorization process and ensuring that every step of the surgery aligns with the pre-defined terms. This unique capability of smart contracts to actively prevent the surgeon from performing specific steps unless authorized is a key differentiator in our approach, streamlining and securing the consent process, offering patients greater control and transparency over their healthcare decisions, and providing a comprehensive audit trail for healthcare providers, while reducing the risk of unauthorized procedures.

Background

Blockchain

Blockchain technology ensures the security and immutability of records through a combination of innovative features and mechanisms. These features make it exceptionally robust in preventing tampering and ensuring the permanence of data. Here, we delve into key aspects of blockchain technology that achieve this.

1. **Decentralization and Consensus Mechanisms:** Blockchains operate on a decentralized network of nodes, eliminating the need for a central authority. Changes to the data are only validated and recorded when a consensus among the network participants is reached (Murray, 2019). Various consensus algorithms, such as Proof of Work (PoW) and Proof of Stake (PoS), verify the accuracy of transactions and the state of the ledger before new blocks are added (Sriman *et al.*, 2021). This consensus mechanism ensures that any attempt to tamper with historical data would require an unfeasible amount of computational power and network control, making it highly secure against manipulation.

http://doi.org/10.18080/jtde.v11n4.766

2. **Immutability Through Cryptographic Hashing:** Blockchain employs cryptographic hashing to secure data. Each block contains a cryptographic hash of the previous block, creating a chain. If any data in a block is altered, the hash of that block changes, causing a cascading effect, rendering all subsequent blocks invalid (Komalavalli *et al.*, 2020). Immutability is further reinforced through the inclusion of timestamps, making it virtually impossible to change the order of blocks.
3. **Data Encryption:** Modern blockchains often integrate advanced encryption techniques, ensuring that data within a block remains confidential and secure (Hassan *et al.*, 2019). Even if an attacker gains access to the blockchain, the encryption of the data within each block makes it difficult to decipher. Encryption methods like Elliptic Curve Cryptography (ECC) are commonly used to secure transaction and identity data (Sammeta & Parthiban, 2022).
4. **Permissioned vs Permissionless Blockchains:** Blockchains can be categorized as either permissioned (private) or permissionless (public) (Helliar *et al.*, 2020). Permissioned blockchains restrict participation to known and authenticated entities, providing tighter control and privacy. In contrast, permissionless blockchains are open to anyone. Both types benefit from the immutability and tamper resistance intrinsic to the blockchain technology. The choice between these models depends on the specific use case and requirements for accessibility, transparency, and control.
5. **Public Ledger Transparency:** In the case of public blockchains, all transactions and data are transparent and accessible to anyone (Murray, 2019). This transparency enables the community to scrutinize the ledger for any inconsistencies or fraudulent activities, adding an additional layer of security. Any malicious actor attempting to tamper with public blockchain data faces the collective vigilance of network participants.

In summary, blockchain technology's robustness against tampering and its ability to maintain the permanence of records stem from a combination of factors. These include its decentralized and consensus-based structure, cryptographic hashing, data encryption, and the choice between permissioned and permissionless models. Such features make blockchain a powerful tool in various domains, including healthcare, finance, and supply chain management, where data integrity and security are paramount.

Blockchain in healthcare

Blockchain technology can revolutionize the healthcare industry by offering secure and transparent platforms for sharing and storing sensitive patient data (Tandon *et al.*, 2020). The decentralized and tamper-proof nature of blockchain allows for greater security and privacy while maintaining transparency and accessibility (Sanda *et al.*, 2022).

http://doi.org/10.18080/jtde.v11n4.766

One of the primary use cases for blockchain in healthcare is to improve the interoperability of electronic health records (EHRs) (Hylock & Zeng, 2019). The utilization of blockchain technology can enhance the sharing of patient data among various healthcare providers in a secure and efficient manner, which can alleviate administrative complexities and ultimately improve patient outcomes.

Another area where blockchain can be applied in healthcare is clinical trials. Clinical trial data is often siloed and not easily accessible, leading to slow and inefficient research processes (Houston *et al.*, 2018). Blockchain can enable the creation of a secure and transparent platform for recording and sharing clinical trial data, allowing for greater collaboration and efficiency in the research process.

In addition, blockchain can also enable secure and transparent supply chain management in the pharmaceutical industry. By tracking the entire supply chain of drugs and medical devices on a blockchain platform, stakeholders can ensure the authenticity and quality of products while reducing the risk of counterfeit or contaminated products (Uddin *et al.*, 2021).

Although blockchain technology has the potential to bring benefits to the healthcare industry, its adoption is limited due to several challenges and limitations. These include regulatory and legal barriers, technical complexities, and concerns around scalability and interoperability (Wright, 2019; Guo & Yu, 2022).

The implementation of blockchain in healthcare raises broad policy issues, requiring alignment with existing laws and regulations, evaluation of benefits and risks, and measures for testing and education. Integration with existing systems and the adoption of a minimal but sufficient approach to data on the blockchain are critical. The focus should also be on robust security and compliance. Additionally, employing blockchain for patient consent introduces specific challenges, including compliance with various jurisdictional laws, like GDPR [General Data Protection Regulation, EU] and HIPAA [Health Insurance Portability and Accountability Act, US], balancing data privacy and utility, defining a governance model, raising awareness, and addressing ethical and social implications.

Overall, blockchain technology has the potential to transform the healthcare industry by enabling secure and transparent platforms for sharing and storing sensitive patient data, improving clinical trials, and ensuring the authenticity and quality of drugs and medical devices.

Telesurgery

Telesurgery is a type of remote surgery that allows surgeons to perform operations on patients in different locations using robotic systems (Choi *et al.*, 2018). The aim of telesurgery is to

http://doi.org/10.18080/jtde.v11n4.766

provide patients with access to specialized surgical care, regardless of their geographic location, while also reducing healthcare costs and improving surgical outcomes (Mohan *et al.*, 2021).

Telesurgery systems typically consist of two main components: a console and a robot (Mohan *et al.*, 2021). The surgeon uses the console to remotely control the robot, which is located at the patient's site.

Telesurgery provides greater precision and control during surgical procedures, which is one of its main benefits. The robotic systems used in telesurgery are often more precise and dexterous than human hands, allowing for more delicate and complex procedures to be performed (Ahmad *et al.*, 2017). Telesurgery also has the benefit of making surgical care more accessible to patients who live in rural or underdeveloped locations. With the use of telesurgery, surgeons can carry out procedures remotely, reducing the need for patients to travel great distances for surgical care and bridging geographic barriers.

Telesurgery adoption faces several challenges and limitations, such as technical issues like latency and connectivity, regulatory and legal barriers, patient safety and data privacy concerns, and a demand for specialized training for healthcare professionals (Mohan *et al.*, 2021; Tamalvanan, 2021). Despite these challenges, telesurgery is an emerging field that holds great promise for improving access to surgical care and enhancing surgical outcomes. As technology continues to evolve and regulatory frameworks are developed, telesurgery is likely to become an increasingly important tool in the delivery of surgical care.

Smart contracts in healthcare

Smart contracts are digital contracts that enforce rules and regulations encoded within them, automatically executing the agreed-upon terms (Wang *et al.*, 2018). They are typically implemented on a blockchain, which provides an immutable ledger and transparent execution of the contract code. Smart contracts can enhance transparency, security, and efficiency in various healthcare industry sectors (Shah *et al.*, 2020).

Smart contracts can be utilized in healthcare to enhance the administration of EHRs. Smart contracts can enable patients to control access to their EHRs and allow healthcare providers to securely and efficiently share patient data across different systems. By providing complete and up-to-date medical histories, this can assist in decreasing administrative burdens and enhancing patient outcomes for healthcare providers.

Despite the potential benefits of smart contracts in healthcare, there are also several challenges and limitations to their adoption. These include technical complexities, concerns

http://doi.org/10.18080/jtde.v11n4.766

around data privacy and security, and the need for regulatory frameworks to ensure compliance with existing laws and regulations (Khan *et al.*, 2021).

Patient consent in healthcare

In healthcare, obtaining consent is a basic principle that guarantees patients the right to be educated about their medical treatment and make decisions regarding their own health management (Pietrzykowski & Smilowska, 2021). Informed consent is typically obtained through a process in which a healthcare provider explains the nature of the proposed treatment, including the risks and benefits, and obtains the patient's agreement to proceed. The significance of obtaining valid and meaningful consent from patients has gained greater recognition in recent years, fuelled by various factors, such as the growth of patient autonomy, advances in medical research and technology, and changing legal and ethical standards (Simon, 2020).

Obtaining valid consent can be challenging, and one of the difficulties lies in ensuring that patients are provided with sufficient information to make informed decisions (Simon, 2020). This can be particularly challenging in complex medical cases, where patients may struggle to understand the risks and benefits of different treatment options. To address this, healthcare providers are increasingly turning to tools like patient decision aids to support informed decision-making.

Ensuring that patients possess the ability to make decisions regarding their healthcare is another obstacle to obtaining valid consent. Patients with cognitive impairments, mental health conditions, or other disabilities may have difficulty understanding their treatment options and making informed decisions (Glezer *et al.*, 2011). Healthcare providers might need to collaborate with family members or other advocates to safeguard the patient's best interests in such situations (Glezer *et al.*, 2011).

In summary, healthcare providers are recognizing the significance of consent in healthcare as it is critical in enabling patients to make informed decisions about their medical treatment. Healthcare providers now utilize patient decision aids to support informed decision-making. With continued attention and investment in this area, we can work towards a healthcare system that fully respects and supports patient autonomy and informed decision-making.

Method

The proposed system is a blockchain-based telesurgery system that uses smart contracts to manage patient consent and surgeon authentication. The system consists of three components: the console, the robot, and the blockchain.

http://doi.org/10.18080/jtde.v11n4.766

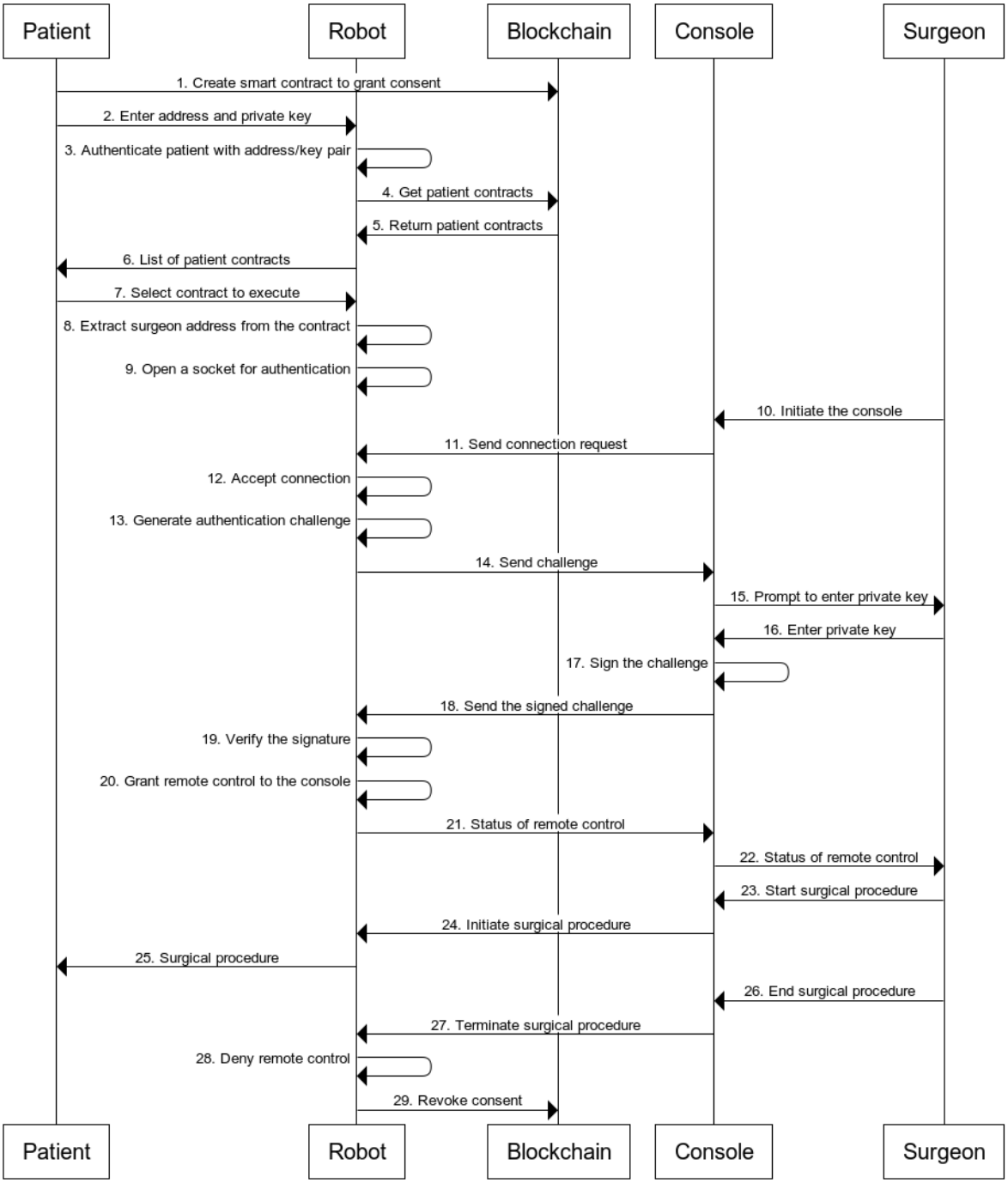


Figure 1. Sequence diagram of the proposed system.

The patient grants consent for the surgery on the blockchain as a smart contract. The smart contract contains three primary details, including the patient's identity, the surgeon's identity, and a validity period for the consent. The identities in this case are the patient's and the surgeon's addresses on the blockchain.

Before the remote procedure commences, the patient must authenticate to the robot and then select the contract for the surgery they wish to perform. The surgeon then authenticates themselves to the robot via the console using their address and private key pair. The robot verifies the surgeon's identity and checks the contract to verify that the surgeon has been

http://doi.org/10.18080/jtde.v11n4.766

granted consent to perform the surgery. If the surgeon is authenticated and has been granted consent, the console gains control of the robot, which can then be used to perform the surgery.

After the surgery is complete, the data is recorded on the blockchain, along with the outcome of the surgery and any follow-up care that may be required. The smart contract is then finalized, and the patient's consent is revoked. This ensures that the patient's privacy and security are protected and that they have complete control over their own medical treatment. The sequence diagram in Figure 1 details the steps we propose for the system.

Robot simulation

While we do not have an actual telesurgery robot, we can simulate the process of the telesurgery system to demonstrate its functionality. These actions include granting consent, authenticating, and revoking consent; and they do not require robotic movements.

In our simulation, we use three Linux endpoints, one for the console, the second for the robot, and the third for the blockchain. The endpoints each had a total of 8.1 GB of memory, and four processor cores with frequency of 3293.725 MHz each. All the components are interconnected, as shown in Figure 2.

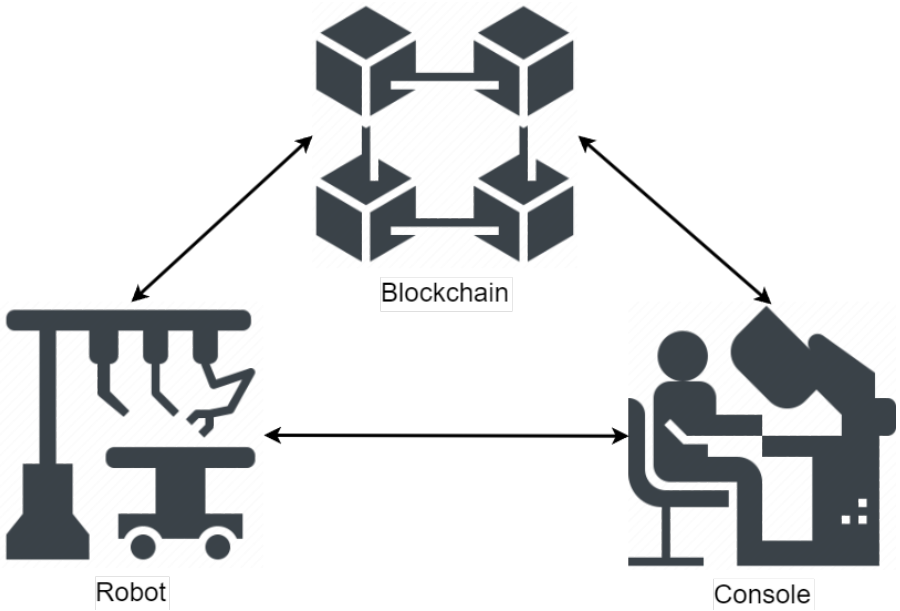


Figure 2. Network architecture.

Both the console and the robot are connected to the blockchain for authentication, and verification of the terms of the contract. We implemented the Blockchain component using the Ethereum blockchain, which is a widely used blockchain platform for developing decentralized applications. We compiled the smart contracts with Truffle (v5.8.1), and we used the Ganache (v2.7.0) blockchain emulator to simulate the Ethereum network. Ganache provides a local blockchain environment for testing, while Truffle provides a suite of tools for deploying and managing smart contracts. Both Ganache and Truffle are open-source and well

http://doi.org/10.18080/jtde.v11n4.766

documented, with a large and active community of developers. We simulated the robot and the console using the Python programming language.

Ethereum is a blockchain platform that enables decentralized applications (DApps) through self-executing smart contracts (Ethereum, 2022). Ethereum supports multiple programming languages, such as Solidity, Vyper, and Serpent, and has a large and active community of developers, researchers, and users. Ethereum uses a proof-of-work (PoW) consensus mechanism, which secures the network and prevents malicious attacks. However, Ethereum grapples with scalability issues, and resource-intensive operations, posing challenges for broader adoption (Chen *et al.*, 2020).

Truffle's capabilities encompass the following features: automated testing of contracts, compatibility with both web and console applications, package management, and network management (Verma *et al.*, 2023). Several drawbacks associated with Truffle and Ganache include their inability to replicate the primary network comprehensively, particularly concerning miners' behaviour and gas limit. According to Khan *et al.* (2021), developers can use Truffle to test that the smart contract meets specification; however, it cannot help them find bugs or vulnerabilities.

The simulation shows how the blockchain-based system can provide a secure and transparent means of managing patient consent and surgeon authorization, while also protecting the patient's privacy and security.

Implementation and Testing

In this section, we provide a detailed account of the simulation of the telesurgery system, including the development environment, the smart contract implementation, and the integration of the various components. We also describe how the telesurgery robot was simulated for the purpose of testing the system. Through this section, we aim to provide a comprehensive overview of the simulation of the telesurgery system.

Smart contract implementation

The smart contract for our telesurgery system was developed using the Solidity programming language, which is the primary language used for writing smart contracts on the Ethereum blockchain. The contract was designed to manage patient consent and surgeon authorization for a telesurgery procedure, and includes functions for granting and revoking consent, as well as for authenticating and authorizing the surgeon to gain access to the telesurgery robot.

The contract includes a consent mapping that maps patient addresses to Boolean values indicating whether consent has been granted or revoked. The contract also includes a surgeon

http://doi.org/10.18080/jtde.v11n4.766

mapping that specifies the surgeon's Ethereum addresses. We show the Solidity implementation of the contract in Listing 1.

Listing 1. Solidity implementation of the smart contract

```
pragma solidity ^0.8.0;

contract TelesurgeryConsent {
    address public patientAddress;
    address public surgeonAddress;
    uint public validityPeriod; // in seconds
    uint public consentTimestamp; // timestamp when consent was signed
    bool public isConsentSigned;

    constructor(address _patientAddress, address _surgeonAddress, uint
_validityPeriod) {
        patientAddress = _patientAddress;
        surgeonAddress = _surgeonAddress;
        validityPeriod = _validityPeriod;
        isConsentSigned = false;
    }

    function signConsent() public {
        require(msg.sender == patientAddress, "Only the patient can sign
the consent");
        require(block.timestamp < consentTimestamp + validityPeriod,
"Consent has expired");
        isConsentSigned = true;
        consentTimestamp = block.timestamp;
    }

    function revokeConsent() public {
        require(msg.sender == patientAddress, "Only the patient can
revoke their consent");
        isConsentSigned = false;
    }

    function getConsentDetails() public view returns (address, address,
uint, uint, bool) {
        return (patientAddress, surgeonAddress, validityPeriod,
consentTimestamp, isConsentSigned);
    }
}
```

The smart contract was tested extensively using Truffle and the Ganache blockchain emulator. Overall, the smart contract implementation provided a secure and efficient mechanism for managing patient consent and surgeon authorization in our telesurgery system. We show an example of one of the contracts we created in Listing 2.

Listing 2. Sample contract

```
{
  "patientAddress": {
    "name": "patientAddress",
    "type": "address",
    "value": "0x52CfF12eae83154..."
```


http://doi.org/10.18080/jtde.v11n4.766

```
  },
  "surgeonAddress": {
    "name": "surgeonAddress",
    "type": "address",
    "value": "0x76f0961247eF40D..."
  },
  "validityPeriod": {
    "name": "validityPeriod",
    "type": "uint",
    "value": "ea60"
  },
  "consentTimestamp": {
    "name": "consentTimestamp",
    "type": "uint",
    "value": "0"
  },
  "isConsentSigned": {
    "name": "isConsentSigned",
    "type": "bool",
    "value": true
  }
}
```

The robot

We simulated the robot using the Python programming language. The robot allows the patient to authenticate using their address and private key, and subsequently select a contract to be executed.

The robot is designed to accept a connection from the console that will provide remote control of the surgical robot. The connection between the robot and the console is established via a socket, and the surgeon is authenticated using their Ethereum address.

The robot imports the necessary modules, including `web3` to interact with Ethereum based smart contracts, `eth_account` to prepare the authentication challenge, `json` to load the ABI (Application Binary Interface) for the smart contract, `socket` to create a socket connection between the robot and the console, and `uuid` to generate a random challenge for authentication. In this context, "challenge" refers to a randomly generated message, typically in the form of a string, that is used to verify the identity of the surgeon during the authentication process. The actions performed by the robot are highlighted below.

- The robot authenticates the patient by prompting them to enter their Ethereum address and private key.
- It checks whether the entered private key corresponds to the entered Ethereum address. It does this by using the `web3.eth.account.from_key()` method to generate the Ethereum account associated with the provided private key. It then compares the lowercase version of the generated account address with the lowercase version of the

http://doi.org/10.18080/jtde.v11n4.766

provided patient address. If the two addresses match, authentication is successful; else the authentication fails.

- If the authentication is successful, the robot retrieves all contracts created by the patient, prompts the patient to select a contract, and verifies that the authenticated patient created the selected contract.
- If the contract selection is successful, the robot extracts the surgeon's address from the contract and opens a socket to listen for incoming connections from the console.
- The robot authenticates the surgeon with the address extracted from the contract when the console establishes a network connection. To authenticate the surgeon, the robot generates a random challenge, sends it to the console, and waits for a response. Refer to the authentication section for more details about the authentication.
- The robot grants the console remote control if the surgeon is authenticated. It does this by setting the value of the `remote_control` Boolean variable to `True`.
- Upon completion of the surgery, the robot disables remote control by setting the value of the `remote_control` Boolean variable to `False`. The robot also revokes the patient's consent by updating the smart contract to set the value of `isConsentSigned` to `False`.

The console

The console connects to the robot via a socket connection. The purpose of this simulation is to authenticate the surgeon who is operating the robot by verifying their private key.

- The console starts by importing the required modules, such as `socket`, `web3`, and `eth_account`.
- The console connects to the robot using the socket module and receives a challenge message from the robot.
- The console then prompts the surgeon to enter their private key.
- The console contains the `sign_challenge()` function, which takes the challenge message and a private key as input, signs the message using the private key, and returns the signature in hexadecimal format.
- The console sends the signed message back to the robot.
- Finally, it receives the authentication result from the robot.

Overall, this simulation plays a critical role in the telesurgery robot system's security by verifying the surgeon's identity before allowing them to operate the robot.

Authentication

The Ethereum signed data standard (ERC-191) (Swende & Johnson, 2016) plays a role in verifying the identity of the surgeon. The authentication steps are detailed below.

http://doi.org/10.18080/jtde.v11n4.766

1. The robot generates a random challenge and sends it to the console using the socket connection. The challenge is a string of the form `"Please sign this challenge: " + nonce`, where nonce is a random hexadecimal string.
2. The console receives the challenge and signs it with the private key of the surgeon using the `web3` library. The signature is a hexadecimal string that is derived from hashing and signing the challenge according to the Ethereum signed data standard version 0x45 (E). The standard requires hashing the challenge with the prefix `"0x19 <0x45 (E)> <thereum Signed Message:\n" + len(message) + challenge`. The signature includes the recovery parameter `v` to identify the chain on which the transaction is signed. The recovery parameter is either `27` or `28` depending on the network (`27` for the mainnets used in production, and `28` for the testnets used for testing purposes) to ensure that transactions are processed on the correct blockchain. The signature also includes the components `r` and `s`, which are components of the ECDSA signature that are generated by the signing algorithm. They are both 256-bit integers that depend on the private key, the message (challenge) hash, and a random number. They can be used to verify the signature by anyone who knows the public key and the message.
3. The console sends the signature back to the robot using the socket connection.
4. The robot receives the signature and verifies it using the `web3` library. The verification involves recovering the public address of the signer from the signature and the challenge according to the Ethereum signed data standard. The standard requires hashing the challenge with the same prefix as before and using the recovery parameter `v` to recover the address. The verification also checks if the recovered address matches the expected surgeon address.
5. The robot sends a confirmation or rejection message to the console based on the verification result.

We write the authentication process in more precise terms:

> Let m be the message, k be the private key, H be the keccak256 hash function, and S be the ECDSA signing function. Then, the signature sig is:
>
> $\text{sig} = S(H(0x19 \mathbin{//} E \mathbin{//} H(m)), k)$
>
> where $//$ denotes concatenation, and E is the version byte 0x45.
>
> To verify the signature sig, we need to recover the public key pk from sig and m, and check if it matches the address a derived from k. We can use the ecrecover function E to do that:
>
> $\text{pk} = E(H(0x19 \mathbin{//} E \mathbin{//} H(m)), \text{sig})$
>
> $a = H(\text{pk})(12:)$
>
> where (12 :) denotes taking the last 20 bytes of the hash.

http://doi.org/10.18080/jtde.v11n4.766

If a matches the expected address of the signer, then the signature is valid and authenticates the message m.

Evaluation and Discussion

To ensure the reliability of our simulated telesurgery robot system, we conducted thorough testing and evaluation. We designed a suite of test cases to cover various scenarios, including successful and unsuccessful authentication attempts, consent revocation, and remote-control requests. Overall, our results suggest that our proposed system can provide secure and efficient control of remote surgical robots, while maintaining patient privacy and consent.

Our simulation consisted of a total of 500 authentication attempts, each using a randomly generated challenge message. The average time it took for the console to sign the challenge using the surgeon's private key was 9.89 ms, while the average time it took for the robot to verify the signature was 7.21 ms.

Overall, our system performed well in terms of authentication speed, considering the fact that we simulated it with an interpreted program rather than a compiled program, which is much faster. The time it took for the surgeon to sign the challenge using their private key was relatively fast, indicating that the private key signing process did not significantly slow down the authentication process. The time it took for the robot to verify the surgeon's identity was also relatively fast. The authentication process can be optimized by ensuring that the communication protocol and the network link between the connected components are fast, efficient, and reliable.

Security and privacy analysis

While smart contracts on public blockchains like Ethereum provide transparency and immutability, they also have the drawback of exposing the transaction data to anyone with access to the network. In certain situations, such as in the case of medical data, confidentiality is a crucial requirement. To address this concern, we recommend that healthcare providers use blockchain platforms that offer confidential smart contracts such as Hyper ledger Fabric or R3 Corda. By using a blockchain platform that supports confidential smart contracts, it is possible to address the concerns around data confidentiality while still benefiting from the transparency and immutability that blockchain technology provides.

Overall, while the telesurgery system we have designed has the potential to improve patient care and provide a secure means of managing patient consent and surgeon authorization, it is important to address any potential security and privacy concerns to ensure that the system is both safe and effective.

http://doi.org/10.18080/jtde.v11n4.766

Comparison with existing systems

The Raven II surgical robot is a popular platform for research in teleoperated surgery (Li *et al.*, 2019); however, unlike our simulated telesurgery robot, it does not offer built-in authentication mechanisms to ensure the identity of the surgeon operating the robot (Bonaci *et al.*, 2015).

One of the most widely used telesurgery systems is the da Vinci Surgical System, which is a robotic surgical system that allows surgeons to perform minimally invasive surgeries (DiMaio *et al.*, 2011). Compared to the da Vinci system, our system has the advantage of using a blockchain-based smart contract to manage patient consent and surgeon authorization, which enhances security and privacy.

Our telesurgery system has several advantages over existing systems, including improvements in security and privacy via decentralized smart contracts, and scalability.

Conclusion

Our blockchain-based patient consent and surgeon authentication system has several potential advantages over traditional telesurgery systems. First, it provides a tamper-proof and transparent way to store and verify authentication data, which can help build trust between patients and surgeons. Second, it can potentially reduce the risk of unauthorized access to telesurgery systems, as only authenticated surgeons with valid private keys can access the system.

However, there are also several potential limitations to our system. One potential limitation is the reliance on blockchain technology, which may be unfamiliar or difficult to implement for some healthcare providers. Additionally, our system currently only supports authentication based on private key signing, which may not be the most secure or practical method for all situations. Finally, our simulation did not include potential network latency or congestion, which could impact authentication speed in a real-world telesurgery scenario.

Overall, our simulation provides a promising proof-of-concept for a blockchain-based patient consent and surgeon authentication system for telesurgery. Further research and development is needed to address the limitations and potential challenges of such a system, but we believe that it has the potential to improve the security and trustworthiness of telesurgery systems in the future.

http://doi.org/10.18080/jtde.v11n4.766

References

Ahmad, A., Ahmad, Z. F., Carleton, J. D., & Agarwala, A. (2017). Robotic surgery: current perceptions and the clinical evidence. *Surgical Endoscopy*, *31*, 255–263. https://doi.org/10.1007/s00464-016-4966-y

Bonaci T., Yan, J., Herron, J., Kohno, T., & Chizeck, H. J. (2015, April). Experimental analysis of denial-of-service attacks on teleoperated robotic systems. In *Proceedings of the ACM/IEEE sixth international conference on cyber-physical systems* (pp. 11-20). https://doi.org/10.1145/2735960.2735980

Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2020). A survey on Ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys (CSUR)*, *53*(3), 1–43. https://doi.org/10.1145/3391195

Choi, P. J., Oskouian, R. J., & Tubbs, R. S. (2018). Telesurgery: Past, present, and future. *Cureus*, *10*(5), e2716. https://doi.org/10.7759/cureus.2716

DiMaio, S., Hanuschik, M., & Kreaden, U. (2011). The *da Vinci* Surgical System. In: Rosen, J., Hannaford, B., Satava, R. (eds) Surgical Robotics. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-1126-1_9

Ethereum (2022). Ethereum development documentation. Ethereum.org. https://ethereum.org/en/developers/docs/

Glezer, A., Stern, T. A., Mort, E. A., Atamian, S., Abrams, J. L., & Brendel, R. W. (2011). Documentation of decision-making capacity, informed consent, and health care proxies: a study of surrogate consent. *Psychosomatics*, *52*(6), 521–529. https://doi.org/10.1016/j.psym.2011.06.006

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. *Blockchain: Research and Applications*, *3*, 100067. https://doi.org/10.1016/j.bcra.2022.100067

Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. *Future Generation Computer Systems*, *97*, 512-529. https://doi.org/10.1016/j.future.2019.02.060

Helliar, C. V., Crawford, L., Rocca, L., Teodori, C., & Veneziani, M. (2020). Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, *54*, 102136. https://doi.org/10.1016/j.ijinfomgt.2020.102136

Houston, L., Probst, Y., Yu, P., & Martin, A. (2018). Exploring data quality management within clinical trials. *Applied Clinical Informatics*, *09*, 072–081. https://doi.org/10.1055/s-0037-1621702

Hylock, R. H., & Zeng, X. (2019). A blockchain framework for patient-centered health records and exchange (healthchain): Evaluation and proof-of concept study. *Journal of Medical Internet Research*, *21*, e13592. https://doi.org/10.2196/13592

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, *14*, 2901–2925. https://doi.org/10.1007/s12083-021-01127-0

Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In Handbook of research on blockchain technology (pp. 349-371). Academic Press. https://doi.org/10.1016/B978-0-12-819816-2.00014-9

Li, Y., Hannaford, B., & Rosen, J. (2019). The Raven open surgical robotic platforms: A review and prospect. *Acta Polytechnica Hungarica*, *16*(8), 9–27. http://acta.uni-obuda.hu/Li_Hannaford_Rosen_95.pdf

Mohan, A., Wara, U. U., Shaikh, M. T. A., Rahman, R. M., & Zaidi, Z. A. (2021). Telesurgery and robotics: An improved and efficient era. *Cureus*, *13*(3), e14124. https://doi.org/10.7759/cureus.14124

Murray, M. (2019). Tutorial: A Descriptive Introduction to the Blockchain. *Communications of the Association for Information Systems*, *45*. https://doi.org/10.17705/1CAIS.04525

Pietrzykowski, T., & Smilowska, K. (2021). The reality of informed consent: empirical studies on patient comprehension—systematic review. *Trials*, *22*, 57. https://doi.org/10.1186/s13063-020-04969-w

Sammeta, N., & Parthiban, L. (2022). An optimal elliptic curve cryptography based encryption algorithm for blockchain-enabled medical image transmission. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1–13. https://doi.org/10.3233/jifs-211216

Sanda, P., Pawar, D., & Radha, V. (2022). Blockchain-based tamper proof and transparent investigation model for cloud VMs. *Journal of Supercomputing*, *78*, 17891–17919. https://doi.org/10.1007/s11227-022-04567-4

Shah, M., Li, C., Sheng, M., Zhang, Y., & Xing, C. (2020). Smarter Smart Contracts: Efficient Consent Management in Health Data Sharing. In: Wang, X., Zhang, R., Lee, Y. K., Sun, L., & Moon, Y. S. (eds), *Web and Big Data. APWeb-WAIM 2020. Lecture Notes in Computer Science*, vol. 12318. Springer, Cham. https://doi.org/10.1007/978-3-030-60290-1_11

Simon, A. (2020). Ethical Issues Concerning Patient Autonomy in Clinical Practice. In: Kühler, M., & Mitrović, V.L. (eds), *Theories of the Self and Autonomy in Medical Ethics*. The International Library of Bioethics, vol. 83. Springer, Cham. https://doi.org/10.1007/978-3-030-56703-3_8

Sriman, B., Ganesh Kumar, S., & Shamili, P. (2021). Blockchain Technology: Consensus Protocol Proof of Work and Proof of Stake. In: Dash, S. S., Das, S., & Panigrahi, B. K. (eds), *Intelligent Computing and Applications. Advances in Intelligent Systems and Computing*, vol. 1172. Springer, Singapore. https://doi.org/10.1007/978-981-15-5566-4_34

Swende, M. H., & Johnson, N. (2016). Erc-191: Signed data standard. *Ethereum Improvement Proposals*, 191. https://eips.ethereum.org/EIPS/eip-191

Tamalvanan, V. (2021). Foreseeable challenges in developing telesurgery for low income and middle-income countries. *International Surgery Journal*, *8*, 3228. https://doi.org/10.18203/2349-2902.isj20214033

Tandon, A., Dhir, A., Islam, N., & Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda.

Computers in Industry, *122*, 103290. https://doi.org/10.1016/j.compind.2020.103290

Uddin, M., Salah, K., Jayaraman, R., Pesic, S., & Ellahham, S. (2021). Blockchain for drug traceability: Architectures and open challenges. *Health Informatics Journal*, *27*, 146045822110112. https://doi.org/10.1177/14604582211011228

Verma, R., Dhanda, N., & Nagar, V. (2023). Application of Truffle Suite in a Blockchain Environment. In: Singh, P. K., Wierzchoń, S. T., Tanwar, S., Rodrigues, J. J. P. C., & Ganzha, M. (eds), *Proceedings of Third International Conference on Computing, Communications, and Cyber-Security*. *Lecture Notes in Networks and Systems*, vol. 421. Springer, Singapore. https://doi.org/10.1007/978-981-19-1142-2_54

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F.-Y. (2018). An overview of smart contract: Architecture, applications, and future trends. 2018 IEEE Intelligent Vehicles Symposium (IV), Changshu, China, 2018, pp. 108–113. IEEE. https://doi.org/10.1109/IVS.2018.8500488

Wright, S. A. (2019). Technical and legal challenges for healthcare blockchains and smart contracts. 2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K), Atlanta, GA, USA, 2019, pp. 1–9. IEEE. https://doi.org/10.23919/ITUK48006.2019.8996146

SBM-SA: A Safety Beacon Message Separation Algorithm for Privacy Protection in Internet of Vehicles

Zheng Jiang
Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia

Fang-Fang Chua
Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia

Amy Hui-Lan Lim
Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Malaysia

Abstract: A safety beacon message (SBM) plays a pivotal role in the Internet of Vehicles (IoV), broadcasting crucial events and road conditions to nearby vehicles. Given the sensitive nature of the data, such as vehicle identity and location, ensuring privacy is paramount. The significance of this research lies in addressing the pressing need for comprehensive privacy protection in the IoV, especially as most existing schemes focus on safeguarding either vehicle identity or location data during exchanges with core servers. The primary objective of this article is to introduce an SBM separation algorithm, termed SBM-SA, designed to holistically protect both identity and location data. Utilising correlation analysis, the SBM-SA stands as an innovative anonymisation privacy algorithm. Through a simulated IoV environment, the accuracy and efficacy of an SBM-SA are meticulously analysed and juxtaposed against prevailing privacy protection schemes. The findings underscore the SBM-SA's potential to significantly enhance privacy measures in the IoV. Implications of this research extend to shaping future privacy protection strategies of the SBM, emphasising the need for holistic and robust solutions in an increasingly interconnected vehicular landscape.

Keywords: Internet of Vehicles (IoV), privacy protection, safety beacon message (SBM).

http://doi.org/10.18080/jtde.v11n4.767

Introduction

With the promotion of the concept of Internet of Things (IoT), the technological evolution and popularity of the IoT are driving the transformation of traditional vehicle self-organising networks in the direction of a connected vehicle network. The development of computing and communication technology as well as a connected vehicle network is expected to provide enormous commercial and research value. Europe commenced the development of intelligent transportation systems (ITS) in the early 1970s and achieved significant advancements in the field of road traffic informatics (RTI). Subsequently, numerous projects were implemented across Europe to expedite the progression of ITS (Lin *et al.*, 2017). In the following decades, ITS has been widely researched and applied, becoming an important research direction and development trend in the field of transportation (Qureshi *et al.*, 2013).

The Internet of Vehicles (IoV) is a network of connected vehicles that can communicate with each other and with external systems, such as traffic management centres, to enhance the safety and efficiency of transportation. IoV safety-related applications comprise collision avoidance systems that leverage sensor data from vehicles to identify possible collisions and notify drivers to take evasive measures. Another safety-related application are emergency response systems, which can automatically call for help and provide location information in the event of an accident. Non-safety-related applications of the IoV include navigation and routing systems, which can help drivers find the most efficient route to their destination, taking into account real-time traffic data. In addition to safety and non-safety applications, there are special types of applications in the IoV called Paid Information Collection (PIC) applications. As the IoV increasingly focuses on using data to provide and optimise services, people are not willing to share their personal or vehicle privacy information. This greatly limits the development of IoV technology. Consequently, IoV service providers are increasingly choosing PIC applications, including crowdsourcing and crowdsensing. The IoV is a typical application of the IoT in ITS, which refers to a network of information exchange between 'people–vehicles–roads–clouds' according to certain communication protocols and data exchange standards. For example, V2V (Vehicle to Vehicle) solves the communication problem between vehicles; V2P (Vehicle to Pedestrian) solves the communication problem between vehicles and pedestrians; V2I (Vehicle to Infrastructure) solves the communication problem between vehicles and roadside infrastructure; and V2N (Vehicle to Network) (vehicle–cloud) (Jeong *et al.*, 2021). These network formats are collectively referred to as V2X (Vehicle to Everything), and their relationships are shown in Figure 1.

http://doi.org/10.18080/jtde.v11n4.767

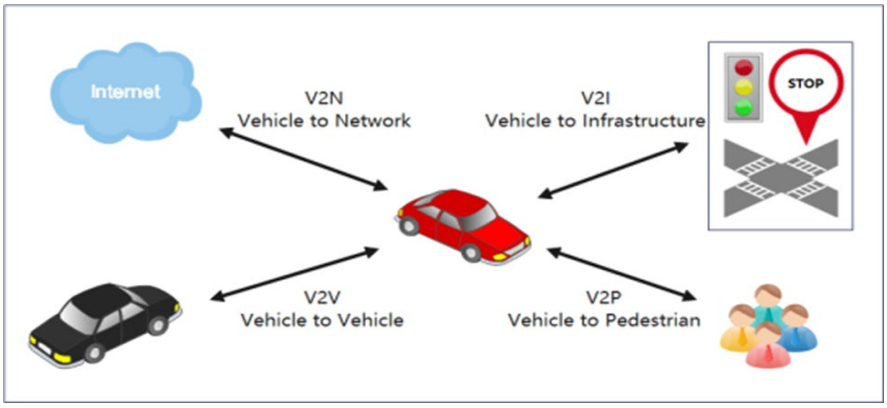


Figure 1. V2X architecture

The architecture of a centralised IoV is depicted in Figure 2, which consists of the core network, certification authority (CA), roadside unit (RSU) and vehicle (Kanumalli *et al.*, 2020). The core network plays an essential role in providing traffic information, services and management functions. The CA is responsible for managing and issuing digital certificates to authenticate vehicles and other devices as legitimate traffic participants. The RSU, installed on the roadside, communicates with vehicles, and provides traffic information and services such as traffic conditions, accident reports and road closure information. The vehicle is the core component of the IoV, communicating with the core network, CA and RSU to receive traffic information and services. The interaction between these components includes the RSU accepting vehicle requests and providing information and services to the vehicle, and the core network accepting vehicle requests and providing information and services to the vehicle. The CA authenticates the vehicle by creating a public key certificate for each vehicle, and the RSU obtains public key certificate information from the CA. Through this interaction, the core network, CA, RSU and vehicle can achieve more intelligent, efficient and secure urban transportation, improving traffic efficiency and safety, and providing a better travel experience for drivers and passengers.

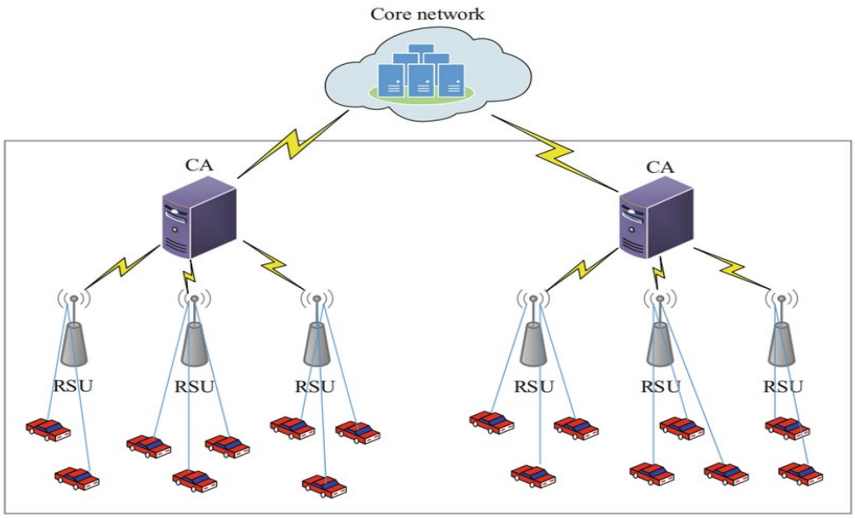


Figure 2. Architecture of a centralised IoV

http://doi.org/10.18080/jtde.v11n4.767

During the V2X interaction, a large amount of message data is transmitted, including an important message type called a safety beacon message (SBM). An SBM is a communication protocol for ITS that aims to improve traffic safety and data exchange rate. It is a short message format used to send specific traffic information to vehicles or other devices. An SBM contains many different types of information, such as road conditions, vehicle driving status, traffic signal status, accident warnings and road closure information. An SBM is transmitted through V2V or V2I communication, allowing driving vehicles to automatically receive and process this information, better adapting to road conditions and improving traffic safety. An SBM is designed to enable different types of vehicles and traffic devices to communicate with each other for improved coordination and management. Standardising and promoting SBMs can help promote the development and application of ITS, improving safety of urban traffic and lower the access threshold of IoV. The SBM uses specific data formats and transmission protocols to ensure timely transmission and correct reception of information. These messages include vehicle position, speed, acceleration, direction and braking statuses. The SBM can also transmit information related to road conditions, traffic flow, accident warnings and other safety-related information. In these messages, identity and location information are particularly important to the IoV. First, identity information is used to identify the legitimacy of participating vehicles in the IoV. Establishing a valid and authorised vehicle identity is essential for maintaining the proper functioning of V2V, facilitating legal responsibility investigation after traffic accidents.

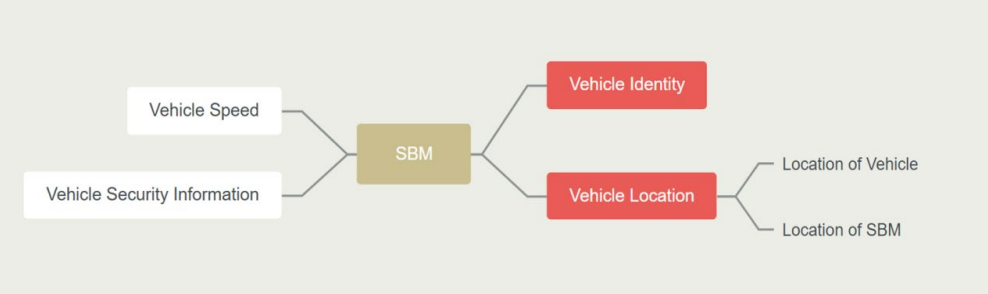


Figure 3. Components of the SBM

As shown in Figure 3, the SBM collected by the vehicle is based on location information and can be divided into two categories: Location of Vehicle (LV) and Location of the SBM (LS). Accurate location information is crucial for V2V to offer high-quality services to users. It is the aggregation and continuous exchange of the SBM that ensures that all connected vehicles can promptly receive safety data and perceive their surrounding traffic environment, including traffic flow, congestion and accidents. At the same time, the SBM can also be integrated with other vehicle communication systems and traffic management centre systems to form a complete traffic management network, make it easier for drivers or other related personnel to understand and use (Li *et al.*, 2018a). SBM is widely used in traffic safety applications in the

http://doi.org/10.18080/jtde.v11n4.767

IoV, including traffic accident warning and avoidance, road traffic information services, and vehicle flow control.

On the other hand, in PIC applications there are privacy leakages before SBM upload. Currently, many scholars have studied privacy protection issues in the IoV and proposed various privacy protection mechanisms based on anonymity, confusion, fuzziness and encryption, etc. However, these privacy protection mechanisms do not consider the correlations of time, space and data factors. Privacy concerns arise in PIC applications, as sharing personal and local sensor data with others is necessary to create useful services and knowledge. For example, the poisson line process algorithm utilises conditional random fields (CRFs) to model the spatiotemporal correlations among group sensing data and proposes an acceleration algorithm to learn the weakness of correlations, thereby enhancing data perception while protecting user privacy through filtering user context (Hou *et al.*, 2022).

The SBM-SA proposed in this paper is an avant-garde algorithm tailored for privacy preservation within the realm of the IoV. This algorithm, underscored by its unique application of correlation analysis, stands in contrast to prevailing methodologies. The SBM-SA is intricately designed to ensure the protection of users' identities and location privacy, all while retaining the comprehensive nature of the data. A salient feature of the SBM-SA is its emphasis on vehicle identity and location during SBM data exchange. Ingeniously, the algorithm clusters vehicles adhering to predefined criteria, leading to the creation of an anonymous group identity (GID). This GID, in essence, acts as a proxy for individual vehicles during the SBM data transmission, fulfilling the overarching privacy mandates. This work delineates a fresh perspective on IoV privacy challenges, setting it apart from previously discussed IoV privacy algorithms.

Literature Review

Privacy protection has gained significant attention in IoV research in recent years (Wu *et al.*, 2020). According to the objectives of privacy protection (PP), it can be divided into three types: PP of identity (Liu *et al.*, 2023), PP of location (Babaghayou *et al.*, 2023) and PP of trajectory (Jegadeesan *et al.*, 2021). Authentication is crucial in protecting the identity privacy of vehicles and receiving data from legitimate vehicles in the IoV. To achieve this, researchers have proposed several authentication mechanisms. For example, fog computing technology is used for pseudonym management in identity authentication, which enhances the ability of identity PP by leveraging the edge computing resources of vehicular networks (Song *et al.*, 2020). Although this solution can partially address the security issues in identity authentication, it is constrained by the computational capability of edge computing resources, leading to performance issues in pseudonym management. Additionally, a decentralised binary

http://doi.org/10.18080/jtde.v11n4.767

lightweight privacy-preserving authentication scheme, called the two-factor lightweight privacy-preserving authentication scheme (2FLIP), has been developed for identity authentication, which reduces authentication costs and achieves conditional privacy protection through a biometric-based binary approach (Nandy *et al.*, 2021). However, the security of 2FLIP relies on the unique system key stored by the CA. Another proposed authentication protocol is the layered pseudonym authentication protocol, which divides pseudonyms into two sub-ranges based on time, primary and secondary pseudonyms, and is beneficial in reducing the burden of the IoV system by communicating with fully trusted institutions and vehicles (Liu *et al.*, 2023).

With the rise of location-based services in the IoV, protecting the privacy of vehicle location has become a major concern for researchers. For example, one approach to protecting location privacy uses the subdivision method (Sadiah *et al.*, 2022). Firstly, an anonymous server generates a region unit that covers at least a certain number of users based on their true locations. To protect users' location privacy, an anonymous server calculates the geometric centre of the region unit as the anonymous location. This allows users to send or request data using the anonymous location instead of their true location. Additionally, the k-anonymity can also be achieved by using the micro-aggregation method (Ye *et al.*, 2023). The anonymous server sends data of k users together to the core server, resulting in confusion for the core server in identifying which data belongs to which user. Therefore, the micro-aggregation method only partially satisfies the requirements of location PP. The collection of vehicle trajectory data can help alleviate the pressure on the traffic management system in areas such as traffic congestion and tracking of offending vehicles. Therefore, research on vehicle trajectory PP has received widespread attention. An example of this data collection is the homomorphic encryption schemes which are used to achieve trajectory PP through key sharing between vehicles (Acar *et al.*, 2018). However, this key-sharing method has limitations and can only be applied in environments with high vehicle density. Another example is the use of a trajectory privacy strategy with multiple mixed regions (Memon *et al.*, 2018). By constantly changing pseudonyms, the pseudonyms cannot be linked, thereby protecting vehicle trajectory privacy. Some researchers have also proposed a route reporting scheme with privacy protection (Zhang *et al.*, 2020b). The proposed scheme employs both homomorphic encryption and error-checking and correction techniques to conceal and combine vehicle trajectories. By doing so, it not only ensures the privacy of drivers' paths but also mitigates collusion attacks from potentially malicious vehicles. In addition, according to the implementation mechanism of privacy protection, it can be divided into three types: PP of anonymity-based, PP of fuzziness-based and PP of encryption-based mechanisms (Garg *et al.*, 2020).

http://doi.org/10.18080/jtde.v11n4.767

The PP of anonymity-based mechanisms aims to protect the privacy of vehicle users by concealing their actual identity or location. To achieve this, k-anonymity technology is often employed, which anonymises the user's identity or location with k-anonymity as the core concept (Wang *et al.*, 2022). The maximum entropy principle is used to identify k suitable vehicles whose historical request probabilities are closest to that of the real vehicle, thereby protecting the privacy of the vehicle's identity or location. However, PP mechanisms based on anonymity typically require a trusted third-party anonymous server (such as a CA). This approach is only suitable for centralised applications, and the anonymous server may become a bottleneck when there are a large number of users, leading to slow service response times and poor user experience. Conversely, when the number of users is small, it may be difficult to achieve k anonymisation in a timely manner, rendering the PP of anonymity-based mechanism ineffective.

PP of fuzzy-based mechanisms often modify data attributes to safeguard user privacy. This involves using fake data for communication to avoid revealing the user's actual information. Random data perturbation techniques, such as adding random noise to the user's actual data, are commonly used. However, the method based on fuzziness results in significant information loss, which seriously affects the quality of service of the vehicular networks. Therefore, in practical vehicular network applications, the PP mechanism based on fuzziness is generally not used to protect user privacy.

The PP mechanism based on encryption is an important means of information protection. The encryption technologies commonly used include group signatures, bilinear mappings, public key infrastructure (PKI) encryption, and elliptic curve encryption; for example, the MixGroup method based on combining the mix-zone and group signature technologies (Hou *et al.*, 2021). The MixGroup method increases opportunities for anonymous exchanges in the group to protect user identity/location privacy. However, the mechanism based on encryption has high performance requirements for the user's terminal device, such as storage and computing capabilities.

With the accelerating evolution of technological revolution and industrial change, the IoV is gradually shifting towards a data-centred model. However, relying solely on naturally uploaded data from users is far from satisfying the data needs of the IoV. Therefore, the current trend in the IoV is towards PICs, such as crowdsourcing (Lin *et al.*, 2020) and crowdsensing (Qian *et al.*, 2021), which are popular low-cost methods for collecting SBM data. Although these are both PIC applications, they address different IoV scenarios: in IoV crowdsourcing applications, vehicles consciously and actively collect SBM data (Li *et al.*, 2020). The IoV backend publishes crowdsourcing tasks, and voluntary vehicles become targeted vehicles to execute the SBM data collection task. Therefore, the crowdsourcing

http://doi.org/10.18080/jtde.v11n4.767

applications of the IoV are targeted towards individual vehicles, without forming a concept of groups between vehicles, and do not have high requirements for vehicle density. However, crowdsensing applications are an extension of crowdsourcing applications, shifting from vehicles taking the initiative to vehicles passively cooperating without awareness. Therefore, in IoV crowdsensing applications, a group concept is formed among vehicles, and the vehicle group passively cooperates to collect SBM data (Mei *et al.*, 2020). The crowdsensing applications in the IoV require a high density of vehicles to participate in the SBM data collection task, which requires a large amount of SBM data collection, and the SBM data should have a certain correlation to each other.

The concept of crowdsourcing has been around for a long time, mainly referring to the practice of companies or enterprises breaking down a task and assigning it to volunteers, who complete the task in a voluntary and self-directed manner (Kietzmann, 2017). Due to its effectiveness and scalability as a business model, crowdsourcing has become a powerful tool for collecting large amounts of data at a relatively low cost, providing a potential solution to the high cost of data collection that has traditionally been a major obstacle. In the crowdsourcing applications of the IoV, connected vehicles use smart devices such as high-definition cameras, traffic recorders, communication devices and other sensors to execute crowdsourcing tasks. In the process of executing crowdsourcing tasks in the IoV, the tasks are first published from the IoV backend (central server). Then vehicles voluntarily receive tasks and become targeted vehicles, actively collecting specific data related to traffic safety, such as road conditions, traffic congestion and accidents.

Researchers have proposed various methods for crowdsourcing applications of the IoV. For example, Wang *et al.* (2020) used crowdsourcing to fill the gap in the ITS where events cannot be captured. By having the driver manually enter basic event information and aggregating it with other existing resources (such as TikTok and Twitter), the complete event is formed. The aggregation process is completed by the CrowdITS processing server. Finally, the CrowdITS processing server pushes events that the driver may be interested in, enhancing the driving experience of the ITS. Misra *et al.* (2014) pointed out that crowdsourcing is widely used to collect data from stakeholders, such as crowdsourcing data to solicit feedback on service quality and real-time information quality. Metlo *et al.* (2019) proposed a method for detecting and identifying specific vehicles based on crowdsourced data. The crowdsourced data comes from location data on vehicles obtained by smartphones. Users can wait for the vehicle they want on different routes, thereby tracking the current location of the vehicle and estimating the time required for the vehicle to reach their location. Zhang *et al.* (2020a) used crowdsourcing to aggregate data from multiple vehicles. Utilising this data, they detected and located potholes on multi-lane roads, improving the accuracy of traffic detection. Ali Sarker *et*

http://doi.org/10.18080/jtde.v11n4.767

al. (2021) first used crowdsourcing to collect sensor data (such as accelerometers and GPSs) from vehicle users' smartphones. Then, through dynamic time warping technology, they automatically processed heterogeneous data such as time deformation, speed and time mismatch, thereby improving the accuracy of road monitoring. Yang *et al.* (2018) used crowdsourcing to track the trajectory data of a large number of vehicles. They used a multi-level strategy and detailed data mining techniques to automatically generate road-based intersection maps.

From the above vehicle network crowdsourcing applications, it could be concluded that crowdsourcing is based on the principle of voluntary and active participation of vehicle users in collecting data related to a specific task. However, the aggregation of data may potentially result in privacy breaches for users. It is only through protecting the privacy of vehicle users that these applications can be more actively involved in crowdsourcing tasks and collecting relevant data. Therefore, privacy protection in vehicle network crowdsourcing applications needs to be further studied in order to promote further development of crowdsourcing applications. The advancement of sensors and mobile devices has led to the emergence of crowdsensing as a significant technology for gathering and transmitting sensing data (Huang *et al.*, 2017; Zappatore *et al.*, 2019). In a crowdsensing system, users utilise handheld devices as sensing units and collaborate through mobile networks such as Wi-Fi, 4G, and 5G to collect sensing data and complete complex social sensing tasks on a large scale. As a result, crowdsensing applications have gained considerable attention in the domain of the IoV (Li *et al.*, 2018a). Figure 4 illustrates the architecture of a typical crowdsensing system. In crowdsensing-based IoV applications, data perception and transmission are achieved through the intelligent terminals of vehicles or vehicle users, to obtain various information required for traffic management in a low-cost, fast and simple way; for example, social media analysis (El Khatib *et al.*, 2019), fine-grained air pollution monitoring (Liu *et al.*, 2016), urban environment monitoring (Nandy *et al.*, 2021), and road traffic data collection, etc. Corresponding measures are then taken based on the content of this information to address potential traffic management issues.

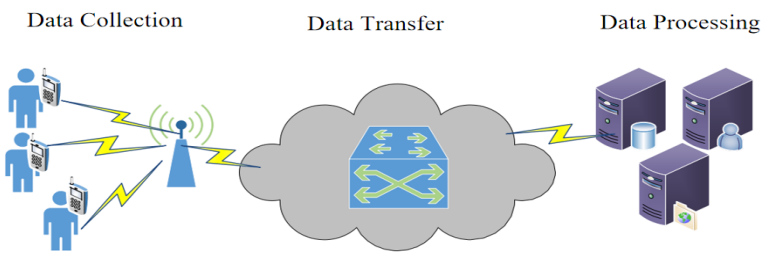


Figure 4. Workflow of crowdsensing system

http://doi.org/10.18080/jtde.v11n4.767

To encourage more users to accept crowdsensing applications, scholars have also studied many incentive mechanisms in crowdsensing systems, such as discrete crowdsensing incentive mechanisms (Liu *et al.*, 2020), trust-based incentive mechanisms based on reverse auctions (Zhang *et al.*, 2022), and offline and online incentive mechanisms for fair task scheduling (Capponi *et al.*, 2019). While incentive mechanisms have boosted users' enthusiasm for crowdsensing and expanded the range of potential applications, more users are now aware of the importance of protecting their personal data and are unwilling to participate in crowdsensing tasks due to privacy concerns. Moreover, the main feature of crowdsensing is the passive involvement of users. Such as users only need to have their smartphones activated, but they may not have complete knowledge of when and what data is being transmitted. The collected sensing data has a large scale and is related to time, space and content. Therefore, the privacy protection of users is worthy of research and discussion concerning crowdsensing applications in the IoV.

Comparison of existing work

In order to determine appropriate proposed methods, it is necessary to collect and compare previous related work. Table 1 summarises the privacy issues in SBM generation due to the inclusion of user location, identity and other information. Many researchers have studied privacy protection in the IoV (Kim *et al.*, 2022; Xiong *et al.*, 2019) and proposed various privacy protection mechanisms, including anonymity-based, obfuscation-based, fuzziness-based and cryptography-based mechanisms. However, these privacy protection mechanisms do not consider the correlation of time, space and data, but simply encrypt or anonymise the data itself. For example, obfuscation-based mechanisms may destroy the semantic information of the data, reduce its comparability, and lead to irreversible obfuscation in the obfuscation process. In the IoV scenario, personal and local sensing data need to be shared with others to generate valuable knowledge and services, which raises concerns about user privacy. Gao *et al.* (2022) proposed a novel trajectory obfuscation algorithm that can effectively hide user location information while maintaining data quality and task completion rates. The algorithm divides the user's trajectory into multiple segments and generates some fake trajectory segments in each segment, which are mixed with the real ones to prevent attackers from determining the user's real location.

However, trajectory obfuscation may affect the accuracy and integrity of data, as fake trajectory segments may introduce noise or interfere with real data. Zhang *et al.* (2021) proposed using geometric range query technology to transform the task recommendation process into finding suitable participants within a geometric range to protect user location privacy. The algorithm first transforms user location information into discrete grid points and

http://doi.org/10.18080/jtde.v11n4.767

then converts the task range into grid point ranges. Next, the algorithm uses geometric range query technology to search for suitable participants within the grid point range, avoiding direct exposure of user location information. The algorithm also uses some privacy protection strategies, such as adding noise to query results and limiting query frequency. However, converting user location and task range into grid points may introduce some discretisation errors, leading to less accurate recommendations. At the same time, geometric range queries require significant computational resources and time, which may affect application performance and response time. An algorithm for task allocation was proposed by Qian *et al.* (2021), which not only optimises task allocation in vehicle-based crowdsensing applications but also ensures PP of location and level of service provided. The algorithm treats participants and tasks in the sensing network as a bipartite graph and uses participants' location privacy and service quality as optimisation objectives and constraints, respectively. The algorithm then uses linear programming techniques to optimise the objective function and constraints to obtain the optimal task allocation algorithm while meeting location privacy and service quality requirements. However, the algorithm only considers location PP and does not consider other types of privacy protection, such as identity and behavioural privacy. At the same time, some researchers have proposed privacy protection strategies for crowdsourcing applications. For example, Zhang *et al.* (2020a) introduced a decentralised spatial crowdsourcing method for location PP in the IoV. This method aims to protect the location privacy of vehicles through decentralisation, while achieving effective spatial crowdsourcing task allocation and data collection. By adopting differential privacy-based data processing techniques, this method ensures that vehicle location information is not leaked, while achieving efficient task allocation and result verification. Liu *et al.* (2022) proposed a privacy protection solution based on data aggregation and batch authentication. By aggregating data, the exposure of individual data is reduced, and batch authentication is used to improve data credibility and processing speed. While protecting data privacy, this method takes into account system processing speed and performance, verifying its effectiveness and feasibility. This solution can be applied to various data-intensive application scenarios, providing a feasible method for privacy protection.

In the rapidly evolving domain of the IoV, a myriad of research has been dedicated to enhancing the privacy of vehicular communications. For instance, Xiong *et al.* (2019) delved into the balance of accuracy and privacy, underscoring the complexities inherent in mobile crowdsensing. While their insights are invaluable, they predominantly cater to specific IoV scenarios, leaving a broader array of challenges unaddressed. On a similar note, Babaghayou *et al.* (2023) and Benarous & Kadri (2022) have made significant strides in location privacy. However, their investigations are largely centred on specific techniques like geometric range

http://doi.org/10.18080/jtde.v11n4.767

queries and obfuscation, respectively. These studies, while groundbreaking in their own right, have yet to offer a comprehensive solution that addresses the multifaceted challenges of IoV privacy in its entirety. The potential of integrating crowdsourcing methodologies with the IoV, as hinted by more recent works like Gao *et al.* (2022) and Hou *et al.* (2021), suggests the possibility of a more encompassing solution. Yet, the literature still yearns for a definitive approach that seamlessly merges these domains.

Table 1. Summary of privacy methods in SBM generation

Source	Description	Method	Limitations
Gao *et al.* 2022	Propose an algorithm for preserving location privacy through obfuscation of trajectories	Differential privacy	➢ The primary focus has been on the protection of location privacy, with an absence of safeguards for other forms of privacy, such as identity and behavioural privacy ➢ Data loss caused by suppressing or obfuscating location data uploads ➢ Algorithms are complex and have performance issues
Zhang *et al.* 2021	Propose the location privacy-preserving task recommendation (PPTR) schemes with geometric range query in mobile crowdsensing without the trusted database owner	Geometric range query	
Qian *et al.* 2021	Use the differential privacy algorithm to preserve location privacy of the vehicle and submit it to IoV applications	Differential privacy	
Zhang *et al.* 2020a	A spatial crowdsourcing method for decentralised location privacy protection based on differential privacy algorithm is proposed for the IoV	Differential privacy	
Liu *et al.* 2022	Propose a privacy-preserving solution for data aggregation and batch authentication using differential privacy algorithm	Differential privacy	

From the synthesis of the literature, it is evident that within the intricate landscape of the IoV, privacy challenges are continuously evolving and diversifying. Concurrently, an escalating urgency exists to protect both the vehicle's location and the owner's identity. Distinct from solutions proposed in existing literature, this paper introduces the SBM-SA, a privacy-centric algorithm. Utilising correlation analysis, the SBM-SA offers a robust dual-layered protection

http://doi.org/10.18080/jtde.v11n4.767

mechanism safeguarding both the vehicle owner's identity and the vehicle's location data, thereby addressing this domain's existing gaps.

SBM-SA Design

In addressing the research gaps mentioned in the earlier sections. In this section, the proposed SBM separation algorithm (SBM-SA) is described. The SBM includes various types of data, and the SBM-SA mainly focuses on three types: road SBM (S1), accident SBM (S2) and traffic flow SBM (S3). Considering the directionality of data transmission, this section mainly analyses the data transmission scenario between vehicles and the core server in the IoV. After generating the SBM, when vehicle users upload the collected SBM to the core server for aggregation, they must also upload the event location (*EL*) of the SBM. This is because knowing the location of the traffic event is necessary to effectively utilise the SBM. For example, in the case of traffic jam, knowing the location of the jam is necessary to guide other vehicles to avoid the road jam segment. Without this location information, the traffic event itself is meaningless. However, the *EL* where the SBM occurred is likely to be the location where the vehicle passed. Therefore, the core server can infer the location where the vehicle appeared by analysing the *EL* in the SBM, which poses a privacy risk in the data generation process. To address this privacy threat, the SBM-SA is proposed. The SBM-SA mainly draws on anonymous privacy algorithms, including k-anonymity and l-diversity. However, anonymous privacy algorithms may lead to data correlation problems, that is, the anonymised data can still be restored or inferred to the original data through other information or multiple queries, thereby reducing the effectiveness of privacy protection. Therefore, the SBM-SA has been optimised for specific scenarios as explained below.

To update the core server with important information such as road maintenance, traffic congestion, traffic light changes, traffic accidents and traffic flow, vehicle U is required to upload the collected SBM. The SBM should also provide the *EL* for accuracy and reliability purposes. If the *EL* of the SBM is not provided, the value of the SBM collected by the vehicle to the IoV will be reduced. Assuming that the collected SBM has been uploaded, the vehicle can infer that it was present at the location where the SBM occurred. Therefore, directly uploading the collected SBM is highly likely to leak the vehicle's *EL*. For example, U is located at location EL_i. Just at this time, there was a car accident at location EL_i. Then, U collected the relevant SBM data Msg (EL_i) and uploaded it to the core server. If location El_i is important to vehicle U, the core server may invade the vehicle's location privacy. Furthermore, regardless of the time and location, if vehicle U sends Msg (EL_i), it can be inferred that vehicle U was present at location EL_i. Therefore, protecting the exact location where the SBM occurred is irrelevant. The purpose of the data upload process is to prevent the core server from obtaining

http://doi.org/10.18080/jtde.v11n4.767

the vehicle's exact location, without considering how to safeguard the location of the SBM occurrence. Therefore, the design purpose of the SBM-SA is to separate the relationship between the vehicle and the core server where an SBM occurs during the data upload process, which helps to safeguard the confidentiality of the vehicle's location information.

The logic and main workflow of the SBM-SA are explained as follows.

The main focus of the SBM-SA is on separation, which ensures the privacy of the vehicle's location by disconnecting the vehicle from the location *EL* where the SBM is collected. To achieve this, when the vehicle (U) collects SBM Msg (*ELO*) at a particular location *ELO*, the SBM-SA employs to separate the vehicle from the location *ELO* where the data was collected.

(1) Vehicle U does not immediately upload the collected SBM data Msg (*ELO*) to the core server. Instead, it first determines the time tolerance of Msg (*ELO*) and selects to upload it to the core server within the time tolerance range T. T is designed based on the corresponding SBM real-time needs to ensure that outdated information is not uploaded.

(2) Instead of uploading the identity of the vehicle, the collected SBM Msg (*ELO*) is uploaded as an anonymous group identity (GID).

(3) The GID not only serves as an identity credential for the uploading vehicle, but also enables data analysis through the correlation between the GID and the SBM, thereby further mining the value of data.

The SBM-SA's goal is to generate vehicle groups and obtain a GID with the help of time tolerance. To achieve this, vehicles passing through location *EL*0 within the time tolerance T are recorded and stored in a vehicle set {V1, V2, V3, ..., Vn}, where n vehicles have passed through *EL*0. The targeted vehicle U is represented by the red vehicle in Figure 5, while all vehicles passing through *EL*0 are represented by the green vehicles. The vehicle group is then initialised as G' = {V1, V2, V3, ..., Vn}. The anonymity degree of vehicle privacy protection is set to p, where a larger anonymity degree indicates better hiding effect of the vehicles. The size of p is determined according to the user's privacy protection requirements. To obtain the final vehicle group G from the initial group G', the final group should include at least p vehicles, and the targeted vehicle U must be included in the final group G to ensure that vehicle U is hidden in group G. In the SBM-SA, if the cardinality of the initial group G' is greater than p (i.e., n >= p), a random selection of p vehicles, which includes vehicle U, is made from G' to update and obtain the final group G = {V1, V2, V3, ..., Vp}. However, if n < p, the SBM-SA needs to select additional p−n vehicles to add to the initial group G'. To do so, a region A is constructed with a centre *ELO* and a radius T, as shown in Figure 5, and the selection of p−n is based on this region. V denotes the average speed of vehicles. According to theoretical analysis, vehicles are unlikely to move beyond region A within time T. In the case where n < p, the SBM-SA will

http://doi.org/10.18080/jtde.v11n4.767

select vehicles in region A that have not yet passed the *ELo*. These vehicles will be merged with the vehicles that have already passed the *ELo* and records them as {V1', V2', V3', ..., Vp–n'}. It is evident that the p–n vehicles are not part of the original set G' of vehicles, as illustrated in Figure 5, where the yellow vehicles represent these p–n vehicles. Subsequently, they are included in the initial set G' to form the final set G and generate a GID for the group G.

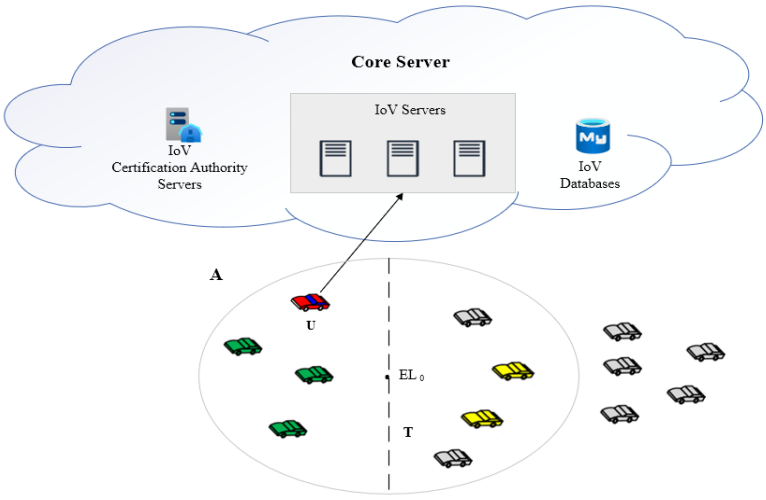


Figure 5. SBM-SA architecture

The generation of a GID can be completed through the above method, and then uploaded to the core server to achieve the goal of separating the connection between vehicles and *ELo* where the SBM occurs, thereby protecting the location privacy of vehicles.

As shown in Algorithm 1, upon collecting SBM data at a location *ELo*, a vehicle waits for a specified time tolerance T before initiating the upload. During this interval, the algorithm tracks all vehicles passing through *ELo*, grouping them into a VehicleSet. If the number of vehicles in this set is less than a desired anonymity degree p, the search expands to a surrounding region A to include more vehicles. Once the set meets the anonymity criteria, a group G is formed, and a GID is generated for it. The SBM data is then uploaded using this GID, ensuring individual vehicle locations remain private. This approach effectively decouples the direct link between a vehicle's exact location and the uploaded data, enhancing location privacy in the IoV context.

Algorithm 1. The pseudo-code of the SBM-SA

Algorithm SBM-SA (SBM data, *ELo*, time tolerance T, anonymity degree p)

Begin

- Wait until time tolerance T before uploading SBM data
- Initialise VehicleSet = vehicles passing through *ELo* within T
- If size of VehicleSet < p then
    - Construct region A centred at *ELo* with radius proportional to T

http://doi.org/10.18080/jtde.v11n4.767

- Add vehicles from region A to VehicleSet until size of VehicleSet = p

End if

- Form group G from VehicleSet ensuring it includes at least p vehicles
- Generate GID for Group G
- Upload SBM data with GID to core server

End algorithm

Data collection for SBM-SA

It is crucial to select the appropriate SBM types that comply with the SBM-SA and utilise them accordingly by filtering out irrelevant ones. Currently, the main sources for obtaining IoV data are open IoV datasets. Two open data sources are considered, namely NGSIM and ApolloScape The NGSIM data set, collected by the US Federal Highway Administration between 2005 and 2010, is a valuable resource for transportation research, including real-world and simulated traffic data from six freeway locations in the United States, with dimensions such as time, location, traffic flow, lane positions, vehicle characteristics and driver behaviour, with a total size of approximately 1.2 terabytes. The ApolloScape dataset was created by Baidu's autonomous driving division, which is a well-known company with map surveying permissions. It includes multiple dimensions for training and testing algorithms for self-driving cars, such as high-definition maps, 3D-point clouds, and camera images. The dataset is currently being maintained and updated by the Apollo team at Baidu. It contains over 100,000 images and high-resolution LiDAR scan data from multiple scenes in multiple cities, and its size depends on the subset used, which may reach several hundred gigabytes or even terabytes.

Selection of simulation platform for the SBM-SA

An IoV simulation environment is a virtual environment used to simulate and evaluate the performance and behaviour of the IoV system. The IoV simulation environment typically encompasses software, hardware and communication networks to mimic diverse IoV application scenarios and traffic situations. The main objectives seek to:

1. Provide simulation scenarios: The IoV simulation environment can provide various traffic scenarios, such as urban traffic, highways, etc., as well as various weather and road conditions to simulate different traffic situations.
2. Simulate vehicle and sensor behaviour: The IoV simulation environment can simulate the behaviour and performance of vehicles and sensors, such as vehicle speed, acceleration, sensor accuracy and response time.

http://doi.org/10.18080/jtde.v11n4.767

3. Evaluate system performance: The IoV simulation environment can simulate the operation and interaction of the IoV system to evaluate its performance and behaviour. For example, it can evaluate communication and collaboration between vehicles and optimise traffic flow and congestion situations.
4. Develop and test IoV applications: The IoV simulation environment can provide an environment for developing and testing IoV applications to verify their functionality and performance.
5. Reduce development and testing costs: The IoV simulation environment can reduce the cost and risk of developing and testing IoV systems and reduce the dependence and impact on the real environment.

Common simulation platforms are presented in Table 2.

Table 2. Summary of privacy methods in SBM generation

Simulation platform	OPNET	CarSim	VIRES VTD
Pros	➢ A relatively complete basic model library is provided ➢ OPNET has a wealth of statistical collection and analysis functions	➢ The simulation results are highly similar to the real vehicle ➢ Co-simulation possible with Simulink	➢ VTD has a rich library of scenes ➢ Synchronously generates OpenDrive high-definition maps
Cons	High cost of learning	Creating a new model takes a long time	Model library is not rich enough
Proposed platform: OPNET is the current mainstream choice, and it has lower requirements on hardware resources, making it more suitable for this research			

OPNET is a commercial network simulation tool that can be used to design, develop and evaluate various networks and systems (Chen *et al.*, 2019). The tool offers a comprehensive range of network models and simulation tools to assess network performance and reliability by emulating different protocols and topologies. To conduct network simulation in OPNET, users need to first define the network topology, nodes and transmission protocols. Users can choose suitable models and components according to their actual needs to build a network system that meets their requirements. OPNET provides users with a variety of tools and analysers that can be used during simulation to assess the performance and reliability of the network system, and to make necessary optimisations. OPNET has rich statistical collection and analysis functions. However, OPNET also has some limitations and challenges, such as a complex configuration and debugging process, which makes the learning curve relatively steep.

http://doi.org/10.18080/jtde.v11n4.767

CarSim is a commercial vehicle simulation software that can simulate various dynamic characteristics and behaviours of vehicles during driving (Wei *et al.*, 2021). CarSim can be used in various application fields, such as vehicle design, control algorithm development, and driver training. CarSim provides multiple vehicle models and control algorithms, which can help users better understand the physical characteristics and behaviour of vehicles during driving. Users can choose suitable models and algorithms according to their actual needs to build a vehicle simulation system that meets their requirements. However, CarSim also has some limitations and challenges, such as the time-consuming process of creating new models, which makes the cost of model creation relatively high.

VIRES VTD (virtual test drive) is a commercial virtual simulation software used for simulating various traffic scenarios and vehicle driving processes (Aoki *et al.*, 2020). It provides a highly customisable virtual environment that helps users better understand the physical characteristics and behaviours of vehicle driving processes. Users can select appropriate vehicle models and control algorithms according to their needs and use various tools and analysers provided by VIRES VTD to evaluate system performance and reliability, and optimise them. VIRES VTD also has some challenges and limitations, such as a relatively small model library, which may limit the range of scenarios that can be tested.

Validation of the SBM-SA

To ensure the accuracy and performance of an SBM-SA, a similar environment must be constructed for validation purposes. Previous studies have suggested several approaches for horizontal comparison, including privacy-preserving schemes based on differential privacy algorithms (Gao *et al.*, 2022; Qian *et al.*, 2021) and geometric range queries (Zhang *et al.*, 2021). These studies can serve as benchmarks for constructing the environment and conducting horizontal comparisons. By using the same environment, the conclusions drawn from these studies can be compared to those of the SBM-SA, thus validating its accuracy and performance.

Application of the SBM-SA

Although the SBM-SA is a privacy protection algorithm specifically designed for the SBM in the IoV, it has broad applications. For example, crowdsourcing and crowdsensing applications in the IoV generate a large amount of SBMs, which is associated with the privacy information of vehicle owners. If this information is not protected, it faces the risk of being misused. Therefore, using the SBM-SA in the IoV is an effective way to protect privacy. The aim of the SBM-SA is to replace vehicle identity with the GID during data upload to separate the

http://doi.org/10.18080/jtde.v11n4.767

association between vehicle identity information and the SBM, thus protecting privacy. Specifically, the steps for designing the SBM-SA in the IoV are as follows:

1. Data collection: First, collecting location and event data of vehicles is essential, such as the location of traffic jams and accident severity, which can be obtained through sensors, in-vehicle radar and other devices.
2. Data preprocessing: Before uploading the SBM, preprocessing work needs to be done, such as removing abnormal data and processing missing values.
3. SBM-SA processing: Through V2I and core server interaction, or through V2V and nearby vehicle interactions, an anonymous vehicle group range is constructed, and key parameters such as anonymity degree p and time tolerance T are obtained. Meanwhile, these core data are passed to the SBM-SA, and the GID is generated through the SBM-SA calculation.
4. Data upload: Use the GID to replace vehicle identity information and upload it with the SBM to the core server for centralised processing.
5. Effect evaluation: Evaluate the data quality and privacy protection effect of SBM-SA processing. Generally, three indicators, anonymity, data availability and data quality, can be used for evaluation.
6. Result application: Apply the SBM-SA processed data to the IoV to protect the privacy information of vehicle owners.

While the SBM-SA effectively decouples the association between vehicle identity and the SBM, it's important to realise that it doesn't offer complete assurance of privacy security and certain risks persist; for example, SBMs still containing sensitive location information. Thus, in real-world applications, further data protection could be accomplished by integrating methods such as differential privacy algorithms. In order to substantiate the efficacy of the SBM-SA in safeguarding the privacy of vehicle owners within the IoV landscape, rigorous testing and validation of the SBM-SA will be conducted and comparative evaluations against other privacy protection algorithms are proposed.

Performance Evaluation

In order to delve deeper into the efficacy and performance of the SBM-SA in terms of privacy protection, this section will undertake rigorous testing and validation of the SBM-SA. We first delineate the details of our simulation environment. Following this, we assess our proposed SBM-SA, contrasting its performance with established privacy protection algorithms such as the PriSC (Zhang *et al.*, 2020a) and the DABAB (Liu *et al.*, 2022). This paper presents a

http://doi.org/10.18080/jtde.v11n4.767

simulation conducted on a PC with an Intel Core i7-7700K @4.0GHz processor and 16GB RAM, leveraging the OPNET simulation software. The simulation creates a vehicle network environment that mirrors a two-way, dual-lane road in accordance with Federal Highway Administration guidelines, with a width of 14.8 metres (four lanes each 3.7 metres wide) and a length of 10 kilometres to replicate a typical 20-minute journey at 30 kilometres per hour. A total of 200 cars are set up to report SBMs, which a designated vehicle collects in three categories: road (S1), accident (S2) and traffic flow (S3), with respective packet sizes of 3,200-bit, 3,400-bit and 3,600-bit. Privacy protection algorithms such as PriSC, DABAB and SBM-SA are implemented during data collection and upload. With a two-second maximum time tolerance for data delay in consideration of user service experience, all three algorithms also maintain a degree of anonymity set at 10. For network communications, the channel spectrum bandwidth is defined at 55 kiloHertz, which affects the data transfer rate and susceptibility to interference. The simulation also employs the Nakagami Channel Model, a flexible tool used to adjust the m parameter, mimicking varying real-world conditions and replicating the fading characteristics of a wireless communication system. Consequently, these parameters (Table 3) significantly shape the simulated network's performance and behaviour.

Table 3. Simulation environment parameter settings

Parameter	Parameter unit	Parameter setting
CPU	X86_64	2 CPU
Storage	TB	1
Road width	metres	3.7 * 4
Road length	km	10
Average vehicle speed	km/h	30
Vehicle transmission power	mW	20
Collected data packet	bit	3,200, 3,400, 3,600
Maximum data transmission rate	Mbps	2
Channel spectrum bandwidth	kHz	55
Channel model	–	Nakagami
Noise power	dBm	-100
Number of cars	–	200

In order to verify the capability of the SBM-SA in protecting the privacy of SBM collection and upload in the IoV, the simulation experiment compares the time delay and privacy leakage probability of PriSC, DABAB, and SBM-SA algorithms in a centralised IoV. Figure 6 shows the time delay of vehicle U collecting different types of SBM through different privacy protection algorithms. When using PriSC and DABAB algorithms to collect the SBM, the data type only causes a minor impact on the delay. However, the PriSC has the largest data delay, approximately 1.6 seconds, while the DABAB performs best at around 0.6 seconds. With the SBM-SA, when the uploaded data is within the permissible time range, different types of SBMs

http://doi.org/10.18080/jtde.v11n4.767

have different time delays. Therefore, in terms of time delay, the SBM-SA does not perform as well as the DABAB.

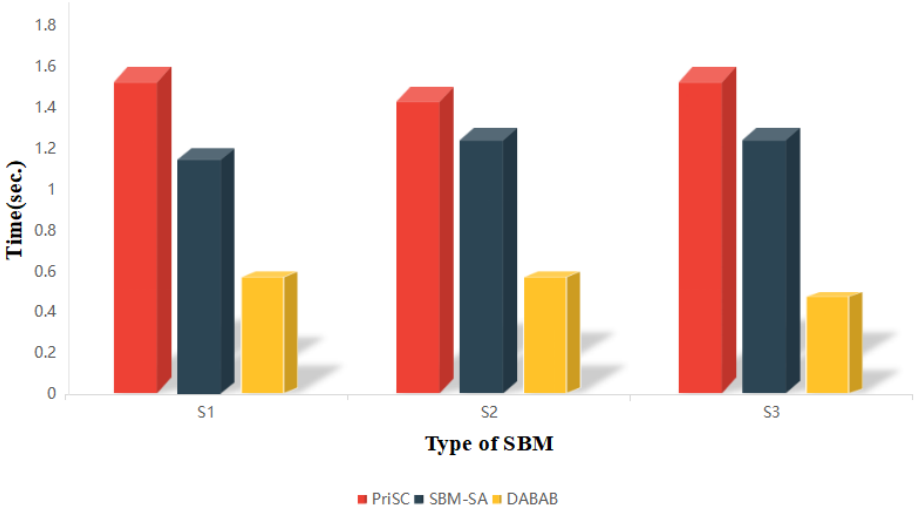


Figure 6. Time delays in the aggregation process of the SBM

The focus of this paper is an experimental exploration of various privacy protection algorithms' efficacy in safeguarding the location privacy of a specific vehicle (U) during its data transmission process. This experimental scenario is set in a context where a core server – functioning as a hypothetical attacker – strives to deduce the location of vehicle U as it uploads data via a message, referred to as Msg (*ELO*), under the effect of different privacy protection algorithms. The core purpose of this investigative setup is to measure how efficiently these diverse algorithms can maintain the vehicle's location privacy throughout the data transfer process. Notably, a successful location guess by the core server equates to a breach of privacy, signifying the respective algorithms' failures in thwarting location exposure. Thus, the experiment provides a comparative evaluation of the tested privacy protection algorithms. Within this experimental setup, certain parameters are accounted for, including the specificities and complexities of the implemented privacy protection algorithms, the volume and variety of data embedded in Msg (*ELO*), and potentially the signal strength or connection conditions during data transmission. While the SBM-SA underperforms the DABAB with regards to time delay, it compensates by delivering superior privacy protection capabilities, albeit at the expense of tolerable time delays, as graphically depicted in Figure 7. With PriSC algorithm, the vehicle U directly uploads the transparent Msg (*ELO*) data to the core server, which then accumulates and processes this data. This direct upload offers the core server a 100% chance of accurately deducing the vehicle's location, implying a complete privacy leak. Conversely, the DABAB, which necessitates an initial data encryption by vehicle U before the upload, decreases the probability of location privacy leakage to between 10% and 20%. Finally, the SBM-SA, being implemented at the user end rather than directly on the core server, poses

http://doi.org/10.18080/jtde.v11n4.767

a greater challenge for the core server in guessing the user's location, consequently reducing the likelihood of privacy leakage for vehicle U to under 10%. Hence, in terms of effective location privacy protection, this paper identifies the SBM-SA as being the most potent algorithm among those tested.

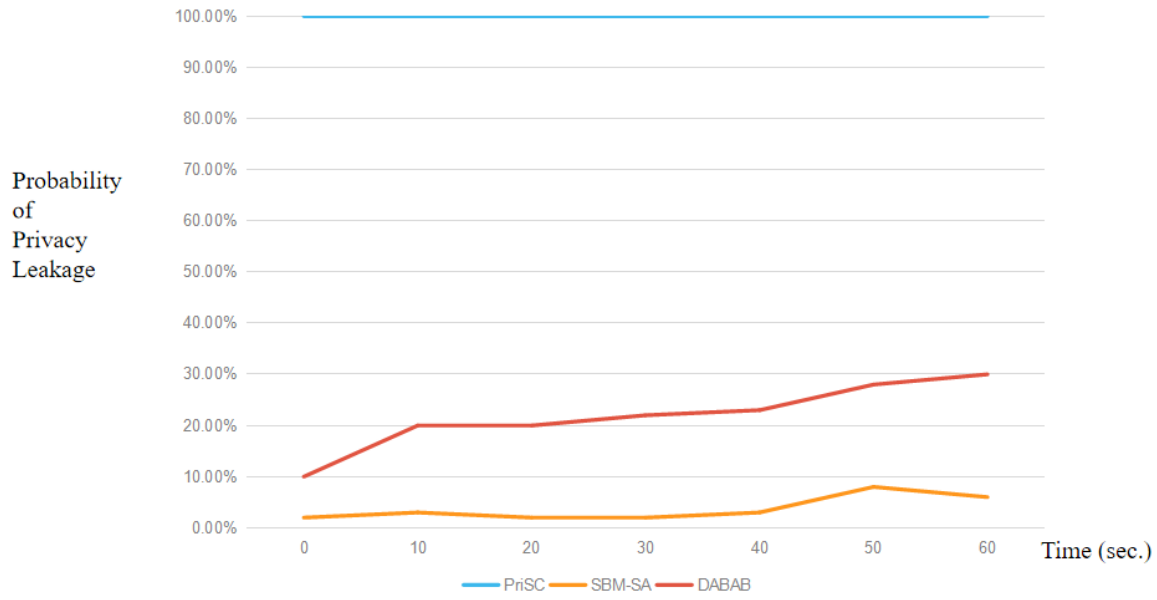


Figure 7. Probability of privacy leakage using different privacy-preserving algorithms during SBM collection

In conclusion, when a series of comparisons are conducted with the PriSC and DABAB algorithms in terms of time and privacy leakage probability, experimental results show that the SBM-SA can effectively protect user location privacy in the IoV.

Conclusion

In the domain of IoV privacy, the SBM-SA has been meticulously evaluated against established algorithms like the PriSC and DABAB. The simulation results derived from the real-vehicle environment simulated by the simulation environment, offer insights into the performance nuances of these algorithms.

The PriSC's architecture is streamlined for swift data transmission, achieved through its direct data upload feature to the core server. However, this expediency compromises privacy, as no encryption or intermediary processing occurs. The DABAB, in contrast, adopts an encryption-first approach. While this ensures data security, the inherent computational demands of encryption introduce latency, evident in the 10% to 20% location privacy leakage. The PriSC's pronounced data delay can be traced back to its simplistic data structure. The absence of protective layers, combined with its direct upload mechanism, renders it vulnerable to location deductions, resulting in a 100% leakage probability. The DABAB, with its layered and

http://doi.org/10.18080/jtde.v11n4.767

encryption-centric design, offers better privacy but at the cost of increased processing time. The encryption process, while bolstering security, adds to the data handling time. The SBM-SA is distinguished by its decentralised data processing, introducing user-end anonymisation. This design choice effectively challenges the core server's location prediction capabilities, reducing privacy leak probabilities to below 10%. The inclusion of the Nakagami Channel Model, simulating real-world wireless communication challenges, further refines the simulation's accuracy. The chosen parameters, especially the 55-kiloHertz channel spectrum bandwidth, play a pivotal role in determining network behaviour. Beyond the surface-level data, the intrinsic design, data structures and processing strategies of these algorithms truly define their efficacy and challenges in IoV privacy.

Discussion

In the realm of IoV privacy protection, the Performance Evaluation section's insights into the SBM-SA's capabilities, especially when juxtaposed with algorithms like the PriSC and DABAB, are enlightening. Grounded in foundational empirical studies, such as those by Zhang *et al.* (2020a) and Liu *et al.* (2022), this research elucidates the nuances and potential of anonymisation of privacy algorithms. The consistent emphasis by prior research on safeguarding user data in today's data-centric era is a testament to the burgeoning interest in this domain. The methodologies adopted in these seminal studies, especially differential privacy, have significantly influenced the trajectory of the SBM-SA. The congruence with prior research not only validates this study's outcomes but also highlights the cumulative wisdom that has shaped this domain. Beyond the immediate results, the broader ramifications beckon attention. The efficacy of the SBM-SA raises pertinent questions about both the IoV's future and ways to amplify privacy protection. While the SBM-SA's success heralds a promising future, inherent limitations delineate ripe scenarios for future exploration and refinement.

Acknowledgements

A version of this paper was presented at the third International Conference on Computer, Information Technology and Intelligent Computing, CITIC 2023, held in Malaysia on 26-28 July 2023.

References

Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. *ACM Computing Surveys (CSUR), 51*(4), 1–35. https://doi.org/10.1145/3214303

Ali Sarker, M. R., Hassanuzzaman, M., Biswas, P., Dadon, S. H., Imam, T., & Rahman, T. (2021). An efficient surface map creation and tracking using smartphone sensors and crowdsourcing. *Sensors*, *21*(21), 6969. https://doi.org/10.3390/s21216969

Aoki, S., Jan, L. E., Zhao, J., Bhat, A., Rajkumar, R. R., & Chang, C. F. (2020, October). Co-simulation platform for developing inforich energy-efficient connected and automated vehicles. In *2020 IEEE Intelligent Vehicles Symposium (IV)*, 1522–1529. IEEE. https://doi.org/10.1109/IV47402.2020.9304664

Babaghayou, M., Chaib, N., Lagraa, N., Ferrag, M. A., & Maglaras, L. (2023). A safety-aware location privacy-preserving IoV scheme with road congestion-estimation in mobile edge computing. *Sensors*, *23*(1), 531. https://doi.org/10.3390/s23010531

Babaghayou, M., Labraoui, N., Ari, A. A. A., Lagraa, N., & Ferrag, M. A. (2020). Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: A survey. *Journal of Information Security and Applications*, *55*, 102618. https://doi.org/10.1016/j.jisa.2020.102618

Benarous, L., & Kadri, B. (2022). Obfuscation-based location privacy-preserving scheme in cloud-enabled internet of vehicles. *Peer-to-Peer Networking and Applications*, *15*(1), 461–472. https://doi.org/10.1007/s12083-021-01233-z

Capponi, A., Fiandrino, C., Kantarci, B., Foschini, L., Kliazovich, D., & Bouvry, P. (2019). A survey on mobile crowdsensing systems: Challenges, solutions, and opportunities. *IEEE Communications Surveys & Tutorials*, *21*(3), 2419–2465. https://doi.org/10.1109/COMST.2019.2914030

Chen, M., Miao, Y., Humar, I., Chen, M., Miao, Y., & Humar, I. (2019). Introduction to OPNET network simulation. *OPNET IoT Simulation*, 77–153. https://doi.org/10.1007/978-981-32-9170-6_2

El Khatib, R. F., Zorba, N., & Hassanein, H. S. (2019, December). Crowdsensing-based prompt emergency discovery: A sequential detection approach. In 2019 *IEEE Global Communications Conference (GLOBECOM)*, 1–6. IEEE. https://doi.org/10.1109/GLOBECOM38437.2019.9013852

Gao, Z., Huang, Y., Zheng, L., Lu, H., Wu, B., & Zhang, J. (2022). Protecting location privacy of users based on trajectory obfuscation in mobile crowdsensing. *IEEE Transactions on Industrial Informatics*, *18*(9), 6290–6299. https://doi.org/10.1109/TII.2022.3146281

Garg, T., Kagalwalla, N., Churi, P., Pawar, A., & Deshmukh, S. (2020). A survey on security and privacy issues in IoV. *International Journal of Electrical & Computer Engineering, 10(5)*. http://doi.org/10.11591/ijece.v10i5.pp5409-5419

Hou, L., Yao, N., Lu, Z., Zhan, F., & Liu, Z. (2021). Tracking based mix-zone location privacy evaluation in VANET. *IEEE Transactions on Vehicular Technology*, *70*(10), 10957–10969. https://doi.org/10.1109/TVT.2021.3109065

Hou, P., Li, B., Wang, Z., & Ding, H. (2022). Joint hierarchical placement and configuration of edge servers in C-V2X. *Ad Hoc Networks*, *131*, 102842. https://doi.org/10.1016/j.adhoc.2022.102842

Huang, Z., Liu, S., Mao, X., Chen, K., & Li, J. (2017). Insight of the protection for data security under selective opening attacks. *Information Sciences*, *412*, 223–241. https://doi.org/10.1016/j.ins.2017.05.031

Jegadeesan, S., Obaidat, M. S., Vijayakumar, P., & Azees, M. (2021). SEAT: secure and energy efficient anonymous authentication with trajectory privacy-preserving scheme for marine traffic management. *IEEE Transactions on Green Communications and Networking, 6*(2), 815–824. https://doi.org/10.1109/TGCN.2021.3126618

Jeong, H. H., Shen, Y. C., Jeong, J. P., & Oh, T. T. (2021). A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications. *Vehicular Communications*, *31*, 100349. https://doi.org/10.1016/j.vehcom.2021.100349

Kanumalli, S. S., Ch, A., & Murty, P. S. R. C. (2020). Secure V2V Communication in IOV using IBE and PKI based Hybrid Approach. *International Journal of Advanced Computer Science and Applications*, *11*(1). https://doi.org/10.14569/ijacsa.2020.0110157

Kietzmann, J. H. (2017). Crowdsourcing: A revised definition and introduction to new research. *Business horizons, 60(2), 151–153*. https://doi.org/10.1016/j.bushor.2016.10.001

Kim, J. W., Edemacu, K., & Jang, B. (2022). Privacy-preserving mechanisms for location privacy in mobile crowdsensing: A survey. *Journal of Network and Computer Applications, 200*, 103315. https://doi.org/10.1016/j.jnca.2021.103315

Li, H., Pei, L., Liao, D., Zhang, M., Xu, D., & Wang, X. (2020). Achieving privacy protection for crowdsourcing application in edge-assistant vehicular networking. *Telecommunication Systems*, *75*, 1–14. https://doi.org/10.1007/s11235-020-00666-w

Li, H., Liao, D., Sun, G., Zhang, M., Xu, D., & Han, Z. (2018a). Two-stage privacy-preserving mechanism for a crowdsensing-based VSN. *IEEE Access*, *6*, 40682–40695. https://doi.org/10.1109/ACCESS.2018.2854236

Li, J., Sun, L., Yan, Q., Li, Z., Srisa-An, W., & Ye, H. (2018b). Significant permission identification for machine-learning-based android malware detection. *IEEE Transactions on Industrial Informatics*, *14*(7), 3216–3225. https://doi.org/10.1109/TII.2017.2789219

Lin, Y., Wang, P., & Ma, M. (2017, May). Intelligent transportation system (ITS): Concept, challenge and opportunity. In 2017 IEEE 3rd international conference on big data security on cloud (bigdatasecurity), IEEE international conference on high performance and smart computing (HPSC), and IEEE international conference on intelligent data and security (IDS), (pp. 167-172). IEEE. https://doi.org/10.1109/BigDataSecurity.2017.50

Lin, H., Garg, S., Hu, J., Kaddoum, G., Peng, M., & Hossain, M. S. (2020). Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *22*(6), 3755–3764. https://doi.org/10.1109/TITS.2020.3025247

Liu, Y., Wang, H., Peng, M., Guan, J., & Wang, Y. (2020). An incentive mechanism for privacy-preserving crowdsensing via deep reinforcement learning. *IEEE Internet of Things Journal*, *8*(10), 8616–8631. https://doi.org/10.1109/JIOT.2020.3047105

Liu, J., Peng, C., Sun, R., Liu, L., Zhang, N., Dustdar, S., & Leung, V. C. (2023). CPAHP: Conditional privacy-preserving authentication scheme with hierarchical pseudonym for 5G-enabled IoV. *IEEE Transactions on Vehicular Technology*, *72*(7), 8929–8940. https://doi.org/10.1109/TVT.2023.3246466

Liu, K., Li, H., Chen, X., Liao, D., Peng, L., & Yurui, L. (2022, October). A privacy protection solution based on data aggregation and batch authentication. In Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, 85–90. https://doi.org/10.1145/3555661.3560869

Liu, T., Zhu, Y., Yang, Y., & Ye, F. (2016, December). Incentive design for air pollution monitoring based on compressive crowdsensing. In 2016 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE. https://doi.org/10.1109/GLOCOM.2016.7841892

Mei, Q., Gül, M., & Shirzad-Ghaleroudkhani, N. (2020). Towards smart cities: Crowdsensing-based monitoring of transportation infrastructure using in-traffic vehicles. *Journal of Civil Structural Health Monitoring*, *10*(4), 653–665. https://doi.org/10.1007/s13349-020-00411-6

Memon, I., Chen, L., Arain, Q. A., Memon, H., & Chen, G. (2018). Pseudonym changing strategy with multiple mix zones for trajectory privacy protection in road networks. *International Journal of Communication Systems*, *31*(1), e3437. https://doi.org/10.1002/dac.3437

Metlo, S., Memon, M. G., Shaikh, F. K., Teevno, M. A., & Talpur, A. (2019). Crowdsource based vehicle tracking system. *Wireless Personal Communications*, *106*(4), 2387–2405. https://doi.org/10.1007/s11277-019-06323-z

Misra, A., Gooze, A., Watkins, K., Asad, M., & Le Dantec, C. A. (2014). Crowdsourcing and its application to transportation data collection and management. *Transportation Research Record*, *2414*(1), 1–8. https://doi.org/10.3141/2414-01

Nandy, T., Idris, M. Y. I., Noor, R. M., Wahab, A. W. A., Bhattacharyya, S., Kolandaisamy, R., & Yahuza, M. (2021). A secure, privacy-preserving, and lightweight Authentication scheme for VANETs. *IEEE Sensors Journal*, *21*(18), 20998–21011. https://doi.org/10.1109/JSEN.2021.3097172

Qian, Y., Ma, Y., Chen, J., Wu, D., Tian, D., & Hwang, K. (2021). Optimal location privacy preserving and service quality guaranteed task allocation in vehicle-based crowdsensing networks. *IEEE Transactions on Intelligent Transportation Systems, 22*(7), 4367–4375. https://doi.org/10.1109/TITS.2021.3086837

Qureshi, K., & Abdullah, H. (2013). A survey on intelligent transportation systems. *Middle East Journal of Scientific Research*, *15*, 629–642. https://doi.org/10.5829/idosi.mejsr.2013.15.5.11215

Sadiah, S., & Nakanishi, T. (2022). An efficient anonymous reputation system for crowdsensing. *Journal of Information Processing*, *30*, 694–705. https://doi.org/10.2197/ipsjjip.30.694

Song, L., Sun, G., Yu, H., Du, X., & Guizani, M. (2020). Fbia: A fog-based identity authentication scheme for privacy preservation in internet of vehicles. *IEEE*

Transactions on Vehicular Technology, *69*(5), 5403–5415. https://doi.org/10.1109/TVT.2020.2977829

Wang, T., Xu, L., Zhang, M., Zhang, H., & Zhang, G. (2022). A new privacy protection approach based on k-anonymity for location-based cloud services. *Journal of Circuits, Systems and Computers*, *31*(05), 2250083. https://doi.org/10.1142/S0218126622500839

Wang, D., Huang, C., Shen, X., & Xiong, N. (2020). A general location-authentication based secure participant recruitment scheme for vehicular crowdsensing. *Computer Networks*, *171*, 107152. https://doi.org/10.1016/j.comnet.2020.107152

Wang, X., Zhang, J., Tian, X., Gan, X., Guan, Y., & Wang, X. (2017). Crowdsensing-based consensus incident report for road traffic acquisition. *IEEE Transactions on Intelligent Transportation Systems*, *19*(8), 2536–2547. https://doi.org/10.1109/TITS.2017.2750169

Wei, H., Wang, J., Jian, M., Mei, S., & Huang, M. (2021, April). Steer-by-Wire Control System Based on Carsim and Simulink. In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 1–5. IEEE. https://doi.org/10.1109/IEMTRONICS52119.2021.9422502

Wu, Z., Wang, R., Li, Q., Lian, X., Xu, G., Chen, E., & Liu, X. (2020). A location privacy-preserving system based on query range cover-up or location-based services. *IEEE Transactions on Vehicular Technology*, *69*(5), 5244–5254. https://doi.org/10.1109/TVT.2020.2981633

Xiong, J., Ma, R., Chen, L., Tian, Y., Li, Q., Liu, X., & Yao, Z. (2019). A personalized privacy protection framework for mobile crowdsensing in IIoT. *IEEE Transactions on Industrial Informatics*, *16*(6), 4231–4241. https://doi.org/10.1109/TII.2019.2948068

Yang, X., Tang, L., Niu, L., Zhang, X., & Li, Q. (2018). Generating lane-based intersection maps from crowdsourcing big trace data. *Transportation Research Part C: Emerging Technologies, 89*, 168–187. https://doi.org/10.1016/j.trc.2018.02.007

Ye, X., Zhu, Y., Zhang, M., & Deng, H. (2023). Differential privacy data release scheme using micro-aggregation with conditional feature selection. *IEEE Internet of Things Journal, 10*(20), 18302–18314. https://doi.org/10.1109/JIOT.2023.3279440

Zappatore, M., Loglisci, C., Longo, A., Bochicchio, M. A., Vaira, L., & Malerba, D. (2019). Trustworthiness of context-aware urban pollution data in mobile crowd sensing. *IEEE Access*, *7*, 154141–154156. https://doi.org/10.1109/ACCESS.2019.2948757

Zhang, J., Yang, F., Ma, Z., Wang, Z., Liu, X., & Ma, J. (2020a). A decentralized location privacy-preserving spatial crowdsourcing for internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, *22*(4), 2299–2313. https://doi.org/10.1109/TITS.2020.3010288

Zhang, C., Zhu, L., Ni, J., Huang, C., & Shen, X. (2020b). Verifiable and privacy-preserving traffic flow statistics for advanced traffic management systems. *IEEE Transactions on Vehicular Technology, 69(9), 10336–10347.* https://doi.org/10.1109/TVT.2020.3005363

Zhang, C., Zhu, L., Xu, C., Ni, J., Huang, C., & Shen, X. (2021). Location privacy-preserving task recommendation with geometric range query in mobile crowdsensing. *IEEE*

Transactions on Mobile Computing, 21(12), 4410–4425. https://doi.org/10.1109/TMC.2021.3080714

Zhang, G., Hou, F., Gao, L., Yang, G., & Cai, L. X. (2022). Nondeterministic-mobility-based incentive mechanism for efficient data collection in crowdsensing. *IEEE Internet of Things Journal*, *9*(23), 23626–23638. https://doi.org/10.1109/JIOT.2022.3190565

Secure Data Sharing in a Cyber-Physical Cloud Environment

Jun-Wen Chan
Multimedia University, Malaysia

Swee-Huay Heng
Multimedia University, Malaysia

Syh-Yuan Tan
Multimedia University, Malaysia

Abstract: Cloud computing plays a significant role in digital workplaces and has become an integral part of everyday life. However, the security issues associated with cloud computing remain a major concern that hinders the wider adoption of this technology. In a cyber-physical cloud environment, achieving secure and efficient file storage remains a tough goal. This is particularly the case owing to the wide variety of devices that are being utilised to access the various services and data. Thus, the employment of a secure data sharing protocol is one of the essential techniques to better protect the shared data. A formal agreement between entities or organisations in exchanging personal or business data is called a data sharing protocol. A secure data sharing protocol ensures that data is encrypted and secured when being transferred. There are many different encryption algorithms and protocols in use to devise various secure and efficient data sharing protocols. This paper first reviews the state of the art of some existing data sharing protocols and subsequently implements a secure and efficient data sharing protocol as an application in a cyber-physical cloud environment. The performance analysis conducted on the developed secure data sharing protocol application shows positive results.

Keywords: cloud computing, data sharing protocol, cyber-physical environment

Introduction

The term 'cyber-physical cloud systems' (CPCS) refers to a technology that has a wide range of applications, some of which include healthcare, smart electricity grids, smart cities, battlegrounds, and the military. Client devices such as those running on Android or iOS, or devices with restricted resource availability such as sensors, are being deployed in these types of systems to gain access to services (Deng *et al.*, 2014). In the context of industry, CPCS is

http://doi.org/10.18080/jtde.v11n4.772

used for collecting, processing, analysing and interpreting large data. The utilisation of Internet of Things technologies in conjunction with real-time analysis of vast amounts of data allows for large-scale monitoring opportunities, thanks to the prevalence of multifaceted devices. This generates novel insights that can enhance decision-making processes and provide an advantageous edge in business (Cheng *et al.*, 2018). However, compared to typical personal computers, client devices sometimes have much less processing capabilities. Recent years have witnessed a rapid and vast adoption of mobile cloud computing as compared to the conventional cloud computing since smart mobile devices such as Android and iOS smartphones have become more prevalent (Salvi, 2019).

Nevertheless, there are still significant concerns regarding security issues such as reliability and privacy in physical devices and in untrusted cloud environments, despite the widespread acceptance of cloud computing in its varied forms. Safe and reliable information exchange between users of a hybrid cloud (cyber and physical) is fortunately made possible through a cryptographic approach known as data sharing protocol (Salvi, 2019). However, a protocol is developed with complex algorithms and, as mobile devices' processors are not very powerful, this will take up a lot of computation time. Therefore, lightweight operation is essential for efficiency and faster computation in mobile devices.

This research reviews the existing data sharing protocols in a cyber-physical cloud environment. Leveraging the strengths of the state-of-the-art protocol, the application will be developed by incorporating the chosen data sharing protocol. The application ensures heightened security and efficiency and promises fast computation times in a cyber-physical cloud environment. The performance analysis attests that the data sharing protocol facilitates a rapid and reliable approach. Thus, this research paves the way for future development in secure and efficient data sharing solutions.

Table 1 contains the list of abbreviations used throughout our discussion.

Table 1. List of abbreviations

LIST OF ABBREVIATIONS/SYMBOLS	
AES	Advanced encryption standard
CC	Cloud controller
CS	Cloud server
DC	Data consumer
DCs	Data consumers
dDHPEKS	Designated-tester decryptable hierarchical public key encryption with keyword search
DH	Data holder
DO	Data owner
DS	Data sharer
HPEKS	Hierarchical public key encryption with keyword search
IBADS	Identity-based authenticated data sharing

http://doi.org/10.18080/jtde.v11n4.772

LIST OF ABBREVIATIONS/SYMBOLS	
IBE	Identity-based encryption
KB	Kilobyte
MC_c	Client
OO-ABPRE	Online/offline attribute-based proxy re-encryption
PEKS	Public key encryption with keyword search
PKG	Private key generator
PKTree	Public key tree
S_{CC}	ID of cloud controller
SSGK	Secret sharing group key management

Current Data Sharing Protocols

Shao *et al.* (2015) proposed a fine-grained data sharing protocol employed in cloud computing through utilising the transformed key approach and online/offline attribute-based proxy re-encryption (OO-ABPRE). The proposed approach protects user data by allowing fine-grained access control, convenient sharing and is also cost-effective. The protocol uses a proxy that is only partially trusted and is equipped with a re-encryption key. As a result, the proxy is able to transform a plaintext that was originally encrypted with one public key into a plaintext that was encrypted with another public key. In other words, this enables encryption to be performed by using the public key of the data holder (DH) or someone else. When the DH decides to engage in sharing the data, all he has to do is produce the relevant re-encryption key. The cloud server (CS) will then be able to use this re-encryption key to transform the ciphertext into a form that the data sharer (DS) will be able to decrypt by using his corresponding private key.

In order to safeguard the information kept in cloud environments, an identity-based authenticated data sharing (IBADS) protocol was designed by Karati *et al.* (2018). This protocol ensures user anonymity which enables the identities of the client and user to be concealed from the attackers, even in the event that they intercepted the public channel over which the message was transmitted. This end-to-end connection will be encrypted using a technique that relies on a small public parameter and bilinear pairing once the authentication of physical devices has been completed. The protocol is distinguished by its deployment of identity-based encryption (IBE) to facilitate the safe exchange of data between the clients and the clients' geographically scattered physical devices.

Han *et al.* (2019) proposed a secret sharing group key management protocol (SSGK) for resolving the issue of increasing security and privacy risks in cloud storage. It employs symmetric encryption algorithms to encrypt the shared data, ensuring its usability by authorised users. The data owner (DO) distributes decryption keys to authorised sharers. Decryption keys control permissions for accessing shared data. Only legitimate participants

http://doi.org/10.18080/jtde.v11n4.772

can decrypt the key associated with the interactive message due to asymmetric encryption algorithms. If unauthorised users obtain access to shared data, a secret sharing scheme assigns the key to legitimate participants.

Lu *et al.* (2020) proposed a data sharing scheme to ensure sensitive data will be shared in a secure and authorised manner. To avoid inaccurate computations, this protocol provides an efficient full validation before users share the data. Using this protocol, sensitive data can be protected during the sharing procedure and authorisation for access can be controlled by the data requester.

Li *et al.* (2022) proposed a protocol for enterprise users that supports hierarchical keyword searching to facilitate secure data sharing in a cloud environment. There are two types of public key encryption with keyword search (PEKS) employed in the protocol, namely, hierarchical public key encryption with keyword search (HPEKS) and designated-tester decryptable hierarchical public key encryption with keyword search (dDHPEKS) which is more advanced than HPEKS. This protocol addresses the challenges of secure data sharing in an enterprise environment. In this protocol, advocated encrypted data should be hierarchically accessible and searchable. To manage the hierarchical structure of users in an enterprise, public key tree (PKTree) was developed. The PKTree algorithm pairs elements from two cryptographic groups to construct complex cryptographic protocols. Users can find the ciphertext encrypted with their public key using HPEKS. Users with lower access permissions can search for ciphertexts sent to a hierarchical group of users. Using this feature in an enterprise setting is particularly beneficial in cases where higher-level employees are required to monitor the data of lower-level employees. dDHPEKS combines symmetric and public key encryption in an advanced version of HPEKS. In addition to preventing outside and offline keyword-guessing attacks, it provides keyword search and decryption functionality. Sharing encrypted data with others does not require knowledge of the enterprise's internal hierarchy due to transparency in the scheme (Li *et al.*, 2022).

Comparison analysis among data sharing protocols

In general, the primary goals of employing the respective data sharing protocols (Shao *et al.*, 2015; Karati *et al.*, 2018; Han *et al.*, 2019; Lu *et al.*, 2020; Li *et al.*, 2022) are to ensure data is encrypted and securely shared, especially in an untrusted cloud environment. Table 2 presents a comparison analysis of the reviewed data sharing protocols.

http://doi.org/10.18080/jtde.v11n4.772

Table 2. Comparison analysis among data sharing protocols

Characteristic	Protocol				
	Shao *et al.* (2015)	Karati *et al.* (2018)	Han *et al.* (2019)	Lu *et al.* (2020)	Li *et al.* (2022)
Underlying cryptographic scheme(s)	Linear secret sharing and access policy schemes Hash function OO-ABPRE	One-way hash function IBE	Symmetric and asymmetric encryption Secret sharing scheme	Linear secret sharing schemes XOR-homomorphic function Algebraic signature	Public key encryption with keyword search
Encryption and decryption method	CS uses the re-encryption key from DH to re-encrypt data and uses DS's transform key to return the transformed ciphertext; DS decrypts using the private key	Encrypt using the public ID as public key; decrypt using the private key of the corresponding ID	Data shared is encrypted with symmetric encryption Asymmetric encryption is used to encrypt the interactive message	Encrypt data using private key generated by the DO; decrypt using private key requested from key generator centre	Encrypted with public key and allows keyword search without decryption
Advantage	Policy access could be inserted to ciphertext Only users with attribute sets that conform to the access policy can decrypt	Provide secure end-to-end communication Designed to be lightweight and has good performance runtime execution	Control permission for shared data Ensure that the key required for decrypting the shared data is not visible to unauthorised users	Authorised data requester can correctly recover the shared data	Sharing encrypted data with an enterprise does not require the sender to know the enterprise's internal hierarchy
Disadvantage	When generating the re-encryption key, DH's device needs to be charged	Complex protocol	Not obvious	Costing is more expensive using cloud storage server and cloud-managed server	dDHPEKS scheme is slower than HPEKS scheme

System Design of Data Sharing Protocol Application

Based on the review and comparison analysis among some existing data sharing protocols as summarised above, the IBADS protocol (Karati *et al.*, 2018) is chosen for implementation because it is a lightweight protocol, meaning it can perform lightweight encryption on a mobile device. The user's mobile device does not spend much time performing encryption, thus speeding up this process. The context diagram depicted in Figure 1 shows the overview of the entity structure of our proposed secure data sharing protocol application. According to the diagram, the external entities are identified as DO, data consumer (DC), cloud controller (CC) and private key generator (PKG). They interact following the processes with the data flow. The DO encrypts and uploads the file to the cloud via the system. The DC could receive the encrypted file and decrypt it while receiving the private key sent from the PKG.

http://doi.org/10.18080/jtde.v11n4.772

Figure 2 shows the use case diagram. Both DO and DC need to register an account with their phone numbers and emails. After that, they need to do mutual authentication with the CC to verify the authenticity of each other. Once mutual authentication has been completed, the DO needs to encrypt the file with the parameters and then upload the file to the cloud. The DC can search files uploaded by the DO by searching the relevant keyword in the system. Following that, the DC can request to download a file from the CC and the CC sends the encrypted file to the DC. Upon receiving the encrypted file, the DC requests the private key from the PKG in order to decrypt the encrypted file. The private key is then used to decrypt the file by the DC.

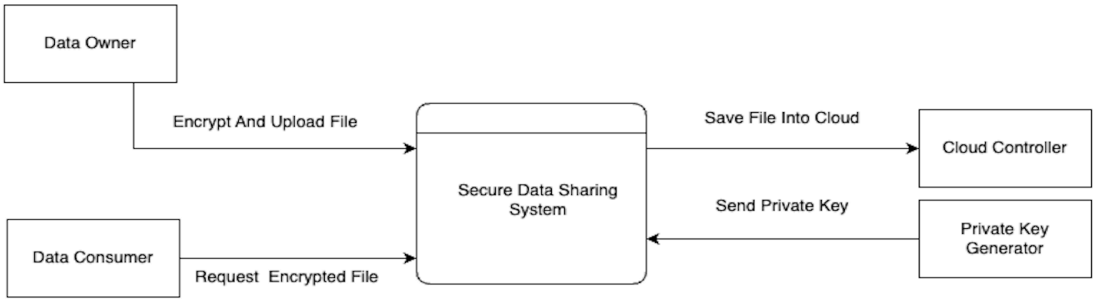


Figure 1. Context diagram

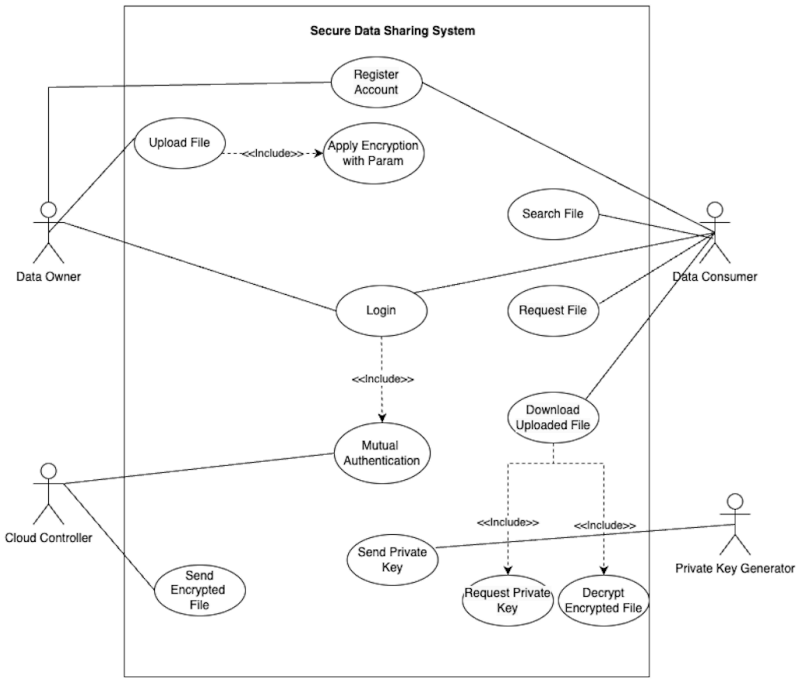


Figure 2. Use case diagram

Implementation of Data Sharing Protocol Application

According to Karati *et al.* (2018), the IBADS protocol uses an IBE scheme and symmetric encryption to perform secure data sharing which provides mutual authentication in order for the CC and user to verify each other's authenticity. The IBE scheme in IBADS protocol uses

http://doi.org/10.18080/jtde.v11n4.772

the device number and mobile number of the DC as the public key to perform encryption. This makes it unnecessary for the DO to ask for the public key from the DC when encrypting files to be sent, thus shortening the time and process of encryption.

Mutual authentication algorithm

Mutual authentication is a technique that discovers if cloud users (DOs and DCs) are valid (non-revoked registered users). It therefore runs through the phases below: registration of client, login and mutual authentication, and password renewal (Karati *et al.*, 2018).

- **Registration of client:** The client MC_c decides a unique identity ID_c and returns it with the identity of email and mobile number to the CC. Knowing that the ID_c parameter is securely sent to the CC, and after the information is received, the CC executes these steps:
  - Creates an app by storing $A_c = h(ID_c \| S_{CC}) \oplus h(ID_c \| PW_c)$, where S_{CC} is the secret key of CC and PW_c is the password of MC_c.
  - Sends the URL link is securely to the email of the MC_c and (PW_c, W_c) to the MC_c mobile number, where W_c is the information generated randomly.
  - Updates the user list LU and stores W_c as the public and unique information of client's email TID_c.

  After receiving the URL link, the MC_c installs software to the mobile device. After the installation is done, the MC_c runs the software and gives ID_c, PW_c and W_c. An array of groups with the group identity G_{ID_j} is received by the mobile device as it is connected to the internet. Now, the MC_c chooses the group fulfilling its requirement and demands as V. The data W_c can only be given once. After that, MC_c runs the below operations:

  - Extracts $B_c = A_c \oplus h(ID_c \| PW_c)$ and new password is asked to be inputted to the MC_c.
  - After receiving the new password PW_c^{new}, it computes

    $$A_c^{new} = B_c \oplus h(ID_c \| PW_c^{new}), D_c = h(ID_c \oplus PW_c^{new})$$

    and $E_c = W_c \oplus h(PW_c^{new})$.
  - Stores $\langle A_c^{new}, D_c, E_c, TID_c \rangle$ and drops A_c.
- **Login and mutual authentication:** This phase is imperative during CC login and the purpose is to execute key agreement and mutual authentication. The phase is defined as follows.

  The MC_cexecutes the software and generates ID_c and PW_c^{new}, after which the software runs the following operations:

  - Calculates $D_c^* = h(ID_c \oplus PW_{new})$ and checks whether $\left(D_c^* \stackrel{?}{=} D_c\right)$ is true.

http://doi.org/10.18080/jtde.v11n4.772

- If $(D_c^* \neq D_c)$, then the session is aborted.
- Otherwise,
  - Random number R_c is generated.
  - Calculates

    $$B_c = A_c^{new} \oplus h(ID_c \parallel PW_c^{new}), W_c = E_c \oplus h(PW_c^{new}), F_c = h(ID_c \| B_c \| R_c)$$

    and then encrypts ID_c and R_c using W_c as the secret key to generate $G_c = E_{W_c(ID_c \| R_c)}$.
  - Forwards through secure channel $\langle TID_c, G_c, F_c \rangle$ to the CC.

After receiving $\langle TID_c, G_c, F_c \rangle$, parameter TID_c is then searched by the CC first in the database and if it returns as false, the session aborts immediately, otherwise it will extract W_c. The CC then runs following operations:

- Decrypts G_c to get ID_c and R_c.
- Calculates

  $$B_c^* = h(ID_c \parallel S_{CC}), F_c^* = h(ID_c \| B_c^* \| R_c)$$

  and determines if $\left(F_c^* \stackrel{?}{=} F_c\right)$ is true.
- If $(F_c^* \neq F_c)$, then the MC_c is denied access.
- Otherwise,
  - A random number R_{cs} is generated.
  - Computes the session key

    $$SK_{cs} = h(ID_c \parallel R_{cs} \parallel R_c), K_c = h(ID_c \| SK_{cs} \| R_{cs}), R_{ccs} = R_c \oplus R_{cs}.$$
  - Forwards $\langle K_c, R_{ccs} \rangle$ to the MC_c.

On receiving $\langle K_c, R_{ccs} \rangle$, the MC_c performs the following operations:

- Extorts $R_{cs}^* = R_{ccs} \oplus R_c$.
- Computes

  $$SK_c^* = h(ID_c \| R_{cs}^* \| R_c), K_c^* = h(ID_c \parallel SK_c^* \parallel R_{cs}).$$
- If $\left(K_c^* \stackrel{?}{=} K_c\right)$ is true, then
  - The protocol achieves mutual authentication as the CC is authenticated and session key is verified.

- **Password renewal:** This is for valid users to renew their password. Firstly, the MC_c runs the installed software and generates ID_c and PW_c^{new}. Following this, the software executes the following tasks:
  - Calculates $D_c^* = h(ID_c \oplus PW_{new})$.

http://doi.org/10.18080/jtde.v11n4.772

- Determines if $\left(D_c^* \stackrel{?}{=} D_c\right)$ if true. If $(D_c^* = D_c)$, it then aborts.
- Otherwise,
  - A new password to the $MC_c$is requested.
  - After receiving a new password PW_c^* , it calculates

$$B_c = A_c \oplus h\left(ID_c \parallel PW_c^{new}\right), A_c^* = B_c \oplus h(ID_c \parallel PW_c^*),\ D_c *= h(ID_c \oplus PW_c^*)$$

and

$$E_c *= W_c \oplus h(PW_c^*).$$

Finally, it records the information $\langle A_c^*, D_c^*, E_c^* \rangle$, and deletes $\langle A_c^{new}, D_c, E_c \rangle$ from the mobile device saved by the MC_c.

IBE scheme

This IBE scheme consists of four algorithms: *IBE.Setup*, *IBE.Extract*, *IBE.Encrypt* and *IBE.Decrypt* (Karati *et al.*, 2018). *IBE.Setup* is an algorithm for generating the parameters that need to be used in the three other IBE algorithms for calculation purposes; *IBE.Extract* is an algorithm which generates the private key for decrypting the message, and *IBE.Encrypt* and *IBE.Decrypt* are the algorithms used to encrypt and decrypt messages, respectively.

- **IBE.Setup (1^k):** The PKG executes the protocol by inputting a security parameter 1^k. After that, it creates a prime p and a bilinear map, e: $G_1 \times G_1 \rightarrow G_2$ of two multiplicative groups $G_1$and G_2. Then, it picks a generator $g \in_R G_1$ randomly and executes $h = \left(g^{\beta}\right)$ with random $\beta \in_R Z_p^*$. Then, it computes $Y = e(g, g)^{\alpha}$ with $\alpha \in_R Z_p$. At last, it picks a one-way cryptographic hash function $H: \{0,1\}^* \rightarrow Z_p$. It then publishes the parameters, params = $\langle g, h, Y, H \rangle$ and keeps MSK = $\langle \alpha \rangle$.
- **IBE.Extract (MN_i, UN_i, params, MSK):** After verifying the mobile number MN_i and device number UN_i properly, the PKG computes

$$r_i = \frac{\alpha}{\beta + ID_i};\quad K_i^{(1)} = g^{r_i} \quad t_i = \frac{\alpha}{\beta + GID_i};\ K_i^{(2)} = g^{t_i}$$

where $ID_i = H(MN_i \parallel UN_i)$, M. Then, it generates the private key $SK_i = (K_i^{(1)}, K_i^{(2)})$ and sends it via a secure network. $K_i^{(1)}$ is the private key for the individual user to decrypt the message while $K_i^{(2)}$ is the private key for decrypting the group message.

- **IBE.Encrypt (M, U, V, params):** The protocol receives the $M \in_R G_2$ and U as the client, where U contains the user's set IDs to publish the message by the recipient. After that, it picks $s_1 \in_R Z_p^*$ and computes $Y1 = (Y^{-s_1})$. It then executes the following operations:

  a) For every client $i \in U$,

http://doi.org/10.18080/jtde.v11n4.772

- Computes $ID_i = H(MN_i \parallel UN_i)$.
- Computes $T_i = \left(\left(g^{ID_i} \cdot h\right)^{s_1}\right)$, $ID_i = H(MN_i \parallel UN_i)$ which is a public key used to encrypt the data.
- Sets $T = T \cup \{T_i\}$ (Initially $T = NULL$).
- Computes $s_2 = H(Y1 \parallel T)$ and $C_U = \left((M \,.\, Y1)^{\frac{1}{s_2}}\right)$.

b) For every group $j \in V$,

- Computes $W_i = \left(\left(g^{GID_j} \cdot h\right)^{s_1}\right)$.
- Sets $= W \cup W_i$ (Initially $W = NULL$).
- Computes $s_3 = H(Y1 \parallel W)$ and $C_V = \left((M \cdot Y1)^{\frac{1}{s_3}}\right)$.

Then, it computes

$$MD = H(IDs \parallel M \parallel C_U \parallel C_V \parallel T \parallel W) \text{ where } ID_s = H(MN_s \parallel UN_s).$$

Finally, it computes the ciphertext $CT = \{C_U, C_V, T, W, MD\}$.

- **IBE.Decrypt** $(\mathbf{CT}, \mathbf{ID_s}, \mathbf{params}, \mathbf{SK_i})$: The ciphertext CT is to be decrypted for a user i. This protocol runs the following operations:

a) Not a group message,

- Computes $Z_1 = e\left(T_i, K_i^{(1)}\right)$ and $Y1' = Z_1^{-1}$.
- Computes $s_2' = H(Y1' \parallel T)$ and $C' = C_U^{s_2}$.
- Computes $M' = (C' \cdot Z_1)$.

b) Otherwise,

- Computes $Z_2 = e\left(W_i, K_i^{(2)}\right)$ and $Y2' = Z_2^{-1}$.
- Computes $s_3' = H(Y2' \parallel W)$ and $C' = C_v^{s_3}$.
- Computes $M' = (C' \cdot Z_2)$.

If $MD \stackrel{?}{=} H(ID_s \parallel M')$ is true, this algorithm will return M'; otherwise, it is NULL. In the *IBE.Decrypt*, the user computes this algorithm and gets the value of $Y1'$, s_2' and $C'$to be the same as $Y1$, s_2 and $M \cdot Y1$ in *IBE.Encrypt*, respectively, which means that the step of retrieving the data is correct.

Implementation of IBADS protocol

The data sharing protocol is developed using the Java Pairing-Based Cryptography Library (De Caro & Iovino, 2011) and the Java Cryptography packages which include java.security and javax.crypto (*Java Platform, Standard Edition Security Developer's Guide*, n.d.).

http://doi.org/10.18080/jtde.v11n4.772

- **System initiation**

  Users must register their account before using the secure data sharing application. After the registration is completed, users will receive an email sent from the CC. The email will provide the link for users to download the application, first time login password and Wc value. They then need to provide their user ID and password to perform mutual authentication with the CC. If users are first time login, they are required to do the first-time setup which is to reset their password and provide the Wc value. Then, the system will generate params for executing the algorithms of mutual authentication. Subsequently, users provide their user ID and password to the system to execute mutual authentication. If users provide the correct information, then they will successfully log in.

- **File encrypting and sharing**

  After the DO logs in successfully, the DO needs to provide a keyword which serves as an index for the file to be encrypted. The DO needs to select the DC as U and the group as V in order to share the data with them. After that, DO performs *IBE.Encrypt*. The *IBE.Encrypt* generates $M \in_R G_2$, so the DO will use this M as a secret key and perform the symmetric encryption to encrypt the file that needs to be shared with the DC. Then, the DO uses W_{DO} as a private key to perform symmetric encryption, encrypt the ciphertext M (CT_M) and send the encrypted to file, CT_M,ID_{DO},U,V and keyword then pass it to the CC.

  The CC receives the encrypted file, CT_M,ID_{DO},U,V, and keyword. Since the CC knows the W_{DO} , the CC can use it as a secret key to perform symmetric decryption to decrypt CT_M and store the encrypted file, CT_M, ID_{DO}, U,V, and keyword.

  Finally, the DO will send the keyword to the users under list U and V as a notification to inform them that there is file to be shared with them.

- **File accessing and decryption**

  After the DC logs in successfully, they need to provide a keyword to the CC for requesting the encrypted file and the related information. In this time, the CC will search the related keyword to make sure it exists. If such a keyword exists in the system, then the CC will determine whether the DC is authorised to receive the file by searching the list U and V. If access is permitted, then the CC will send CT_M and the encrypted file to the DC.

  After the DO successfully receives the details from the CC, the DC needs to request the private key to decrypt the CT_M in order to get the proper M' to perform the symmetric decryption on the encrypted file. So, he needs to provide the keyword as an index to request the key from the PKG. Once the PKG receives a request from the DC, the PKG must determine whether the specified keyword already exists in the system. Then, the PKG will determine whether the DC is authorised to receive the key and to check if the DC is in the

http://doi.org/10.18080/jtde.v11n4.772

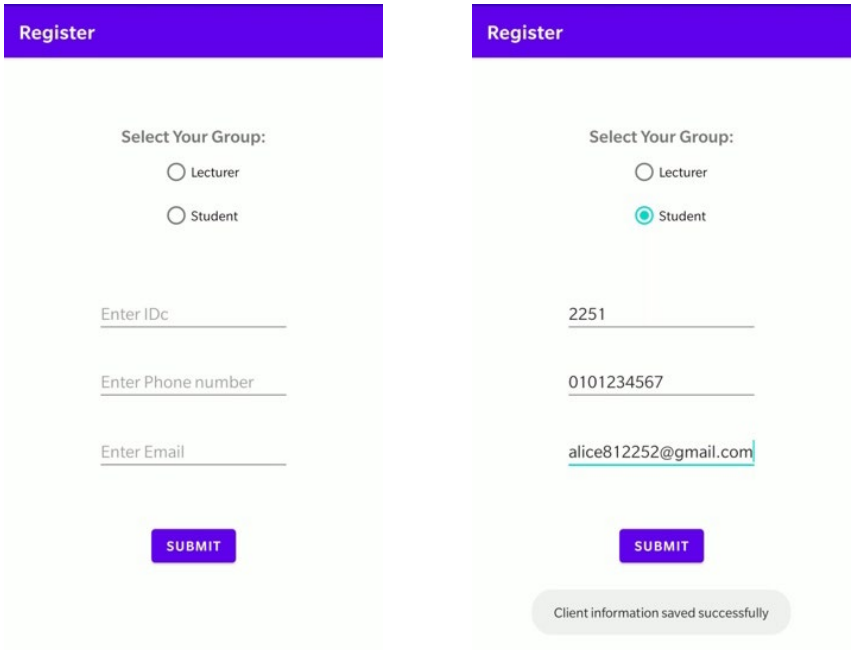
list U or V for generating the proper private key. If access is permitted and the user is in the list U, then the PKG will execute *IBE.Extract* algorithm by using the MN_{DC} and UN_{DC} to generate the private key $K_i^{(1)}$ and send it to the DC. Otherwise, if the user is in the list V then the PKG will generate the private key $K_i^{(2)}$.

Finally, the DC will execute *IBE.Decrypt* by using the proper inputs and the DC will receive the M′. After that, the DC will use the M′ as a private key to execute symmetric decryption to decrypt the encrypted file that he requested from the CC. If M′ and M are the same value, it means that the DO and the DC are using the same key to perform the symmetric encryption and symmetric decryption. So, the DC will receive the correct original file by using the correct M′to decrypt the encrypted file.

User Interface and Functionality

Register

Figure 3(a) shows the register interface for a user to register the account. The user needs to select the group and fill in the ID, phone number and email, then click the submit button to submit the information. The system will check whether the submitted information has been registered with the system. If not, the user will receive notification that client information is saved successfully (see Figure 3(b)) and get the email notification for downloading the secure data sharing application and the related details for login.



(a) (b)

Figure 3. (a) User registration interface; (b) Successfully registered

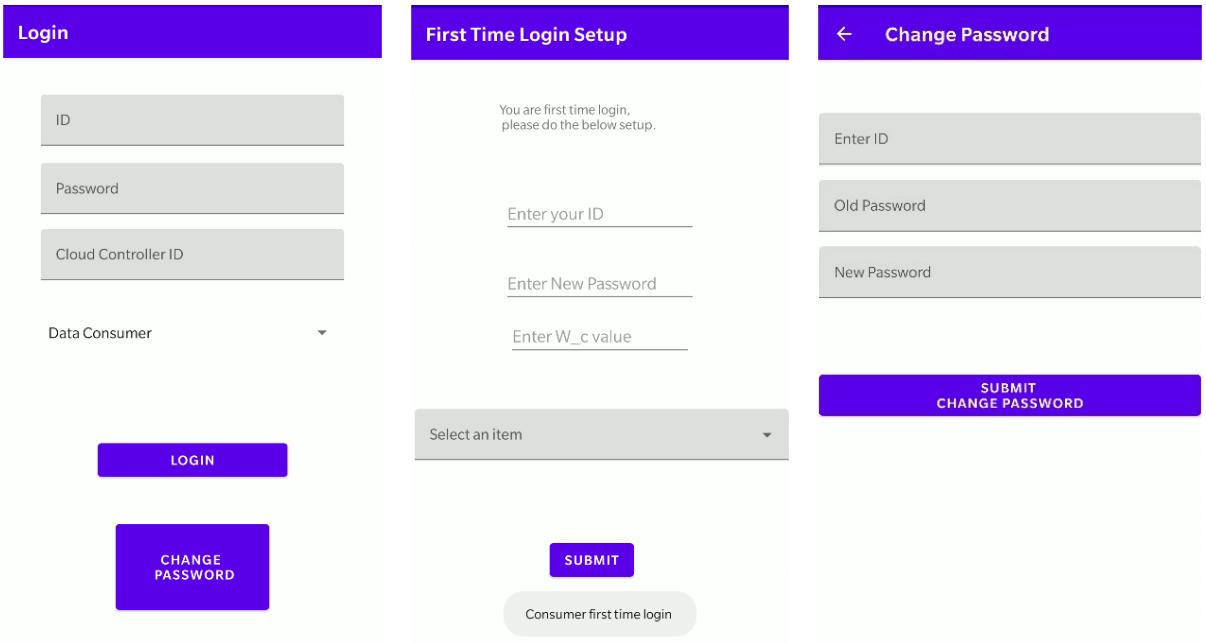
http://doi.org/10.18080/jtde.v11n4.772

Login

After the user downloads the application (see Figure 4(a)), the system will allow user input ID, password and cloud controller ID received from the previous email. If the user is first time login, then the system will navigate the user to first time login setup (see Figure 4(b)). The user needs to fill in the ID, new password and W_c value, and then click the submit button. After completing the first-time setup, the user needs to fill in the required information to log in.

After submitting, the system will execute mutual authentication to check the user and CC. If successful, the user will navigate to the home page and receive notification of authentication success.

Furthermore, the user clicks the change password button and the system will navigate to the change password page (see Figure 4(c)). The user is required to enter the ID, old password and new password to change the password. After completing the required information, the system will run a password renewal algorithm to change the user's password.



(a) (b) (c)

Figure 4. (a) Login interface; (b) First time login interface; (c) Reset password interface

Figure 5(a) shows the home page interface comprising five buttons: sharing/encrypt file, decrypt file, request file, request key and data analysis. Figure 5(b) is the interface of a sharing/encrypt file where the DO needs to enter a keyword as an index of an encrypted file and selects a user and a group list for them to access the encrypted file. After the selection, the user needs to click the encrypt file button, and the system will allow the DO to select which file the user intends to encrypt. Next, the system will run the *IBE.Setup and IBE.Encrypt* to generate the parameter M as a private key and use M to execute the Advanced Encryption

http://doi.org/10.18080/jtde.v11n4.772

Standard (AES) to encrypt the file. After that, the system will request the DO to save the encrypted file on his phone (see Figure 5(c)) and the encrypted file and CT_M will be sent to the CC. The CC will upload them to the cloud. Afterwards, the system will send an email notification to the user and the group selected by the DO.

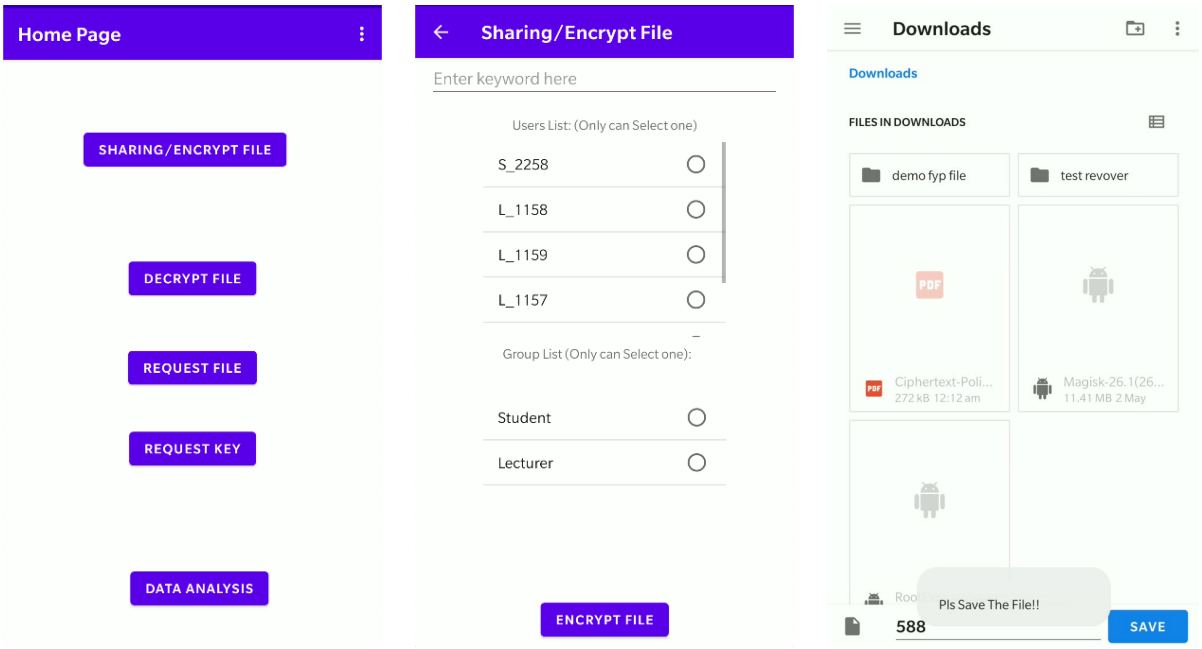


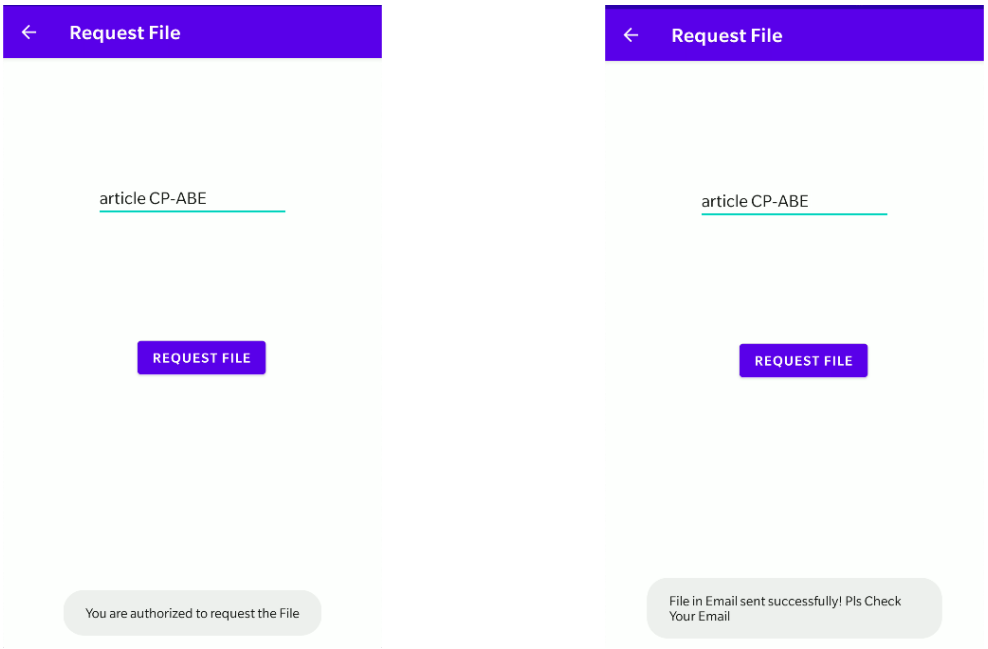
Figure 5. (a) Home page interface; (b) Sharing/encrypt file interface; (c) Save the encrypted file

When data consumers (DCs) request the file, they must click the *request file* button from the home page and fill in the keyword. After that, the CC will check if the DCs have been granted permission and send them the requested file. Figure 6(a) shows the user has permission to request the file and the requested file will be sent via email as shown in Figure 6(b).

To request the key, the DCs must click the *request key* button on the home page and enter the keyword. After that, the PKG will check if the DCs have been granted permission, the PKG will run *IBE.Extract* and send them the requested private key. Figure 7(a) shows the user has permission to request the private key and the requested private key will be sent via email as shown in Figure 7(b).

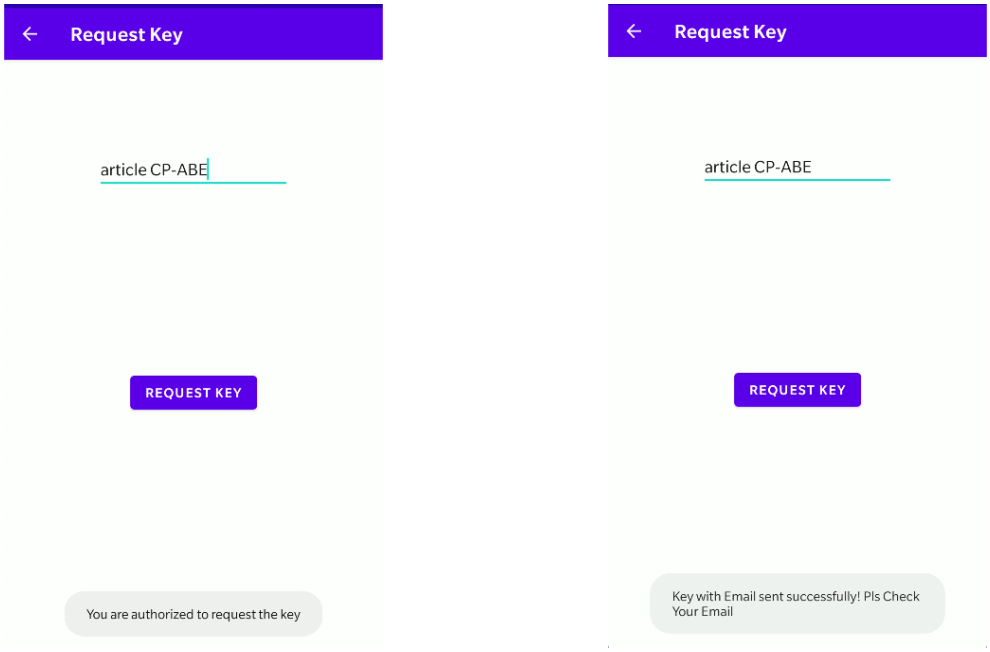
After the DCs successfully requested the encrypted file and private key, they need to click the button *decrypt file* in home page. Figure 8 shows the interface of a decrypt file. The DC needs to enter private key, keyword and DO ID. The DO ID is for the CC to decrypt the encrypted CT_M to be sent to the device of the DC, then the system will use this CT_M to run the *IBE.Decrypt* and generate the final value which is M'. After that, this M' will be used as a secret key and the system will perform AES to decrypt the file. If the DC successfully decrypts the file by providing the true information, the system will require the DC to save the decrypted file on his device.

http://doi.org/10.18080/jtde.v11n4.772



(a) (b)

Figure 6. (a) Result of check DC permission request file; (b): Email notification file sent successfully



(a) (b)

Figure 7. (a) Result of check DC permission request private key; (b): Email notification private key successful

http://doi.org/10.18080/jtde.v11n4.772

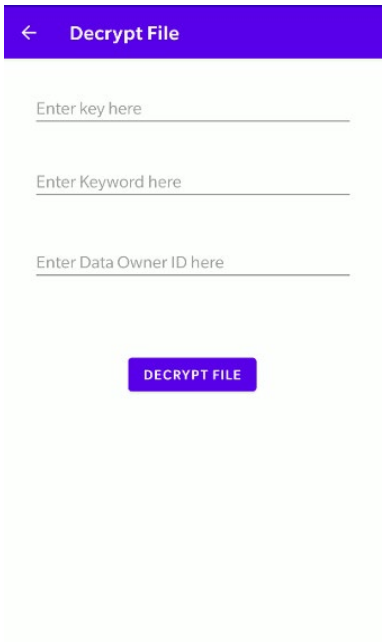


Figure 8. Decrypt file interface

Performance Analysis

IBADS is a protocol which employs IBE and AES to perform and achieve secure data sharing. Following is a discussion of the performance analysis of the IBADS protocol. The first analysis includes the execution time of the IBE scheme and include *IBE.Setup*, *IBE.Extract*, *IBE.Encrypt*, *IBE.Decrypt* in a java environment and mobile application environment. The second analysis includes the time required for encrypting and decrypting file in a mobile application environment.

The analysis is performed using MacBook Air with M2 chip 3.49GHz with 16GB RAM running on macOS Monterey for IBE scheme in java environment. The analysis is performed using Xiaomi 12T with Snapdragon 8+ Gen1 Mobile Platform Octa-core Max 3.2GHz with 11GB RAM for IBE scheme and AES encryption in Android application environment.

Performance analysis for IBE scheme

It is important to note that Karati *et al.* (2018) adopted the Pairing-Based Cryptography Library to run the bilinear pairing cryptographic operations, while this project used the Java Pairing-Based Cryptography Library in the implementation. Thus, the execution time cannot be compared directly since different cryptographic libraries are used to implement the IBADS protocol, respectively. In order to achieve faster pairing computation, Type-A curve of group size 512-bit is chosen to compute the pairing.

The performance analysis in Figure 9 shows that the IBE scheme running on the mobile application obtains good performance based on its running time. There is little difference

http://doi.org/10.18080/jtde.v11n4.772

when compared to its execution on a computer. We also take into consideration that the technical specifications of the device will also affect the running time.

Figure 9 depicts the performance of IBE algorithms, namely *IBE.Setup, IBE.Extract, IBE.Encrypt* and *IBE.Decrypt*. The X-axis represents the respective algorithms while the Y-axis represents the time taken in milliseconds. The two-colour legend represents the Java platform and Android application platform, respectively.

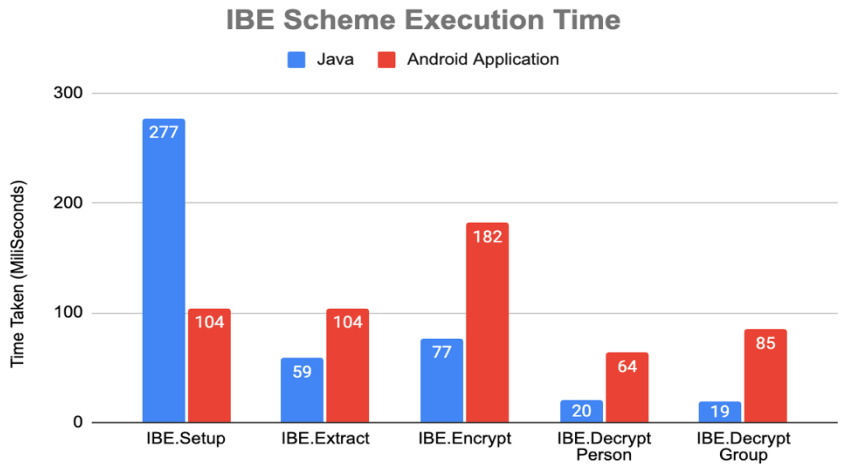


Figure 9. Performance of IBE scheme

Performance analysis for secure data sharing

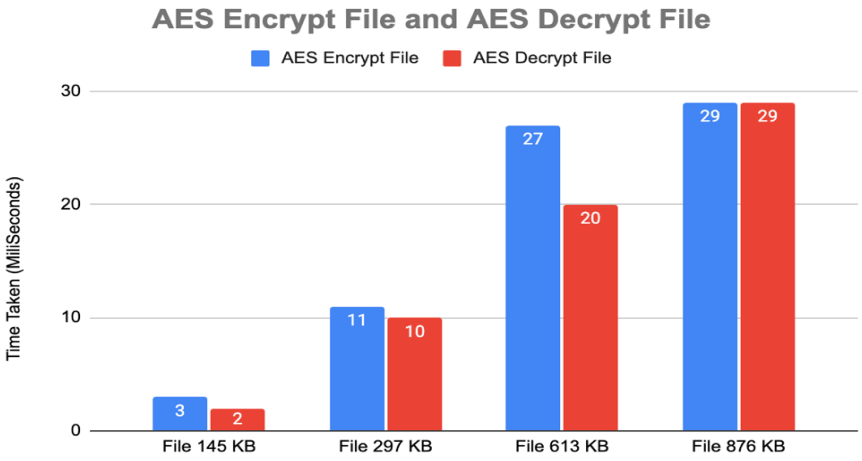


Figure 10. Performance of AES encryption

Similarly, Figure 10 shows that the AES encryption experiences good performance in the process of file encryption and decryption. This results in fast AES encryption runtime and less consumption of time in performing encryption and decryption in the mobile application. From this analysis, it is obvious that the IBADS protocol aligns with the characteristics of lightweight efficiency. This means the IBADS protocol can carry out encryption tasks on a mobile device swiftly and smoothly, assuring efficient running time and speed.

http://doi.org/10.18080/jtde.v11n4.772

This analysis records the time taken using a 256-bit key to perform AES file encryption and decryption in the mobile application. In this analysis, the files used to run the AES encryption are 145 kilobytes (KB), 297 KB, 613 KB and 876 KB, respectively.

Figure 10 presents the performance via Android application. The X-axis represents the file sizes to be encrypted and decrypted while the Y-axis represents the time taken in milliseconds. The two-colour legend represents the AES encryption time and AES decryption, respectively.

Conclusion and Potential Future Work

With the increasing number of users, the issue of secure data sharing in an untrusted cloud has become a major concern. It can lead to the privacy of users being unprotected, and the data of users being potentially stolen in a mobile cloud environment. Hence, this proposed application has implemented a secure data sharing protocol based on the IBADS protocol to ensure the data sharing process is secure and protected. The IBADS protocol performs lightweight computation operations and uses IBE as the main algorithms to perform the data sharing protocol. IBE is a user-friendly encryption based on using simple user identity as the public key to perform the encryption. It does not require the user to enter or obtain any public key prior to encryption.

Future work would consider improving the algorithms of *IBE.Encrypt* and *IBE.Decrypt* such that they can be designed to perform one-to-many operations, meaning that the DO can encrypt a file and share it to multiple users and multiple groups at once. Considering the lightweight running requirement in Android applications, this adjustment needs to be improved carefully as the one-to-many operations will increase the running times accordingly. Also, the IBE scheme employed in the IBADS protocol is using Type 1 symmetric pairing $G_1 \times G_1 \rightarrow G_T$ to execute the pairing-based cryptography. This type of pairing is simpler to implement, but has a drawback in that it requires larger parameters for a given level of security, which can then lead to inefficiencies. For better performance, Type 3 asymmetric pairing $G_1 \times G_2 \rightarrow G_T$ should be used for better performance and security as it can provide smaller parameters for the same level of security.

Acknowledgements

A version of this paper was presented at the Third International Conference on Computer, Information Technology and Intelligent Computing, (CITIC 2023), held in Malaysia on 26–28 July 2023.

This work was supported by the Telekom Malaysia Research and Development Grant (RDTC/221045).

http://doi.org/10.18080/jtde.v11n4.772

References

Cheng, B., Zhang, J., Hancke, G. P., Karnouskos, S., & Colombo, A. W. (2018). Industrial cyberphysical systems: Realizing cloud-based big data Infrastructures. *IEEE Industrial Electronics Magazine*, *12*(1), 25–35. https://doi.org/10.1109/MIE.2017.2788850

De Caro, A., & Iovino, V. (2011). Introduction. JPBC – Java Pairing-Based Cryptography Library. Proceedings of the 16th IEEE Symposium on Computers and Communications, ISCC 2011, Corfu, Greece. http://gas.dia.unisa.it/projects/jpbc/

Deng, H., Wu, Q., Qin, B., Domingo-Ferrer, J., Zhang, L., Liu, J., & Shi, W. (2014). Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. *Information Sciences*, *275*, 370–384. https://doi.org/10.1016/j.ins.2014.01.035

Han, S., Han, K., & Zhang, S. (2019). A data sharing protocol to minimize security and privacy risks of cloud storage in big data era. *IEEE Access*, *7*, 60290–60298. https://doi.org/10.1109/ACCESS.2019.2914862

Java Platform, Standard Edition Security Developer's Guide. (n.d.). Oracle. https://docs.oracle.com/javase/9/security/java-security-overview1.htm#JSSEC-GUID-2EF91196-D468-4D0F-8FDC-DA2BEA165D10

Karati, A., Amin, R., Islam, S. H., & Choo, K.-K. R. (2018). Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment. *IEEE Transactions on Cloud Computing*, *9*(1), 318–330. https://doi.org/10.1109/TCC.2018.2834405

Li, H., Huang, Q., & Susilo, W. (2022). A secure cloud data sharing protocol for enterprise supporting hierarchical keyword search. *IEEE Transactions on Dependable and Secure Computing*, *19*(3), 1532–1543. https://doi.org/10.1109/TDSC.2020.3027611

Lu, X., Pan, Z., & Xian, H. (2020). An efficient and secure data sharing scheme for mobile devices in cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *9*, 60. https://doi.org/10.1186/s13677-020-00207-5

Salvi, A. H. (2019). Information and network security with cryptography. *International Journal of Research in Electronics and Computer Engineering – a Unit of I2OR*, *7*(3), 879–883. http://nebula.wsimg.com/8340cc87de92fbce086c7959a2ab45e1?AccessKeyId=DFB1BA3CED7E7997D5B1&disposition=0&alloworigin=1

Shao, J., Lu, R., & Lin, X. (2015). Fine-grained data sharing in cloud computing for mobile devices. *2015 IEEE Conference on Computer Communications (INFOCOM)*, 2677–2685. https://doi.org/10.1109/INFOCOM.2015.7218659

CNN-based Occluded Person Re-identification in a Multi Camera Environment

Ali Imran Bin Shahrin
Multimedia University

Noramiza Binti Hashim
Multimedia University

Abstract: In the context of rising global urban security concerns and the growing use of surveillance cameras, this study aims to enhance individual identification accuracy in occlusion scenarios using deep learning. Four CNN-based models for person re-identification are analyzed and put into practice. Additionally, comparative studies are conducted, and the model's performance is assessed using the Market-1501 and Occluded-Reid datasets. We propose the use of ensemble learning and convolutional neural networks (CNNs) to address occlusion issues. Our results show that the ensemble approach performs better in re-identification tasks than traditional deep learning algorithms with an improvement of 1%–2% in mAP and Rank-1 scores, respectively.

Keywords: Person re-identification, deep learning, ensemble deep learning

Introduction

Person re-identification is a crucial discipline in computer vision, tasked with matching a person's identity across disparate surveillance cameras using different types of algorithms. This technology, which is essential for ensuring safety in crowded areas like supermarkets, airports, and cities, faces significant obstacles. Person re-identification in a multi-camera environment involves multiple camera setups to capture person identities in a certain location. As compared to a single camera setup, where person identities are caught in only one perspective, a multi-camera environment must capture the same person identity across multiple camera perspectives. With multiple camera perspectives, significant variations in an individual's appearance, due to viewpoint variation, scaling problems and occlusion, make identifying a person more difficult.

The most challenging of these obstacles is occlusion, the phenomenon where an object or person is completely or partially obscured, as it greatly reduces the visual information in an

http://doi.org/10.18080/jtde.v11n4.773

image, because of interfering elements like pedestrians and moving objects (Wei *et al.*, 2022). Although there are other factors that make this problem worse, like viewpoint and image scale variability, occlusion remains the main problem. Our research is built around the application of deep learning algorithms, with a focus on Convolutional Neural Networks (CNNs) and a straightforward ensemble learning technique. Ensemble learning, which combines predictions from various models, frequently improves performance. It is especially promising for tackling the issue of occlusion in person re-identification. Our study aims to shed light on challenging single-target, multi-camera settings plagued with occlusion issues.

Related Works

Person re-identification involves comparing identities across photos captured at different times and locations, a process referred to as multi-target multi-camera (MTMC) tracking, applied in fields like crowd analysis, traffic management, and municipal security (Shim *et al.*, 2021)

Person re-identification in a single camera and multi-camera setting

Person re-identification can be tackled from two different camera perspectives: one being from single camera settings; the other from multi-camera settings. For a single camera setting, Zhang *et al.* (2019) have managed to perform person re-identification by taking only a single camera perspective for training from a multi-camera dataset, such as Market-1501 or DukeMTMC-reID.

Significant research has been dedicated to resolving person re-identification challenges in multi-camera settings. Numerous CNN-based methods have been proposed, with each introducing innovative techniques to improve re-identification accuracy. For instance, Zhou *et al.* (2019) developed an Omni-Scale Network (OSNet) to facilitate Omni-Scale feature learning. Despite its small model size, OSNet, capable of being trained from scratch on existing re-identification datasets, has shown to outperform larger models like ResNet50 (He *et al.*, 2015) and DenseNet (Huang *et al.*, 2016). On the other hand, Yan *et al.* (2021) proposed a re-identification model that employs a bounded distance loss on occluded data to learn pedestrian features. In addition, the research presented in He *et al.* (2019) integrates pyramid pooling with a Full Convolution Network (FCN), achieving an impressive accuracy of 95.42% on the Market-1501 dataset. Lastly, the work by Wang *et al.* (2020) merges a CNN model with an adaptive direction graph, achieving a promising accuracy of 55.1% on the Occluded-Duke dataset.

http://doi.org/10.18080/jtde.v11n4.773

Deep-learning-based Person Re-identification approaches

The two main approaches to person re-identification are hand-crafted features and deep learning-based methods. Hand-crafted features encompass low-level, mid-level, and high-level semantic representations but are less utilized recently due to complications with lighting changes and occlusion (Wei *et al.*, 2022).

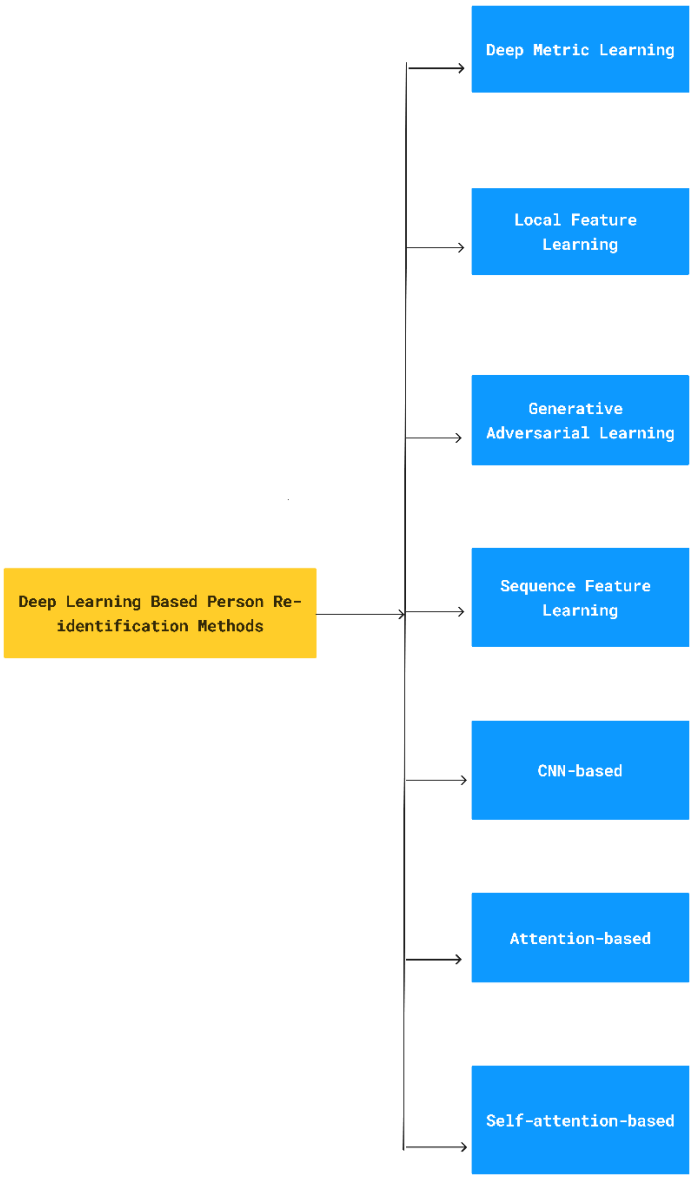


Figure 1. Deep-Learning-Based Person Re-identification Methods

Deep learning, on the other hand, has gained popularity and can be categorized into deep metric learning, local feature learning, generative adversarial learning, and sequence feature learning (Ming *et al.*, 2022), as shown in Figure 1.

Deep metric learning focuses more on training a deep neural network to learn a distance metric, thereby assisting in accurately measuring the similarity between different identities of

http://doi.org/10.18080/jtde.v11n4.773

an image. However, deep metric learning requires a considerable amount of data to perform well and can struggle with overfitting in smaller datasets (Kaya & Bilge, 2019). Local feature learning focuses on robust features to combat certain challenges, such as pose, illumination and clothing changes. Although local feature learning provides consistency in identification on appearance changes, it sometimes still suffers a variation in pose and background clutter (Wang *et al.*, 2018). On the other hand, generative adversarial learning uses a generative model to create new images and a discriminative model to distinguish real from generated images. While generative adversarial learning is useful for data augmentation, it commonly suffers from poor interpretability of neural networks (Wang *et al.*, 2017). Finally, sequence feature learning is designed to extract features from sequences of pedestrian images. It is useful in video-based person re-identification. However, it requires a large amount of sequential data and can be computationally expensive (Wei *et al.*, 2022).

Recently, newer deep learning-based solutions for person re-identification have emerged, including Convolutional Neural Network (CNN) based solutions, attention-based solutions, and self-attention-based solutions. CNN-based solutions leverage the deep learning capabilities of CNNs, using a series of convolutional layers to progressively learn image attributes and their surroundings. However, the performance of CNNs is heavily reliant on image quality (Karahan *et al.*, 2016). For example, if the training data consisted of image degradation such as occlusion, the model tends to perform much worse compared to non-occluded scenarios. Attention-based solutions focus on specific attributes, ignoring less useful background information. While effective at enhancing focus on critical details, attention-based solutions lacked semantic information from the local feature regions that they are extracting from, making it difficult to comprehend (Wei *et al.*, 2022). Self-attention-based solutions employ transformers and multi-head self-attention mechanisms to learn image embeddings. These solutions provide promising results but can be computationally heavy and less effective on smaller datasets due to their high-capacity models.

Datasets for Person Re-identification

In this research, we have decided to focus on the Market-1501 and Occluded-ReID datasets, which examine occlusion in person re-identification. A vast collection of 32,668 images from 1,501 different identities can be found in the exhaustive Market-1501 dataset developed by Zheng *et al.* (2015). In addition, the Occluded-ReID dataset created for occlusion scenarios by Zhuo *et al.* (2018) will be crucial for the needs of this study. The numerous other datasets that are readily available and contribute to the rich diversity in the field of person re-identification must also be mentioned. Examples of this kind include the CUHK01 and CUHK03 datasets by Li, W. *et al.* (2018) and the DukeMTMC-ReID by Ristani *et al.* (2016), all of which vary in the

http://doi.org/10.18080/jtde.v11n4.773

number and variety of images and identities they contain. The MSMT-17 dataset, also by Wei *et al.* (2017), stands out as the largest dataset currently available, while the VIPeR dataset by Gray *et al.* (2007) poses difficulties in terms of real-world conditions despite its smaller size. Each dataset presents distinct characteristics and difficulties, opening the door for numerous studies and developments in the field (see Table 1).

Table 1. Datasets for image-based person re-identification

Dataset	Number of identities	Number of images	Number of cameras
Market-1501 (Zheng *et al.*, 2015)	1501	32,668	6
DukeMTMC-ReID (Ristani *et al.*, 2016)	1,852	22,515	8
CUHK01 (Li, W., *et al.*, 2018)	971	3,884	2
VIPeR (Gray *et al.*, 2017)	632	1,264	2
CUHK03 (Li, W., *et al.*, 2018)	1,360	13,614	6
MSMT-17 (Wei *et al.*, 2017)	4,101	126,441	15
Occluded-ReID (Zhuo *et al.*, 2018)	200	2,000	1

Table 2. Datasets for video-based person re-identification

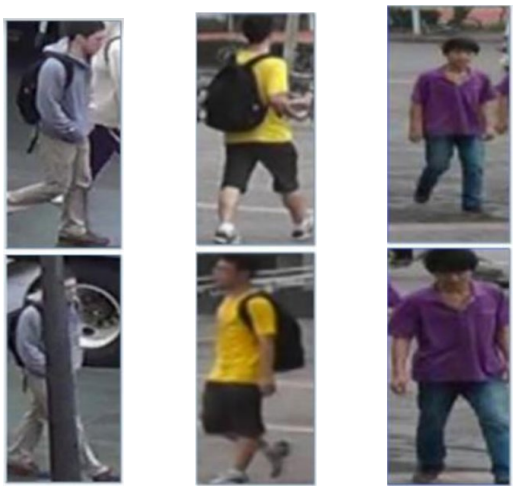
Dataset	Number of identities	Number of images	Number of cameras
DukeMTMC-VideoReID (Wu *et al.*, 2018)	702	2,196 training videos and 2,636 test-related videos	8
MARS (Zheng *et al.*, 2015)	1,261	1,191,003	8
iLIDS-VID (Li, M., *et al.*, 2018)	300	22,000	2

Several important datasets in the field of video-based person re-identification deserve to be noted as well. A sizable collection of 2,196 training videos and 2,636 test-related videos for 702 identities are available in the DukeMTMC-VideoReID dataset (Wu *et al.*, 2018). The MARS (Zheng *et al.*, 2015) dataset is notable for its size, containing over 1.19 million images from 1,261 distinct identities, captured from 8 camera viewpoints. The iLIDS-VID dataset (Li, M., *et al.*, 2018) contains 22,000 images spread across 300 identities, recorded from 2 camera views, and presents a condensed yet difficult environment for video-based re-identification

http://doi.org/10.18080/jtde.v11n4.773

studies. Each dataset (see Table 2) adds unique features and insights that broaden the scope of research on video-based person re-identification.

Challenges in Person Re-identification



(a) (b) (c)

Figure 2. Challenges in Person Re-identification (a) Occlusion; (b) Viewpoint variation; (c) Scale issues

Despite being heavily researched, person re-identification presents challenges, such as the need for more camera perspectives, high cost of data labelling for unsupervised approaches, accuracy of manual labelling, and handling appearance features, like clothing similarity or attire changes. In person re-identification, there still exist many issues that affect the performance of person re-identification, which we will highlight. One of them is occlusion, as seen in Figure 2(a).

Occlusion happens when a person is blocked by an overlapping object that can lead to inaccurate information from an image. In a person re-identification scenario, people are often occluded by environmental objects, such as a traffic sign board, vehicles in a parking lot or simply by other pedestrians. When a person is occluded, or when a portion of their body is hidden from view, the features that are extracted from the entire image may contain some distracting information and result in errors if the model cannot differentiate between the individual region and the occluded region (Zahra *et al.*, 2022).

Another problem that arises for an image when conducting person re-identification is viewpoint variation. Viewpoint variation is when a person appears in different positions of the capturing camera, as illustrated in Figure 2(b). It is challenging to create a model with great generalizability, because a person's visual appearance can change depending on the angle and proximity from which they are photographed by various cameras.

The final issue that arises when conducting person re-identification is scale differences. Scale difference is when an object appears to be in a smaller or larger form, as seen in Figure 2(c). The issue of scale difference is a challenging one to resolve, because image appearances are

http://doi.org/10.18080/jtde.v11n4.773

greatly influenced by a given camera setting. Instead of using a multiple-scale technique, most person re-identification methods use a fixed-scale approach (Ahmed *et al.*, 2015; Li *et al.*, 2014).

Deep ensemble learning

Deep ensemble learning has become an effective machine learning technique in recent years, providing a solid way to improve model performance (Serbetci & Akgul, 2020; Yang *et al.*, 2018). By utilizing the strengths of multiple learning models, this method lowers the risk of overfitting to training data, increasing robustness and generalizability. As a result, deep ensemble learning has demonstrated to be helpful in several challenging tasks, including person re-identification.

In the context of person-reidentification, ensemble approaches are employed to take advantage of the strengths of multiple person re-identification models or methods to overcome some of the limitations of individual methods. An ensemble of deep learning-based person re-identification models can contain a mixture of CNN models, attention mechanism models, self-attention mechanism models, and other types of models (Mauldin *et al.*, 2019). By strategically combining these different approaches, an ensemble model can potentially overcome some of the limitations of the individual approaches. For instance, while CNNs can sometimes overlook critical local features, attention mechanisms can help focus on these details. Conversely, where attention mechanisms may overemphasize certain regions and neglect others, the global feature learning capability of CNNs can balance this out. The self-attention mechanism, with its focus on relationship between all parts of an image, can further enhance this balance, adding a comprehensive understanding of the image context.

One key consideration when designing an ensemble model is the issue of diversity. Having a diverse set of person re-identification models can make the ensemble more robust and improve its generalization capabilities. This is because different types of models can excel in different aspects of a person re-identification task and be able to compensate for each other's weaknesses. However, ensemble learning comes with its own challenges. It is more prone towards overfitting (Li *et al.*, 2019) and more computationally expensive compared to single-model person re-identification approaches. Additionally, ensemble learning also requires careful design and tuning to ensure that the base person re-identifications are complementary with each other and that their outputs are combined in an effective way. Some of the methods of approaching ensemble learning are dropout ensemble, snapshot ensemble and boosting.

Deep ensemble learning has been investigated for person re-identification in a few notable studies. In Srivastava *et al.* (2014) and Singh *et al.* (2016), a regularization technique called dropout is often used and seen as a form of ensemble learning. During training, dropout

http://doi.org/10.18080/jtde.v11n4.773

involves randomly "dropping out" or deactivating a proportion of neurons in the network. Apart from that, snapshot ensemble can also be seen being used by Garipov *et al.* (2018). Snapshot ensemble involves saving model parameters at several points during training, and then averaging their predictions. Boosting is also another ensemble technique that involves training several models sequentially, where each model learns from the errors of its predecessor. Li *et al.* (2019) utilized boosting by adaptively assembling features and metrics from a ranking perspective.

Research gap

Currently, the training strategies employed for ensemble learning models often necessitate the independent training of multiple deep learning networks. This can prove to be computationally expensive and raises the question of whether there could be more efficient approaches to use ensemble deep learning. In addition, despite noteworthy advances in the field, occlusion remains a substantial problem in person re-identification. The existing research field is notably insufficient when it comes to addressing occlusion issues through ensemble deep learning. While past studies (Serbetci & Akgul, 2020) have demonstrated that ensemble learning can significantly boost the performance of person re-identification in general datasets like Market-1501, its implementation in occlusion-based datasets, such as Occluded-Reid, remains in a premature stage. This underlines an urgent need for more intensive research in this area. Therefore, we propose a baseline solution for a simple ensemble learning method called model averaging for other researchers to implement this technique and possibly improve their own person re-identification models.

Research Methodology

Data collection

For this research, we use publicly available datasets. The Market-1501 dataset (Zheng *et al.*, 2015) is used for image-based person re-identification. It comprises 1,501 IDs and 32,668 bounding boxes. As an attempt at solving the problem of occlusion in person re-identification, the Occluded-Reid dataset (Zhuo *et al.*, 2018) will be used. This dataset consists of 2000 images of 200 occluded identities. Each identity contains 5 full body person images and 5 occluded person images.

Data pre-processing and feature extraction

Data splitting and feature extraction will both be applied to the chosen datasets. Each dataset has a distinct split that was established by the dataset's creators, and this study will abide by that split. Consider the 32,668 image Market-1501 dataset as an illustration. Of these images,

http://doi.org/10.18080/jtde.v11n4.773

12,936 will be used for training, 3,368 as the query set, and the remaining 15,913 will be used as the gallery set. The Occluded-Reid dataset uses occluded person images as query, full-body person images as the gallery, and randomly divided identities with half going to training and the other half going to testing.

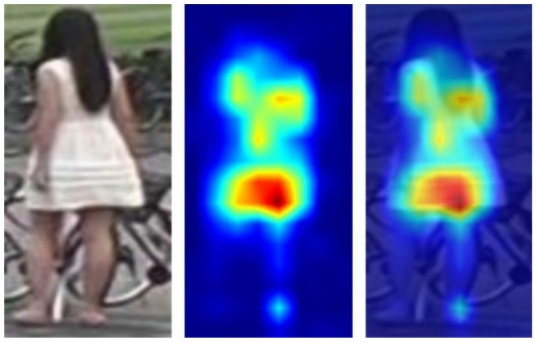


Figure 3. Feature extraction using OSNet (Zhou *et al.*, 2019)

Following the data splitting procedure, feature extraction is done to extract important attributes from the source data. The research's feature extraction procedure is dependent on the model being used. For example, if we are choosing the OSNet model, it performs two functions: it extracts features; and acts as a predictive model. In other words, the model does not require any additional feature extraction algorithms or manual intervention to extract pertinent features from the input data directly. It is crucial to remember that the features that are extracted have an unbreakable connection to the particulars of the selected model. For instance, based on Figure 3, depending on the nature and depth of its architecture, it might extract features from the input data such as the clothing information of a specific identity. In this method, the internal layers of the loaded model's architecture are used to automatically identify and extract significant features from the data. The subsequent phases of model training and testing make use of this extracted data.

Model training and testing

We implement the deep learning method known as CNN for model training and testing. The goal is to uniquely classify person images based on the specified dataset. Model configuration also includes choosing an optimizer and loss function. In the model training and testing phase, a selection of baseline models provided by the torchreid library (Zhou *et al.*, 2019), including ResNet50 (He *et al.*, 2015; Xie *et al.*, 2016), OSNet (Zhou *et al.*, 2019) and its variations, DenseNet (Huang *et al.*, 2016), and others, will be utilized.

The primary reasons for selecting these models are threefold. Firstly, these models have been extensively validated in the literature and have demonstrated high performance in a range of computer vision tasks, including person re-identification. Their robust performance is attributed to their unique architectures that allow for the extraction of hierarchical, multi-

http://doi.org/10.18080/jtde.v11n4.773

scale features, which are crucial in the context of person re-identification. Secondly, these models provide a diverse set of architectures for comparison and ensemble learning. ResNet50, for instance, introduces a residual learning framework to ease the training of networks, while DenseNet connects each layer to every other layer in a feed-forward fashion, enabling feature reuse. On the other hand, OSNet incorporates omni-scale feature learning into deep neural networks, making it highly effective for person re-identification. The diversity in architecture not only allows for comprehensive comparison but also increases the potential for ensemble learning to achieve more robust results. Finally, these models are readily available in the torchreid library (Zhou *et al.*, 2019), making them convenient to employ in our research framework. The availability of these models, along with the necessary training and evaluation utilities, reduces implementation time and allows for a focus on the experimental design and results analysis.

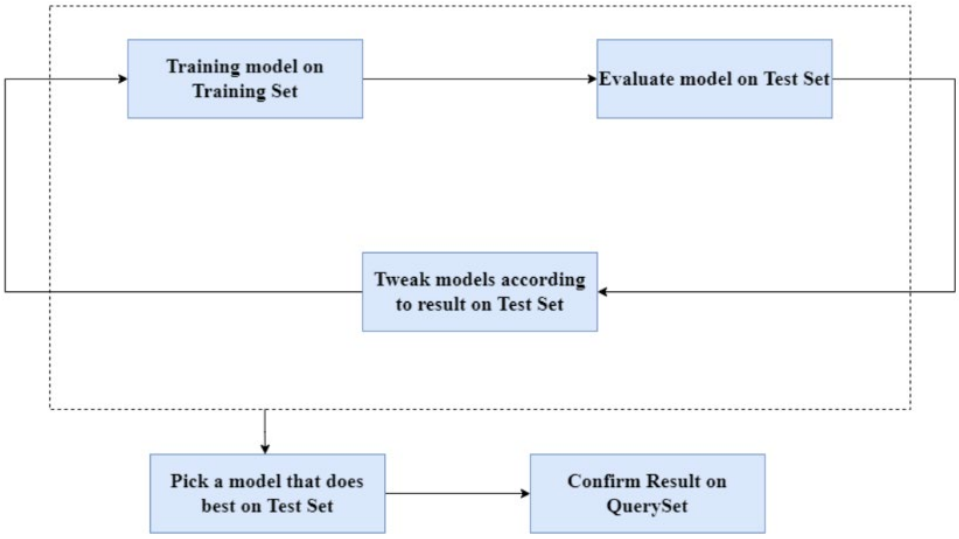


Figure 4. Framework of the model training and testing process

Loss function and optimizer

We used the Triplet loss engine, which is renowned for its effectiveness in person re-identification tasks, during the training and testing phases of our models (Hermans *et al.*, 2017). By enhancing anchor-positive-negative triplets, this function increases the capacity of learned embeddings for discrimination. The Adam optimizer (Kingma & Ba, 2014) was used, and its learning rate was set to 0.0003, because it has a track record of success (Zhou *et al.*, 2019) and is computationally efficient for deep-learning model training. These hyperparameter selections, along with our choice of deep learning models, were made with the goal of creating a robust and effective system for person re-identification.

http://doi.org/10.18080/jtde.v11n4.773

Simple ensemble learning

This study makes use of Model Averaging (Srivastava *et al.*, 2014), a type of ensemble learning technique. The predictions of various models are combined in this method, which is renowned for its effectiveness in improving model performance. This is accomplished by averaging the results from each model in a way that lowers variance, encourages generalizability, and minimizes the risk of overfitting.

Model averaging is used in this study in a novel way. We combine the unique predictive power of two distinct models by averaging the features they extract, as opposed to averaging predictions. By encapsulating each model's unique strengths in a new feature space, this process increases the robustness of the resulting ensemble model. While not explicitly tailored to occlusion, viewpoint variation, or scale differences individually, we have conducted comprehensive evaluations, including testing on an occlusion-focused dataset. The results, presented in a subsequent section, demonstrate notable effectiveness in addressing challenges posed by occluded images. The Euclidean metric is used to calculate a distance matrix after averaging the features. This matrix measures how different each pair of features from the query set and the gallery set are from one another. The foundation for subsequent evaluation tasks is provided by this integral computation, demonstrating how model averaging can be creatively used to support person re-identification efforts.

Integration of learners from CNN

As we highlight the use of model averaging, we also need to explain how this ensemble approach is specifically customized for our use case. We purposefully include CNNs as the base learners in the group. Notably, the superior individual performance of OSNet models is the main factor in CNN selection. OSNet models, as proposed by Zhou *et al.* (2019), exhibit remarkable capabilities in extracting intricate features from complex data. These models have demonstrated robustness and high accuracy as standalone entities. In our ensemble framework, we leverage the inherent strengths of OSNet models, combining OSNet with its sub-models, such as OSNet_x0_75, with OSNet_x1_0, which we can observe in the result subsection later. The individual strengths of OSNet models—which demonstrate high mAP scores, Rank-1, Rank-5, Rank-10, and Rank-20 accuracy metrics on the Market-1501 dataset—are the main justification for using them. Our goal is to leverage the complementary features of two different OSNet models to improve the performance of the ensemble model in a synergistic way. As the following model comparison section shows, this strategic combination works especially well for addressing issues like occlusion.

http://doi.org/10.18080/jtde.v11n4.773

Model evaluation

Two metrics are employed for evaluating the performance of the models: the CMC curve and the mAP score.

- Cumulative Match Characteristic (CMC) Curve: The CMC curve provides a visual representation of the identification job's performance by comparing the number of candidates returned with the probability of accurate identification (Paisitkriangkrai *et al.*, 2015). The curve is generated by determining the accuracy of the top-k retrieved images in the test set containing the query identity. Based on Figure 5, the accuracy of Rank-1 will increase generally because the first image is a correct prediction based on the query. But as the rank gradually increases, for example in Rank-5, the first 5 images will be taken to evaluate the prediction based on the query. As we can observe, the first 5 images contain 3 wrong predictions, making the accuracy at Rank-5 decrease.

Figure 5. Predictions made by a model based on query image.

- Mean Average Precision (mAP) Score: The mAP score calculates the average precision for each query image. It considers the number of correct person retrievals, helping gauge the model's performance at retrieving more accurate people and ranking the correct person higher in the list of retrieved images.

Calculation Results and Discussion

When examining the person re-identification task on the non-occluded dataset, the OSNet ensemble model surpasses other individual models, achieving a mAP score of 80.6%, and Rank-1, Rank-5, Rank-10, and Rank-20 accuracies of 93.1%, 97.5%, 98.5%, and 99.1%, respectively. In addition, when compared to single architecture models, our model seems to be the best performing among them all. Our model's performance is likely due to the ensemble model's ability to leverage the distinct strengths of multiple models, thereby enhancing its adaptability and generalization capabilities (Perin *et al.*, 2020). Such strengths make it an effective approach in handling the unique challenges posed by person re-identification tasks.

http://doi.org/10.18080/jtde.v11n4.773

Table 3. Comparison of rank 1/5/10/20 on the Market-1501 dataset
(*Result highlighted in bold is the best performing in our experimentation)

Dataset	**Market-1501**				
Model Name	mAP score	Rank-1	Rank-5	Rank-10	Rank-20
DenseNet121 (Huang *et al.*, 2016)	64.0%	83.3%	92.4%	94.9%	96.7%
DenseNet169 (Huang *et al.*, 2016)	65.8%	84.2%	92.8%	95.2%	96.7%
DenseNet201 (Huang *et al.*, 2016)	63.5%	81.9%	91.8%	94.4%	96.2%
ResNet101 (He *et al.*, 2015)	67.8%	84.1%	93.9%	95.9%	97.4%
ResNet50 (He *et al.*, 2015)	67.6%	84.6%	93.5%	96.3%	97.8%
ResNext50 (Xie *et al.*, 2016)	67.9%	84.8%	93.4%	95.7%	97.6%
OSNet_x0_75 (Zhou *et al.*, 2019)	76.4%	91.3%	97.1%	98.3%	98.7%
OSNet_x1_0 (Zhou *et al.*, 2019)	79.5%	92.5%	97.2%	98.3%	98.9%
OSNet Ensemble	**80.6%**	**93.1%**	97.5%	98.5%	99.1%

Table 4. Comparison of rank 1/5/10/20 for state-of-art models on the Market1501 dataset

Dataset	**Market-1501**				
Model Name	mAP score	Rank-1	Rank-5	Rank-10	Rank-20
OSNet Ensemble	80.6%	93.1%	97.5%	98.5%	99.1%
PAT (Li *et al.*, 2021)	88.0%	95.4%	-	-	-
GASM (He & Liu, 2020)	84.7%	95.3%	-	-	-

However, when compared to sophisticated state-of-the-art architecture, our ensemble model tends to fall off in terms of mAP score and Rank-1. This might be because GASM leverages spatial features that can help extract rich information from the input data, creating a more effective person re-identification model. Apart from that, PAT might perform better because of its dealing with occlusion. The model addresses occlusion using part discovery, which is useful in crowded scenarios, making the model learn and recognizing individual parts.

For this occlusion-based dataset, ensemble learning also helps improve the general performance of the person re-identification model. For comparative analysis, we have benchmarked our results against other state-of-the-art CNN methods, such as AFBP (see Table 5). Numerically, the ensemble model exhibits the highest mAP score at 56.0% compared to the individual models, suggesting superior average precision across all queries.

http://doi.org/10.18080/jtde.v11n4.773

Furthermore, when compared to more sophisticated methods, such as AFBP, it achieves a comparable performance across Rank-n accuracy, attaining Rank-1, Rank-5, Rank-10, and Rank-20 scores of 62.8%, 81.8%, 88.4%, and 93.4% respectively. This can be because ensemble learning can reduce model variance (Rajaraman *et al.*, 2019) by optimally combining predictions from multiple models.

Table 5. Comparison of rank 1/5/10/20 on the Occluded-Reid dataset
(*Result highlighted in bold is the best performing in our experimentation)

Dataset	**Occluded-Reid**				
Model Name	mAP score	Rank-1	Rank-5	Rank-10	Rank-20
DenseNet121 (Huang *et al.*, 2016)	49.6%	54.2%	73.2%	81.2%	86.6%
DenseNet169 (Huang *et al.*, 2016)	55.0%	61.8%	78.8%	85.0%	90.0%
DenseNet201 (Huang *et al.*, 2016)	55.4%	60.2%	80.4%	86.6%	90.8%
ResNet101 (He *et al.*, 2015)	41.1%	43.8%	62.4%	72.2%	79.8%
ResNet50 (He *et al.*, 2015)	45.7%	49.8%	67.8%	78.2%	86.6%
ResNext50 (Xie *et al.*, 2016)	50.4%	55.0%	74.2%	80.8%	87.8%
OSNet_ibn_x1_0 (Zhou *et al.*, 2019)	53.6%	58.8%	77.4%	84.4%	90.4%
OSNet_x1_0 (Zhou *et al.*, 2019)	51.8%	60.4%	76.6%	84.0%	90.8%
OSNet Ensemble	**56.0%**	**62.8%**	81.8%	88.4%	93.4%
AFBP (Zhuo *et al.*, 2018)	-	68.14%	88.29%	-	-

Conclusion

For this occlusion-based dataset, ensemble learning also helps improve the general performance of the person re-identification model. For comparative analysis, we have benchmarked our results against other state-of-the-art CNN methods such as AFBP. Numerically, the ensemble model exhibits the highest mAP score at 56.0% compared to the individual models, suggesting superior average precision across all queries. Furthermore, when compared to more sophisticated methods such as AFBP it achieves a comparable performance across Rank-n accuracy, attaining Rank-1, Rank-5, Rank-10, and Rank-20 scores of 62.8%, 81.8%, 88.4%, and 93.4% respectively. This can be because ensemble learning can reduce model variance (Rajaraman *et al.*, 2019) by optimally combining predictions from multiple models.

http://doi.org/10.18080/jtde.v11n4.773

Acknowledgement

A version of this paper was presented at the third International Conference on Computer, Information Technology and Intelligent Computing, CITIC 2023, held in Malaysia on 26–28 July 2023.

References

Ahmed, E., Jones, M., & Marks, T. K. (2015). An Improved Deep Learning Architecture for Person Re-Identification. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 2015, pp. 3908–3916. https://doi.org/10.1109/CVPR.2015.7299016

Garipov, T., Izmailov, P., Podoprikhin, D., Vetrov, D., & Wilson, A. G. (2018). *Loss Surfaces, Mode Connectivity, and Fast Ensembling of DNNs*. http://arxiv.org/abs/1802.10026

Gray, D., Brennan, S., & Tao, H. (2007). *Evaluating Appearance Models for Recognition, Reacquisition, and Tracking*. https://api.semanticscholar.org/CorpusID:15225312

He, K., Zhang, X., Ren, S., & Sun, J. (2015). *Deep Residual Learning for Image Recognition*. http://arxiv.org/abs/1512.03385

He, L., & Liu, W. (2020). Guided Saliency Feature Learning for Person Re-identification in Crowded Scenes. In Vedaldi, A., Bischof, H., Brox, T., Frahm, J. M. (eds), Computer Vision – ECCV 2020. ECCV 2020. Lecture Notes in Computer Science, vol. 12373. Springer, Cham. https://doi.org/10.1007/978-3-030-58604-1_22

He, L., Wang, Y., Liu, W., Zhao, H., Sun, Z., & Feng, J. (2019). Foreground-aware Pyramid Reconstruction for Alignment-free Occluded Person Re-identification. 2019 IEEE/CVF International Conference on Computer Vision (ICCV), Seoul, Korea (South), 2019, pp. 8449–8458. https://doi.org/10.1109/ICCV.2019.00854

Hermans, A., Beyer, L., & Leibe, B. (2017). *In Defense of the Triplet Loss for Person Re-Identification*. http://arxiv.org/abs/1703.07737

Huang, G., Liu, Z., van der Maaten, L., & Weinberger, K. Q. (2016). *Densely Connected Convolutional Networks*. http://arxiv.org/abs/1608.06993

Karahan, S., Yildirim, M. K., Kirtac, K., Rende, F. S., Butun, G., & Ekenel, H. K. (2016). How Image Degradations Affect Deep CNN-based Face Recognition? 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 2016, pp. 1–5. https://doi.org/10.1109/BIOSIG.2016.7736924

Kaya, M., & Bilge, H. Ş. (2019). Deep metric learning: A survey. *Symmetry*, *11*(9), 1066. https://doi.org/10.3390/sym11091066

Kingma, D. P., & Ba, J. (2014). *Adam: A Method for Stochastic Optimization*. http://arxiv.org/abs/1412.6980

Li, M., Zhu, X., & Gong, S. (2018). *Unsupervised Person Re-identification by Deep Learning Tracklet Association*. http://arxiv.org/abs/1809.02874

Li, W., Zhao, R., Xiao, T., & Wang, X. (2014). DeepReID: Deep filter pairing neural network for person re-identification. Proceedings of the IEEE Computer Society Conference on

Computer Vision and Pattern Recognition, pp. 152–159. https://doi.org/10.1109/CVPR.2014.27

Li, W., Zhu, X., & Gong, S. (2018). Harmonious Attention Network for Person Re-identification. Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 2285–2294. https://doi.org/10.1109/CVPR.2018.00243

Li, Y., He, J., Zhang, T., Liu, X., Zhang, Y., & Wu, F. (2021). Diverse Part Discovery: Occluded Person Re-identification with Part-Aware Transformer. 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Nashville, TN, USA, 2021, pp. 2897–2906 https://doi.org/10.1109/CVPR46437.2021.00292

Li, Z., Han, Z., Xing, J., Ye, Q., Yu, X., & Jiao, J. (2019). High performance person re-identification via a boosting ranking ensemble. *Pattern Recognition*, *94*, 187–195. https://doi.org/10.1016/j.patcog.2019.05.022

Mauldin, T. A., Ngu, A., Metsis, V., Canby, M. E., & Tesic, J. (2019). Experimentation and Analysis of Ensemble Deep Learning in IoT Applications. *Open Journal of Internet of Things (OJIOT)*, *5*(1), 133–149. https://api.semanticscholar.org/CorpusID:264249126

Ming, Z., Zhu, M., Wang, X., Zhu, J., Cheng, J., Gao, C., Yang, Y., & Wei, X. (2022). Deep learning-based person re-identification methods: A survey and outlook of recent works. *Image and Vision Computing*, *119*. https://doi.org/10.1016/j.imavis.2022.104394

Paisitkriangkrai, S., Shen, C., & Van Den Hengel, A. (2015). Learning to rank in person re-identification with metric ensembles. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 2015, pp. 1846–1855. https://doi.org/10.1109/CVPR.2015.7298794

Perin, G., Chmielewski, Ł., & Picek, S. (2020). Strength in numbers: Improving generalization with ensembles in machine learning-based profiled side-channel analysis. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2020*(4), 337–364. https://doi.org/10.13154/tches.v2020.i4.337-364

Rajaraman, S., Jaeger, S., & Antani, S. K. (2019). Performance evaluation of deep neural ensembles toward malaria parasite detection in thin-blood smear images. *PeerJ*, *7*. https://doi.org/10.7717/PEERJ.6977

Ristani, E., Solera, F., Zou, R. S., Cucchiara, R., & Tomasi, C. (2016). *Performance Measures and a Data Set for Multi-Target, Multi-Camera Tracking*. http://arxiv.org/abs/1609.01775

Serbetci, A., & Akgul, Y. S. (2020). End-to-end training of CNN ensembles for person re-identification. *Pattern Recognition*, *104*, 107319. https://doi.org/10.1016/j.patcog.2020.107319

Shim, K., Yoon, S., Ko, K., & Kim, C. (2021). Multi-Target Multi-Camera Vehicle Tracking for City-Scale Traffic Management. 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Nashville, TN, USA, 2021, pp. 4188–4195. https://doi.org/10.1109/CVPRW53098.2021.00473

Singh, S., Hoiem, D., & Forsyth, D. (2016). *Swapout: Learning an ensemble of deep architectures*. http://arxiv.org/abs/1605.06465

Srivastava, N., Hinton, G., Krizhevsky, A., & Salakhutdinov, R. (2014). Dropout: A Simple Way to Prevent Neural Networks from Overfitting. *Journal of Machine Learning Research*, *15*(56), 1929–1958. http://jmlr.org/papers/v15/srivastava14a.html

Wang, G., Yang, S., Liu, H., Wang, Z., Yang, Y., Wang, S., Yu, G., Zhou, E., & Sun, J. (2020). *High-Order Information Matters: Learning Relation and Topology for Occluded Person Re-Identification*. https://arxiv.org/abs/2003.08177

Wang, K., Gou, C., Duan, Y., Lin, Y., Zheng, X., & Wang, F. Y. (2017). Generative adversarial networks: Introduction and outlook. *IEEE/CAA Journal of Automatica Sinica*, *4*(4), 588–598. https://doi.org/10.1109/JAS.2017.7510583

Wang, K., Wang, H., Liu, M., Xing, X., & Han, T. (2018). Survey on person re-identification based on deep learning. *CAAI Transactions on Intelligence Technology*, *3*(4), 219–227. https://doi.org/10.1049/trit.2018.1001

Wei, L., Zhang, S., Gao, W., & Tian, Q. (2017). *Person Transfer GAN to Bridge Domain Gap for Person Re-Identification*. http://arxiv.org/abs/1711.08565

Wei, W., Yang, W., Zuo, E., Qian, Y., & Wang, L. (2022). Person re-identification based on deep learning — An overview. *Journal of Visual Communication and Image Representation*, *82*, 103418. https://doi.org/10.1016/j.jvcir.2021.103418

Wu, Y., Lin, Y., Dong, X., Ya, Y., Ouyang, W., & Yang, Y. (2018). Exploit the Unknown Gradually: One-Shot Video-Based Person Re-Identification by Stepwise Learning. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 2018, pp. 5177–5186. https://doi.org/10.1109/CVPR.2018.00543

Xie, S., Girshick, R., Dollár, P., Tu, Z., & He, K. (2016). *Aggregated Residual Transformations for Deep Neural Networks*. http://arxiv.org/abs/1611.05431

Yan, C., Pang, G., Jiao, J., Bai, X., Feng, X., & Shen, C. (2021). Occluded Person Re-Identification with Single-scale Global Representations. 2021 IEEE/CVF International Conference on Computer Vision (ICCV), Montreal, QC, Canada, 2021, pp. 11855–11864. https://doi.org/10.1109/ICCV48922.2021.01166

Yang, Y., Liu, X., Ye, Q., & Tao, D. (2018). Ensemble learning-based person re-identification with multiple feature representations. *Complexity*, *2018*, 5940181. https://doi.org/10.1155/2018/5940181

Zahra, A., Perwaiz, N., Shahzad, M., & Fraz, M. M. (2022). *Person Re-identification: A Retrospective on Domain Specific Open Challenges and Future Trends*. http://arxiv.org/abs/2202.13121

Zhang, T., Xie, L., Wei, L., Zhang, Y., Li, B., & Tian, Q. (2019). *Single Camera Training for Person Re-identification*. http://arxiv.org/abs/1909.10848

Zheng, L., Shen, L., Tian, L., Wang, S., Wang, J., & Tian, Q. (2015). Scalable Person Re-identification: A Benchmark. 2015 IEEE International Conference on Computer Vision (ICCV), Santiago, Chile, 2015, pp. 1116–1124 https://doi.org/10.1109/ICCV.2015.133

Zhou, K., Yang, Y., Cavallaro, A., & Xiang, T. (2019). *Omni-Scale Feature Learning for Person Re-Identification*. http://arxiv.org/abs/1905.00953

Zhuo, J., Chen, Z., Lai, J., & Wang, G. (2018). *Occluded Person Re-identification*. http://arxiv.org/abs/1804.02792

http://doi.org/10.18080/jtde.v11n4.773

Interview with Teresa Corbin

Telstra's Chief Customer Advocate

Teresa Corbin
Telstra Corporation Ltd

Robert Morsillo
RMIT University

Abstract: Teresa Corbin's name was synonymous for many years with consumer advocacy in Australian telecommunication in her role as CEO of Consumers' Telecommunications Network (CTN) from 2003 and Australian Communications Consumer Action Network (ACCAN) from 2010. In November 2021 Teresa joined Telstra Corporation Ltd as their Chief Customer Advocate. Here she speaks with Robert Morsillo about her new role, its opportunities and challenges, and how she sees Australian consumers engaging with telecommunications and the digital economy.

Keywords: Customer Advocate, Telecommunications, Telstra Corporation Ltd

Interview

This interview with Teresa Corbin, Telstra's Chief Customer Advocate, was conducted by Robert Morsillo via video conference on 27 November 2023.

[Morsillo] Thanks for your time, Teresa. It must have been a big change from working in a small not-for-profit community organisation to a large corporate. What has your experience been like?

[Corbin] Well, I would say that the first year was really fascinating, because what I expected was quite different to the reality. I had thought that people in large companies were driven by different things and must be interested in very different problems. However, even though obviously you're thinking about shareholders instead of members (when I was CEO at ACCAN [Australian Communications Consumer Action Network]), the problems and issues are not as vastly different as you think. The reality is still the same. We're still talking about limited resources and the same telecommunications environment, the same challenges for customers with vulnerable circumstances – none of that has changed. It's

http://doi.org/10.18080/jtde.v11n4.908

just that you're working on the problems from a different angle. And even though you're now inside the telco you should be able to have the same if not better impact on what's happening. So, I guess it's my role that has shifted rather than the problems or issues having shifted. It's the way I engage with the problems or issues that is different.

[Morsillo] Only a few organisations in Australia have a Chief Customer Advocate or similar role. Why has Telstra decided to maintain such a function?

[Corbin] I'm not the first person in the role of Customer Advocate at Telstra, though Telstra is the first telecommunications provider in Australia to have such a position. When I was thinking about taking up the role and talking to people who set up the position, it was clear that Telstra already does an enormous number of things to listen to customers. The question is: what's missing in that existing mix? I think Telstra realised that they could do with having an independent perspective all the time, not just every three or six months when they're having a particular stakeholder meeting or when there is a set agenda to ask specific questions — but to be able to have issues raised independently on the fly while the company is dealing with and grappling with some really challenging matters. And so, it's probably just the next step along the line of how you listen most effectively to consumers and to customers. The banks have Customer Advocate roles, and the Royal Commission was a prompt. While telecommunications hasn't had that sort of inquiry, I think that everybody could see that there were some good things coming out of the fact that there were customer advocates in banking and financial services and that was something that Telstra could benefit from.

[Morsillo] Telstra has a very large customer base, including small businesses and large enterprises. How do you decide where to focus your efforts?

[Corbin] What we do is try to work out where we can have the most impact – and that means focussing on customers that are really struggling to stay connected. It aligns with Telstra's purpose "to build a connected future so everyone can thrive". It's a focus on customers in vulnerable circumstances. Telstra has existing detailed advocacy and work going on internally in relation to People with a Disability and First Nations people – not just as customers but in relation to employees through our Accessibility Action Plan and Reconciliation Action Plan. And there's also been an enormous program with low-income measures for a long time. So, it's looking at where the gaps might be as new services and products get created and as some products get retired. What does the new environment look like and how do we make sure that the products and services meet the needs of customers? Rather than trying to pick out specific areas, we've tried to develop a strategy that provides a framework of fairness and inclusion, some overarching perspectives, and

http://doi.org/10.18080/jtde.v11n4.908

then educate the business that this is the role of the Customer Advocate. If you think that something you're working on might raise questions that you are not sure of in this regard, come and talk to the Customer Advocate so that we can try and look at the issues before they become a problem. It's not just a question of addressing problems but trying to prevent problems as well.

[Morsillo] What are you seeing as the biggest issues for consumers of telecommunications services and digital platforms in Australia today?

[Corbin] Probably the one that we're most interested in, no surprise, is artificial intelligence (AI) and how that impacts on consumers' connectivity and digital capability. While we work on accessibility, availability and affordability, the truth is that if we haven't improved digital capability then none of those things matter. You kind of need to have all four addressed to ensure that people can stay adequately connected. And when I say adequately connected, we're not just talking about having a connection, you must have enough data and you must have the right kind of devices to access it. So, the complexity of these services is not reducing, and neither is the cost, even though the accessibility and availability are gradually improving. Going forward, we need to focus more on affordability and digital capability because the capabilities piece is constantly shifting. And AI has highlighted this all to us. The main issue is whether consumers can deal with the impacts of AI in all the apps and platforms that are using it. What does it mean for privacy? For online search? What's happening to your data that's for sale? You need to understand a lot more about how it all works to get what you need. And so that comes back full swing to capability. You may not need to know everything about digital, but you do need digital skills in whatever your sphere of life is, like accessing government services, or education, if that's where you are in your life or employment.

[Morsillo] What's a typical day-in-the-life of a Chief Customer Advocate look like?

[Corbin] Well, I spend a lot of time talking to various people who are working on lots of different things throughout the company. So, I get visibility of the enormous range and scope of the company, which can be quite a challenge when I think I was working in an organisation of 20 people previously, compared to more than 20,000 people now. So, on any day I'm grappling with scale, I'm grappling with how do I have impact amid such huge scale?

The other thing that I do that is important to my role is to spend as much time as I can on the front line by going to the Telstra stores, spending a day with a field services technician, and visiting contact centres. It's useful for me to understand how Telstra's systems and processes work with the staff that are providing services to our customers. The other thing

http://doi.org/10.18080/jtde.v11n4.908

I do is spend a lot of time talking to our stakeholders: consumer representatives, charities, organisations that are supporting the type of customers that I'm worried about staying connected and understanding what the trends are that they're seeing. And then, last but by no means least, I spend a lot of time engaging with the senior leadership at Telstra to talk through what I'm seeing, what I think are really important issues that they need to be across and aware of.

[Morsillo] What have you found most difficult about the role of Chief Customer Advocate?

[Corbin] So, the scale of the business is challenging, but somebody said to me early on: don't worry so much about the complexity of the place, just focus on what you know, the small things you want to achieve and the messages you want to get across. But something I've found even more challenging, which I've had to accept, is that my role sits in tension. I'm a go-between, which means you're never going to entirely please everyone in Telstra about what you're saying and you're never going to entirely please everybody in the consumer movement. But you do have more visibility than most about the challenges and the problems that are being faced both internally and by our customers, and so the greatest challenge is turning that into a message on either side that has traction and gets outcomes. I feel like I have trust, but it's more than just trust. You have to turn that trust into outcomes and the amount of time and resources that takes from so many different people can be incredibly challenging.

[Morsillo] Is it possible to maintain an independent point of view, "holding Telstra to account", after having been a Telstra employee for a time?

[Corbin] Well, I think that that's always going to be a challenge for anybody that works in a commercial company. After all, you're an employee. So, there's been a few things when I've had to step back and think to myself: hang on, maybe there needs to be another level of independence brought to this piece. So, for example, there've been a few times when I've engaged more directly with the Telecommunications Industry Ombudsman (TIO) on an issue, because I've felt that there needed to be an extra level of oversight that I couldn't provide. And secondly, I think that it's quite important to just invite people to hold you to account and to ask you those tough questions. Even though I might not always be able to answer them, and I might not always be comfortable answering them, I think the fact that they get asked to me means that I'm continually reflecting on how independent I am being. How honest am I being? Am I giving the easy answer? I think that comes back to the point about tension. You have to continually think it's not about sending somebody away satisfied necessarily. It's about making sure that the right information is getting in front of the right people.

http://doi.org/10.18080/jtde.v11n4.908

[Morsillo] As CEO of CTN and ACCAN, you were involved in public policy debates for the telecommunications industry. Are you still able to do this in your role at Telstra?

[Corbin] Yes! In fact, I was very excited last week to participate in the submission for the draft financial hardship standard that is going to the Australian Communications and Media Authority (ACMA). Obviously, there are lots of voices in Telstra that contributed to that submission, but I was really pleased to be asked specifically as Customer Advocate what a consumer perspective might be and that led to an improved submission. So, yes is the answer.

[Morsillo] Not many consumer advocates choose to go to work on the "inside". How do you think your position is regarded by those advocating on the "outside"?

[Corbin] Well, one issue is they can't necessarily see everything that you do on the inside. There's only so much you can share. That's just the reality of working in a commercial entity. Sometimes I find that a little bit hard. But I've also been impressed with how much Telstra does share externally. More than I thought we would, but we do. I think it's OK for some consumer advocates to be unhappy about what they might perceive as what you've done, because you're taking a slightly different approach when you're a Customer Advocate. You do have to be effective in the company, which means you can't be an activist. You're there as part of the company doing the work, right? Advocates externally play their part as well. But it doesn't mean that internally you're not raising those very same issues or making sure that they are front and centre, but you're not going to necessarily be drawing lots of attention to the fact that you're doing so, because it's a different role.

[Morsillo] What are you most proud of achieving so far after these couple of years?

[Corbin] I've been working on a major report on customer vulnerability from Telstra's perspective. It covers what Telstra does and what I think the company might be able to do a bit better or a bit more of. It tries to provide a transparent, honest perspective about where Telstra is at, mistakes and all, and how some of those things have impacted customers who are in vulnerable circumstances. So, I'm very proud of that report, due to be released soon. It's a lot longer than I thought it would be, even though I probably understand more than most how much Telstra does. But what is really awesome is that the company is looking at making it a regular event, part of our suite of annual reporting, to track progress. So, there's some real accountability about what we are and aren't doing, and it will make it a lot better for consumer representatives to engage with Telstra because they can understand where the starting point is. This is a way to make sure that people will know where Telstra sits in relation to these things and hopefully it might drive better practices throughout the

http://doi.org/10.18080/jtde.v11n4.908

industry and potentially a better conversation about what is best practice. I'll be very proud of that.

Of course, there are a couple of other things that have been great, like Telstra moving to offer more flexible payment options beyond direct debit for its Upfront Plans. It might seem like a small thing, but it's quite a significant achievement. And, further, when I put the report together, I realised that there are quite a lot of things that have been improving, which you lose sight of when you're in there working on the details. So that's another reason why an annual report is a really good idea.

[Morsillo] Thank you, Teresa.

For more information, including Teresa Corbin's report, visit https://www.telstra.com.au/aboutus/community-environment/chief-customer-advocate.

http://doi.org/10.18080/jtde.v11n4.908

Rebalancing Regulation in an Era of Distrust

Telecommunications Industry Ombudsman and Developing Consumer Regulation

Cynthia Gebert
Ombudsman, Telecommunications Industry Ombudsman

Abstract: On Thursday, 21 September 2023, TelSoc hosted an online event to discuss a number of important developments involving the Telecommunications Industry Ombudsman (TIO). The first development was the continuing reduction in the number of complaints by consumers about the services provided by telecommunications operators.

The second development is that the TIO has called for a different model – direct regulation – to be adopted for regulation in the sector where it impacts consumers. This call has occurred at a time when the Telecommunications Consumer Protection Code is progressing through the approval stages. Over the past twenty-five years in Australia, the preferred approach to the development of industry codes of practice has been largely by the industry, with subsequent regulatory adoption by the ACMA. Is this model serving Australia well in the current environment?

Keywords: Telecommunications regulation, Telecommunications Industry Ombudsman, Ombudsman, Digital Platforms

Introduction

This is a transcription (lightly edited) of Cynthia Gebert's speech to TelSoc on 21 September 2023.

I acknowledge the Traditional Owners of Country throughout Australia, and recognise their enduring connection to land, water, culture and community. I pay my respects to Elders past and present, for they hold the memories, the traditions, the culture, and the hopes of First Nations People. Sovereignty has never been ceded; this always was and always will be Aboriginal land.

http://doi.org/10.18080/jtde.v11n4.900

Good morning everybody. I would like to thank TelSoc President, Jim Holmes, for inviting me to speak today. I hope I can do this subject matter justice.

I would also like to welcome my co-presenter, Dr Karen Lee, from the University of Technology Sydney. I had the pleasure of meeting Karen in November last year at a digital platforms roundtable and the first thing that struck me was how important it is to have people like Karen and other academics, who are not in the trenches of the day-to-day industry, policy and regulatory environment. They stand back, look at the bigger picture, and can talk about what the facts look like from that view. We can gain genuine insight from these facts because they are impartial and therefore can be trusted.

Our industry is changing.

Open and honest dialogue has never been more critical because, in the face of change, we will work better together if we are open and honest with one another.

Today I will discuss with you the current complaints decline, the TIO's call for direct regulation for consumer protections, and the need for a telco registration scheme with minimum entry requirements. I will also touch on what tips the TIO [Telecommunications Industry Ombudsman] can share for the development of a new digital platforms' consumer protection framework.

But, first, we need to understand why it is important for me to talk about these topics today. This means we need to talk about consumer trust and a quick delve into telco regulatory history.

Trust

In April of this year, for the first time since Roy Morgan began measuring trust and distrust in 2018, the telco industry replaced the social media industry as the most distrusted industry in the Australian economy (Roy Morgan, 2023a). And, in the 12 months to June 2023, Roy Morgan reported, two of Australia's largest telcos appeared in the top five most distrusted brands in Australia (Roy Morgan, 2023b).

When commenting on why a majority of Australians have little to no trust in telcos, Roy Morgan CEO, Michele Levine, said:

> While trust builds human connections with businesses, distrust is a more powerful driver in the decisions people make (Roy Morgan, 2022).

Ms Levine continues:

> The underlying message to consider is that increasing distrust can heavily impact commercial and economic outcomes for businesses and brands. Although trust is

http://doi.org/10.18080/jtde.v11n4.900

> important for building human connections, distrust is the bellwether for an unsustainable future… [R]isk assessments and procedures by telco executives and company directors need to formally factor-in distrust – indeed distrust should be on the risk register of every board in Australia (Roy Morgan, 2022).

According to the 2023 Edelman's Trust Barometer, the good news is businesses as a whole are seen as the institutions that are most competent and ethical. This is a powerful statement at a time when our social fabric is weakened by deepening divisions. Edelman (2023) defines the way forward for business, and I will take the three points I believe are the most relevant for us today:

1. Business should leverage its comparative advantage to inform debate and deliver solutions.
2. Business and government can build consensus and collaborate to deliver results that push us towards a more just, secure, and thriving society; and
3. Business should be a source of reliable information, promote civil discourse, and hold false information sources accountable.

If we view these three ideas as pillars, they can give our sector the aspiration and insight we so desperately need to repair the distrust of telco consumers.

Now let's go back to the past.

The TIO opened its doors in December 1993 with three members — Telecom, Optus and Vodafone — under the watchful eye of Ombudsman Warwick Smith. In our first year of operation, those three members generated 8,500 complaints, 90 per cent of which were received by phone.

New Ombudsman John Pinnock joined in early 1995 at a time of significant change.

Telstra was created on 1 July 1995 through the amalgamation of Telecom Australia and the Overseas Telecommunications Commission. In March 1996, the Federal Government announced the partial privatisation of Telstra through the sale of one-third of its equity, and the Australian telco industry was opened to full competition on 1 July 1997, with the passing of the *Telecommunications Act 1997* (Cth) and associated instruments.

The package also saw the establishment of the Australian Communications Authority (ACA) and emphasised self-regulation through industry Codes developed by the new Australian Communications Industry Forum.

The period following 1 July 1997 was one of activity and rapid growth for the TIO as it responded to the newly deregulated telecommunications market. Most new entrants were start-up Internet Service Providers (ISPs), unused to telecommunications regulation, and even opposed to the concept of alternative dispute resolution. During this time, the TIO sought

http://doi.org/10.18080/jtde.v11n4.900

to educate its new members, and was heavily involved in consultations about the new industry-developed consumer codes of practice. As complaint numbers and membership increased, so too did the number of TIO staff, which grew to 30 people in 1999.

And, on 1 July 1999, the implementation of the Telecommunications (Consumer Protection and Service Standards) Act 1999 finally made it a legal requirement for all eligible service providers, including ISPs, to comply with the requirements of the TIO scheme.

Today the TIO has nearly 200 employees and almost 1,700 members delivering over 45 million services in operation (ACMA, 2023).

Telco regulation has not experienced wholesale change since 1997, yet the world has changed exponentially, and so have consumer expectations.

It should be an easy flow chart:

- Telcos rightly care about business sustainability.
- Consumers care about their products and services being reliable and accessible.
- And Government cares about keeping constituents happy, because this keeps them in power.

Yet, despite this, the consumer protection framework has not changed, and this is incongruent with telecommunications being an essential service. External dispute resolution schemes are key parts of the consumer protection ecosystem. Without the TIO, what would regulation look like? What would complaint volumes look like? What would relationships between the community and telcos look like?

We have clever people at the TIO, passionate about fair and reasonable outcomes, but we need to keep working together with stakeholders to make sure understanding and value of the TIO's role continues to mature. Maturity looks like collaborative working relationships with an understanding that our role is to independently resolve complaints and share our insights based on what we see. Our role is also to help improve the way industry operates, so that as a sector we can restore and maintain broken community trust.

Maturity in action looks like a deeper understanding of fair and reasonable outcomes for complaints, to reduce the sometimes combative nature of the relationship of the industry with the TIO. Maturity is understanding that the telco industry and the TIO will have different perspectives on things, as we perform fundamentally different roles, but we share a genuine desire and curiosity to understand each other's perspectives.

A healthy and productive relationship between the TIO and industry is one in which we work together to improve consumer outcomes — consumers who are your customers.

http://doi.org/10.18080/jtde.v11n4.900

We need the industry to be open to sharing when things are not working, so we can help stop problems escalating and resolve systemic issues before customers are impacted. In many cases, it is possible to do this before any regulator sees a need to get involved. For telco providers, the TIO is an opportunity to improve your service delivery.

I have been in the role of Ombudsman for a year and a half now and I want to take this opportunity to acknowledge the great work being done to drive down complaints. The investment in your people, processes and technology improvements that sit behind the drop in complaints is welcomed. We know work done by industry has helped to reduce complaints, and we also know regulation has helped this along.

There is more to the story. And it is important we understand the broader context because, despite the decline, there is more work to be done.

Complaints decline and complaints landscape

The collective voices of customers who turn to Ombudsman services for dispute resolution provide a wealth of data — what they are frustrated about, what problems they are facing, and where patterns may be emerging that show a need for change. Ombudsman data can inform the way industries and government agencies improve their products and services and support moves to a more customer-centric approach. This is to the benefit of customers, but ultimately of benefit to the industries and agencies themselves.

So where are complaints today?

Over the past five years, since the heightened days of the NBN rollout, complaints to the TIO have steadily declined (TIO, 2023, p. 79).

We can attribute some of this decline to the positive efforts by the telcos and the ACMA to drive down complaints. In 2018, the ACMA introduced the Complaint Handling Standard; then, two years later in 2020, the Mobile Number Pre-Porting Identity Verification Standard. Also in 2020, 4G backup became more widely available and more telcos began offering unlimited data plans. These changes improved reliability for consumers.

In 2022, the ACMA published its Statement of Expectations, and the Customer Identity Authentication Determination came into force. Telstra brought call centres onshore, and the Reducing Scam Calls Code expanded to include Scam SMS. More recently, we have seen investments by some telcos to improve the customer experience. Outside of the telco sector, the lasting social effects of the COVID-19 pandemic and current cost-of-living crisis are being felt nationwide.

A recent report by the Consumer Policy Research Centre (CPRC, 2023) revealed consumers do not always make complaints or raise issues when something goes wrong. Twenty-eight per

http://doi.org/10.18080/jtde.v11n4.900

cent of people who were surveyed said they did not take action because they thought it was not worth the effort. The CPRC sees a link between this finding and the frustrations with customer service. Fourteen per cent of Victorians had difficulty contacting a company when something went wrong and the comments from the survey clearly show how many people are losing time when they have to chase businesses who have not done what they promised.

Closer to home for the TIO, the news is just as grim.

The CPRC report showed that **only 3 per cent** of surveyed consumers tried to resolve their problem via the relevant Ombudsman, such as the Australian Financial Complaints Authority, Energy and Water Ombudsman Victoria, or the TIO (CPRC, 2023).

Consumer reasons for not taking action? The report states twenty-eight per cent of respondents replied it was not wort the effort, and a further fourteen per cent said it was not worth the cost involved (CPRC, 2023, p. 29). Others indicated they were not confident that taking action would solve the problem, or the process was too complicated.

The CPRC (2023) is absolutely correct in its assertion that this points to a need to look at dispute resolution options for consumer issues. We need to address the perception that complaints processes will be difficult by improving the processes overall.

The TIO is not immune to the wave of consumer distrust — we have some work ahead of us to fix our part. But trust and consumer perceptions of complexity are only one part of the picture.

In July we commenced a pilot process that saw us following up on complaint referrals, a recommendation from the recent Independent Review of our scheme. The process involved an automated message being sent to consumers via text or email at the end of the referral period, once our members had an opportunity to address the consumer's issue. During this process, we saw an increase in consumers telling us their complaint remained unresolved, and they were returning to the TIO for conciliation and investigation.

We deferred the referral follow-up process in mid-August so we could review the data and the insights gathered over those six weeks, but this result poses the question — why are complaints requiring two or more pass-backs before a resolution can be found?

This result also presents challenges for telcos and the TIO to resource the additional work, if a consumer's complaint remains unresolved after initial contact.

The results we saw in the first month of this trial suggest there is a significant unmet complaint demand which needs to be addressed by our members. The time, resourcing, and associated costs to resolve a complaint at first referral is beneficial for our members and their customers. It is also a signpost that further work is needed to ensure the consumer experience remains front and centre of the complaint handling process.

http://doi.org/10.18080/jtde.v11n4.900

We do not always know the drivers of complaints to our office, but what I can say with confidence is that no matter how complex the answer, today we can deal with what we know to be true — we all need to clean up our trust problem.

As Edelman (2023) has pointed to, we need to think bigger. We need to see the customer experience through the eyes of those who use our services.

A Refreshed Regulatory Framework

I have talked about the state of play for complaints and consumer issues, and now I would like to talk about the status quo for regulation in the telco sector and what I believe needs to change.

Put simply, we need consumer protections to be set in direct regulation and we need a registration scheme with minimum entry requirements.

Since the deregulation of telco in 1997, not much has changed.

Today the telco sector operates under a co-regulatory framework and there are no barriers to entering the market. The bulk of telco-specific consumer protections are contained in the industry-made Telecommunications Consumer Protections Code, or TCP Code, which is approved by the ACMA.

The uncomfortable truth is that there is an inherent tension here. Community expectations of essential service providers have changed, but the responsibility for setting key consumer protections in telco has not. People and small businesses who complain to us tell us they view telecommunications in much the same way as they see other utilities. They make comparisons between the essential nature of utilities and the need for reliability.

Accountability and responsibility for the regulation of phone and Internet services should sit with the government and the regulator.

Why do we still have key consumer protections drafted by industry?

Why is the balance of industry-made and government-made regulation in such stark contrast with the rules for energy, water, and key elements of banking services?

There are two threads I would like to pull on to help us consider these questions. The first thread, as I flagged earlier, is there are some rules that benefit from the knowledge of industry experts. Consumers benefit from industry-made rules on technical specifications and collaborative supply-chain efforts time and time again.

The second thread is history matters; and it is worth noting again that the telco industry and framework have not had a large shakeup since 1997, yet so much has changed since then.

http://doi.org/10.18080/jtde.v11n4.900

For contrast, let us look at the banking sector. After the Hayne Royal Commission findings came out in 2017, the banking sector changed. They had lost the trust of the public and the framework had to be altered to get that trust back (Gilligan, 2018). Broadly speaking, I think it is fair to say that the banking industry has responded well to the increase of direct regulation, and consumer trust has continued to improve. As always, there is more work to be done, but generally the shake-up led to better outcomes for consumers and industry alike.

While there has been no comparable Royal Commission in the telco sector and, to be clear there, I am not suggesting there should be one, the telco sector has been touched by a Royal Commission. In 2016, the telco industry was one of the many groups tasked with responding to recommendations from the Victorian Royal Commission into Family Violence (Victoria, 2016, p. 75).

The industry undertook a number of joint activities to support consumers who had experienced family violence. In 2017, Comms Alliance, the peak telco industry body, worked with the TIO and Financial Counselling Australia to create a financial hardship guideline for telcos to better assist consumers. In 2018, the TCP Code was amended to explicitly capture family violence as a financial hardship indicator, and in that same year Comms Alliance also published a non-mandatory guideline for telcos to assist consumers experiencing family violence, a guideline that was updated earlier this year.

I may not have been the Ombudsman in the telco sector back then, but I know this work was challenging, it was demanding, and it was valuable. This work led to real tangible benefits for consumers struggling with family violence, and I thank every member of industry and Comms Alliance for their push to make those changes happen.

What we know now is those changes did not go far enough.

It was clear when my office released a systemic report in 2020 highlighting that the telco industry still needed to improve the way it helps consumers who experience family violence — two years after industry changed the TCP Code and released its guideline.

And although we applaud the work and outcomes in the updated guideline published in April this year, it remains clear key consumer protections like this should be set by government. A short time ago, the Government directed the regulator to intervene before the completion of the TCP Code review, to create an enforceable standard with minimum requirements for financial hardship assistance. This direction led by government aligns with community expectations that key consumer protections cannot be optional – they must be mandatory, and they must be enforced.

The conversation we are having today is not about misconduct. It is a conversation about complaints and trust and the right framework for an evolving telco sector. We know that

http://doi.org/10.18080/jtde.v11n4.900

consumer trust in the telco industry is low. The time is right for the balance in the co-regulatory framework to be reconsidered to help rebuild that trust.

Government should regulate the minimum standards consumers can expect.

I have come from the energy and water sector, a sector that is much more directly regulated, and I can tell you first-hand that direct regulation has benefits for consumers and industry (Energy Networks Australia, 2019).

Introducing direct regulation for key consumer protections in telco would promote consistent outcomes for consumers and guarantee a basic quality standard for all players in the market. It would bring the telco sector in line with the policy approach in other essential areas, such as energy and water.

Now, I would like to address a registration scheme with minimum entry requirements, and need for parameters around who can participate in the telco market. Unlike other essential service sectors, the telecommunications sector does not have a registration, authorisation, or licensing scheme for service providers that sell directly to consumers.

Why should just anybody be allowed to sell telco? Where is the barrier to entry? Where is the protection for consumers? Telco providers should be required to demonstrate they can satisfy the minimum capabilities required to deliver such an essential service.

Today the TIO has the most accurate list of participants in the telco sector, but it seems to me it should be the regulator who has this information.

I hope we can all agree that the telecommunications market has outgrown the policy settings that prioritised competition. The original policy intent of having no barriers to market entry and no registration requirement for providers was designed to open up competition after Telstra's privatisation in 1997 (ACCC, 1997).

Given the broad changes to product and service delivery, and very healthy competition in a marketplace of nearly 1,700 telco providers, now is the time to renew the policy settings to ensure there is proper regulation of the telecommunications market.

Under the current framework, there is no requirement for providers to demonstrate key telecommunications regulatory knowledge, or ability to follow the rules in the sector beyond an attestation process, which is not always complied with. There is no requirement to demonstrate suitable leadership, or to demonstrate organisational, technical, or financial capacity to operate in the telco market.

Telco consumers should not be used as test subjects for the viability or profitability of a business. While we do encounter unprepared providers that strive to do better, consumers should not be subject to providers who lack the knowledge and ability to deliver an essential

http://doi.org/10.18080/jtde.v11n4.900

service. Introducing a registration scheme with minimum entry requirements would go some of the way towards rebuilding trust with consumers, knowing their telco has had rigour applied to their right to trade in the Australian communications market.

I have covered a lot of ground about the telco sector — where we have been, where we are, and what needs to change.

So, if we could start again, what would we do differently?

The Lessons Telco Can Offer to Digital Platforms

As the government and the ACCC look to the future of digital platforms regulation, there is a lot that can be learned from the telco sector. Dr Karen Lee and the team at UTS are in the enviable position of exploring a new regulatory framework that touches so many people. Much like we are with phone and Internet, the vast majority of Australians are intrinsically locked into a relationship with digital platforms.

What can telecommunications offer to digital platforms by way of lessons learned?

Both are sectors that have transformed the way we live at a greater pace than could have been imagined by policy makers. The Digital Platforms Inquiry that is happening right now will precede a new framework, much like what happened in the banking sector. We have a unique opportunity as the thought leaders and experienced captains of industry to set the right course.

Whether or not you respect the role of the TIO in helping your business resolve complaints with your customers, the first lesson we can share is that we know the industry-based Ombudsman model works. This is comprised of effective internal dispute resolution as a first step, followed by external dispute resolution when the provider and the consumer cannot solve the problem.

This is a well-established and time-tested complaint handling framework, further strengthened in 2018 with the addition of the Complaints Handling Standard. This direct regulation provides clear minimum standards for complaint processes, timeframes, and accessibility for consumers, and creates positive outcomes for providers. The Ombudsman model has consistently been endorsed by Government and independent reviews as being in the best interest of consumers. It has also been proven that the Ombudsman model is most effective when internal dispute resolution processes are mandatory and regulated.

The internal dispute resolution framework is a precursor to external dispute resolution. To this point, a real pathway for consumers to make complaints can be prioritised. The government does not have to wait for the ACCC to finish its Digital Platforms Inquiry in 2025, and neither do digital platforms. I am on the record as saying I recommend that digital

http://doi.org/10.18080/jtde.v11n4.900

platforms get started today on improving their internal dispute resolution processes. This is a first step towards consumers having access to the dispute resolution processes that are missing and sorely needed.

The second lesson we can share is we need to ensure adequate consumer protections are in place as part of a regulatory framework.

Through complaints to my office, we see that it is vulnerable consumers who are impacted the most by inadequate consumer protections. We see complaints about poor selling practices, we see a lack of proactive and early support for consumers experiencing payment difficulties, and a lack of choice around payment methods. And we see telco consumers impacted by inaccessible communication channels and complaint pathways.

In her presentation to the United Nations Conference on Trade and Development, Dr Christine Riefa spoke about the protection of vulnerable consumers in the digital age (Riefa, 2020). She pointed out targeted vulnerable-consumer protections are needed, because disengaged consumers in digital markets can become even more vulnerable after being subject to unfair treatment (Riefa, 2020).

In the digital platform space, the ACCC has reported several times that unfair treatment includes pressuring consumers to agree to confusing privacy policies (ACCC, 2023). Unfair treatment also includes designing user experiences that push consumers to make decisions they do not fully understand.

In this type of unbalanced market, it is critical we get the balance of regulation right. The digital platform space could get the balance of co-regulation right from the outset.

And the third lesson we can share is there must be clarity and simplicity in jurisdiction.

It is vital that all parties with a role in the digital platforms consumer protection framework come together and establish who does what, with appropriate escalation pathways. It needs to be clear which external dispute resolution bodies each platform must engage with and for which complaints. Consumer protection rules should be in place, so it is clear to complaint handlers what rules to factor in in deciding what is fair and reasonable.

Having ready and willing players in the dispute resolution landscape is great, but it means little without clear legislative backing. Without clear legislative backing, the cracks consumers are falling through cannot be properly sealed — and new cracks could even be created.

Conclusion

In conclusion, today's market is complex, and its consumers even more so. The demand for change is getting louder and more pressing as telco and digital platforms irrevocably converge.

http://doi.org/10.18080/jtde.v11n4.900

But this year's Edelman survey results provide some guidance for us as a sector to start rebuilding trust.

We should leverage our comparative advantage to inform debate and deliver solutions. Let us build consensus where we can and collaborate to deliver results that push us towards a more just, secure, and thriving society.

I cannot encourage the telco sector enough to keep its door open to the TIO. Together we can rebuild consumer trust and drive complaints down even further than today's levels.

We will not always agree, and we may just agree to disagree, but we all have a role to play and we can play that role best if we work together.

References

ACCC. (1997). Australian Competition and Consumer Commission. 1997. Deregulation and its Effect on the Market. Available from https://www.accc.gov.au/system/files/Deregulation%20and%20its%20Effect%20on%20the%20Market.pdf, retrieved 5 September, 2023.

ACCC. (2023). Australian Competition and Consumer Commission. 2023. Digital platform services inquiry 2020-25. [Internet]. Australian Government. Accessed 6 September 2023. Available from https://www.accc.gov.au/inquiries-and-consultations/digital-platform-services-inquiry-2020-25

ACMA. (2022). Australian Communications and Media Authority Statement of Expectations 2022, at https://www.infrastructure.gov.au/sites/default/files/documents/acma-statement-of-expectations-2022.pdf

ACMA. (2023). Australian Communications and Media Authority. 2023. Telco complaints-handling performance. [Internet]. Australian Government. Accessed 6 September 2023. Available from https://www.acma.gov.au/publications/2022-10/report/telco-complaints-handling-performance

Consumer Policy Research Centre. (2023). Victorian Consumer Survey: Problems, complaints and resolutions. https://cprc.org.au/vic-consumers/, retrieved 6 September 2023.

Edelman. (2023). 2023 Edelman Trust Barometer: Navigating a polarized world. [Internet]. Edelman. Accessed 6 September 2023. Available from https://www.edelman.com/trust/2023/trust-barometer

Energy Networks Australia. (2019). Rewarding Performance: How customers benefit from incentive-based regulation. Available from https://www.energynetworks.com.au/resources/reports/rewarding-performance-how-customers-benefit-from-incentive-based-regulation/, retrieved 6 September, 2023.

Gilligan, G. (2018). The Hayne Royal Commission and Trust Issues in the Regulation of the Australian Financial Sector. *Law and Financial Markets Review*, *12*(4), 175–185. Accessed 6 September 2023. http://dx.doi.org/10.2139/ssrn.3360183

Riefa, C. (2020). The protection of vulnerable consumers in the digital age. Eleventh Meeting of the UNCTAD Research Partnership Platform, London. Available from

https://unctad.org/system/files/non-official-document/ccpb_RPP_2020_05_Present_Christina_Riefa.pdf

Roy Morgan. (2022). A majority of Australians have no trust in telcos. [Internet]. Roy Morgan Research. Accessed 6 September 2023. Available from https://www.roymorgan.com/findings/a-majority-of-australians-have-no-trust-in-telcos

Roy Morgan. (2023a). Telecommunications industry overtakes Social Media as the most distrusted industry. [Internet]. Roy Morgan Research. Accessed 6 September 2023. Available from https://www.roymorgan.com/findings/9193-risk-monitor-telco-most-distrusted-industry-2023

Roy Morgan. (2023b). Distrust after data breaches lingers for months. [Internet]. Roy Morgan Research. Accessed 6 September 2023. Available from https://www.roymorgan.com/findings/9306-risk-monitor-quartely-update-june-2023

Telecommunications (Consumer Complaints Handling) Industry Standard 2018, at https://www.legislation.gov.au/Details/F2021C00265

Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020, at https://www.legislation.gov.au/Details/F2020L00179

TIO. (2023). Telecommunications Industry Ombudsman. 2023. Annual Report 2022-23: Transformation through innovation. Available from https://www.tio.com.au/sites/default/files/2023-10/TIO_2022-23%20Annual%20Report_fa.pdf, retrieved 6 September, 2023.

Telecommunications Service Provider (Customer Identity Authentication) Determination 2022, at https://www.legislation.gov.au/Details/F2022L00548

Victoria, State of. (2016). Royal Commission into Family Violence: Summary and recommendations. Parliament Paper No 132. Available from http://rcfv.archive.royalcommission.vic.gov.au/MediaLibraries/RCFamilyViolence/Reports/RCFV_Full_Report_Interactive.pdf, retrieved 6 September, 2023.

http://doi.org/10.18080/jtde.v11n4.900

Digital Transformation, Social Innovation and the Not-For-Profit Sector in Australia

Invitation to Correspond

Robert Morsillo
ARC Centre of Excellence for Automated Decision Making & Society,
RMIT University, Melbourne, Australia

Abstract: Digital transformation also includes the potential and practice of digital *social* innovation, whereby the affordances of digital technologies are used to address contemporary social issues. This is particularly relevant to the not-for-profit sector, which plays an important role in Australian society delivering community services. There is a growing appreciation of the ability of this sector to innovate, given its closeness to grass-roots social issues, its flexibility, and capacity to recruit staff and volunteers from all walks of life to contribute to its operations. The sector often operates in-between and in-connection-with government and business, and such collaboration with diverse viewpoints can also be a stimulus for innovation. However, various constraints have been identified, such as the lagging digital proficiency of the sector and its workforce, and the general standoff between purpose, profit and regulatory motivations. The relationship between modern technologies and social innovation by the not-for-profit sector is of national policy interest and worthy of investigation into its originality, opportunities and obstacles. From this brief discussion article, the author invites interested readers to correspond and contribute to this research project.

Keywords: not-for-profit sector, digital social innovation, digital transformation, collaboration, research

Introduction

Telecommunications is regarded by consumers and the regulators as an essential service in Australia today (cf. Consumer Action Law Centre, 2022; Australian Communications and Media Authority, 2023). It underpins access to education, health, employment and social welfare services. It supports our personal wellbeing by assisting us to navigate multiple relationships and connect with others.

http://doi.org/10.18080/jtde.v11n4.892

However, in the aftermath of COVID-19 and with other recent economic shocks such as significant increases in mortgage interest rates and energy prices, managing the cost of living is front-of-mind for many Australians. In these circumstances, "people living in poverty, disadvantage and hardship increasingly seeking help with the essentials of life" and turn to community welfare services for assistance (Cortis & Blaxland, 2022). A significant indicator of this economic stress is that searches on the Ask Izzy website were at a record high in February 2023, the top three categories being hardship, emergency food relief, and mental health and wellbeing services (Infoxchange Australia, 2023).

Ask Izzy (AskIzzy.org.au) is a mobile-friendly web portal that provides a searchable database of over 400 000 support services across Australia and can direct users to their nearest facility. It is but one outstanding example of Australian social innovation by a not-for-profit organisation using the affordances of the digital economy to help people and social service providers to navigate available support services and to upscale access to anyone with a rudimentary online connection. It is also an example of innovation through collaboration with government and business sectors, who have contributed to its development and accessibility.

Social Innovation Going Digital

Concepts of social innovation have been traced back to the early 19th century, pre-dating that of technological innovation (Godin, 2012). However, the term has only more recently come to prominence and been subjected to analysis and theorising (cf., Mulgan, 2006; Pol & Ville, 2009; Howaldt & Schwarz, 2010). Defining social innovation can be problematic, since it might encompass a very wide range of actors, activities and outcomes. However, it is often differentiated from technological innovation and business or commercial innovation, since its primary focus is on social outcomes. Mulgan goes so far as to define social innovation in conjunction with social purpose organisations: "'innovative activities and services that are motivated by the goal of meeting a social need and that are predominantly developed and diffused through organisations whose primary purposes are social" (Mulgan, 2007, p. 8). The example of Ask Izzy above fits this definition well.

Digital social innovation is a more recent concept relating to the use of digital technologies for the purpose of social innovation (Rodrigo *et al.*, 2019). The affordances of online and digital technologies are primarily used to create a social or environmental benefit (cf., Morsillo, 2011). In a 2019 keynote, *Social Innovation: Where Next?*, Mulgan suggested that digital social innovation, data and artificial intelligence, and corporate social innovation were growing themes (Mulgan, 2019). For example, there is great interest today in the use of data analytics by the not-for-profit sector for public good (Farmer *et al.*, 2023). The development of a Digital Social Innovation Index for Europe highlights such contemporary interest (Bone *et al.*, 2018).

http://doi.org/10.18080/jtde.v11n4.892

Again, the example of Ask Izzy in Australia fits these conceptions of digital social innovation very well.

The Relevance of the Not-For-Profit Sector

The not-for-profit sector plays an important role in Australian society, particularly in delivering community support services. McKinsey & Company reported that: "this mission-driven sector is critical to meeting fundamental societal needs and fostering social cohesion. It is also an important part of the economy, employing 1.38 million people—11 percent of jobs in Australia—and contributing an estimated AU$129 billion, or 4.8 percent, of the country's gross value added in direct and indirect contributions" (Dillon *et al.*, 2021, p. 3).

Considerable philanthropic contributions support digital social innovation in Australia: for example, the Telstra Foundation, "Our purpose is to enable social change through technology, and we have been helping non-profits improve their impact for over two decades" (Telstra Foundation, 2023); Google, "We connect innovative nonprofits, social enterprises, and civic entities with Google's resources to help solve complex human challenges" (Google, 2023); Optus Future Makers, "Empowering social innovators to change the world. A capacity building and accelerator program for social start-ups that are using technology for good" (Optus, 2023); and the auDA Foundation providing grants for "educational and research activities that will enhance the utility of the internet for the benefit of the Australian community" (auDA Foundation, 2023).

Not-for-profit organisations are often involved in co-creation efforts and act as partners to sustainability or social responsibility efforts by corporate Australia: for example, the ANZ Bank's MoneyMinded financial literacy education program in partnership with Berry Street, Brotherhood of St Laurence and The Smith Family (ANZ Bank, 2020); and The Telstra Top-Up pre-paid mobile credit program in partnership with Infoxchange Australia (Infoxchange Australia, 2020).

However, various constraints to innovation have been identified in the not-for-profit sector in Australia. In particular, "the sector lags behind on the adoption of ICT" (Australian Government Productivity Commission, 2010, p. 230). In their annual survey of not-for-profit organisations, Infoxchange found that the COVID-19 pandemic had been a catalyst for the uptake of basic information technology systems, such as cloud applications; however, there is still a long way to go and "[b]uilding the digital capability of staff is now the number one priority for organisations" (Infoxchange *et al.*, 2022, p. 4). The current consultation on a *Not-for-profit Sector Development Blueprint*, a recent Government initiative, explicitly asks: "What standards of digital capability should the sector aim for and how might these be achieved" (Blueprint Expert Reference Group, 2023, p. 33).

http://doi.org/10.18080/jtde.v11n4.892

Conclusion

As businesses and government increasingly focus on technology for productivity or efficiency outcomes, how well-placed are Australian not-for-profits to utilise technology to pursue their primary purposes? Is there a compelling rationale for the greater use of technology by not-for-profits in their traditional role of strengthening civil society? What capabilities are needed to maximise participation in new digital service provision opportunities? Digital social innovation among Australian not-for-profit organisations is an emergent activity and worthy of investigation to better understand its originality, opportunities and obstacles, and the transformations it is engendering for the sector and its constituencies. Readers with an interest in this area of research are invited to correspond with the author.

Acknowledgements

My interest in digital social innovation in Australia grew out of a previous investigation into new uses of online technologies by not-for-profit organisations, which was presented as a paper to the 2011 Communications Policy & Research Forum, Sydney, Australia (Morsillo, 2011). This current research is supported by an Australian Government Research Training Program (RTP) Scholarship.

Corresponding author

Robert Morsillo, HDR student, ARC Centre of Excellence for Automated Decision Making & Society, RMIT University, Melbourne, Victoria, Australia. https://orcid.org/0009-0000-8366-7705. Email: s8310559[at]student.rmit.edu.au.

References

ANZ Bank. (2020). MoneyMinded. https://moneyminded.com.au/

auDA Foundation. (2023). auDA Foundation. http://audafoundation.org.au

Australian Communications and Media Authority. (2023). Financial hardship in the telco sector: Keeping the customer connected. https://www.acma.gov.au/sites/default/files/2023-04/Financial%20hardship%20in%20the%20telco%20sector_Keeping%20the%20customer%20connected.pdf

Australian Government Productivity Commission. (2010). Contribution of the Not-for-Profit Sector. https://www.pc.gov.au/inquiries/completed/not-for-profit/report

Blueprint Expert Reference Group. (2023). Not-for-Profit Sector Development Blueprint Issues Paper. https://engage.dss.gov.au/blueprint-expert-reference-group-developing-a-not-for-profit-sector-development-blueprint/

Bone, J., Cretu, C., & Stokes, M. (2018). A theoretical framework for the DSI index. European Commission. https://media.nesta.org.uk/documents/7-A_theoretical_framework_for_the_DSI_index.pdf

Consumer Action Law Centre. (2022, May 24). Telcos are an essential service and must step up to help customers in need. https://consumeraction.org.au/telcos-are-an-essential-service-and-must-step-up-to-help-customers-in-need/

Cortis, N., & Blaxland, M. (2022). Helping people in need during a cost-of-living crisis: Findings from the Australian Community Sector Survey. ACOSS. https://www.acoss.org.au/helping-people-in-need-during-a-cost-of-living-crisis-findings-from-the-australian-community-sector-survey/

Dillon, R., Brown, E., Carmichael, A., Radford, P., Agrawal, P., & Fletcher, B. (2021). Building from purpose: Unlocking the power of Australia's not-for-profit sector. McKinsey & Company. https://www.mckinsey.com/au/our-insights/building-from-purpose-unlocking-the-power-of-australias-not-for-profit-sector

Farmer, J., McCosker, A., Albury, K., & Aryani, A. (2023). *Data for Social Good: Non-Profit Sector Data Projects*. Palgrave MacMillan. https://doi.org/10.1007/978-981-19-5554-9

Godin, B. (2012). Social Innovation: Utopias of Innovation from c.1830 to the Present. *Project on the Intellectual History of Innovation Working Paper 11*, 1–5. http://www.csiic.ca/PDF/SocialInnovation_2012.pdf

Google. (2023). *Philanthropic Initiatives For Local Communities—Google.org*. https://www.google.org/our-work/

Howaldt, J., & Schwarz, M. (2010). *Social Innovation: Concepts, research fields and international trends*. Sozialforschungsstelle Dortmund.

Infoxchange Australia. (2020, July 6). Telstra Top Up. Infoxchange. https://www.infoxchange.org/au/community-programs/telstra-top-up

Infoxchange Australia. (2023, March 22). Number of People Searching for Food Keeps Growing. Infoxchange. https://www.infoxchange.org/au/news/2023/03/number-people-searching-food-keeps-growing

Infoxchange, Connecting Up, & Techsoup New Zealand. (2022). Digital Technology in the Not-For-Profit Sector. https://www.infoxchange.org/au/digital-technology-not-for-profit-sector

Morsillo, R. (2011). Purpose driven productivity: Digital case studies in social innovation. In Franco Papandrea & Mark Armstrong (Eds.), *Record of the 2011 Communications Policy & Research Forum* (pp. 309–323). Network Insight Institute. https://apo.org.au/node/69336

Mulgan, G. (2006). The process of social innovation. *Innovations (MIT Press)*, *1*(2), 145–162. https://doi.org/10.1162/itgg.2006.1.2.145

Mulgan, G. (2007). *Social Innovation: What it is, why it matters, and how it can be accelerated*. Oxford Said Business School. https://www.youngfoundation.org/wp-content/uploads/2012/10/Social-Innovation-what-it-is-why-it-matters-how-it-can-be-accelerated-March-2007.pdf

Mulgan, G. (2019, October 28). *Social innovation: Where next?* ESSI, Dortmund. https://www.essi-net.eu/wp-content/uploads/2019/11/Mulgan_28Oct2019_Keynote.pdf

Optus, S. (2023). *Future Makers | Optus*. https://www.optus.com.au/about/sustainability/community/future-makers

Pol, E., & Ville, S. (2009). Social innovation: Buzz word or enduring term? *The Journal of Socio-Economics*, *38*, 878–885.

Rodrigo, L., Palacios, M., & Ortiz-Marcos, I. (2019). Digital Social Innovation: Analysis of the conceptualization process and definition proposal. *Dirección y Organización*, *67*, 59–66. https://doi.org/10.37610/dyo.v0i67.545

Telstra Foundation. (2023). Telstra Foundation. https://www.telstra.com.au/aboutus/telstra-foundation

AI Chatbot Innovation – Leading toward Consumer Satisfaction, Electronic Word of Mouth and Continuous Intention in Online Shopping

Asad Hassan Butt
Department of Marketing, Faculty of Business Administration, University of Tabuk, Tabuk, Saudi Arabia

Hassan Ahmad
Business School, Liaoning University, Shenyang, PR China

Abstract: AI-powered chatbots have emerged as influential tools in the realm of online shopping, effectively driving digital users toward heightened satisfaction, sustained usage intention and positive electronic word of mouth (e-WOM). This research delves deep into the intricate behavioural dynamics that consumers exhibit in their interactions with AI chatbots. A comprehensive online survey, encompassing 554 respondents who willingly engaged with AI chatbots, was conducted, with a focus on established frameworks like the information systems success (ISS) model, the technology acceptance model (TAM), engagement, and the elicitation of pleasurable feelings. The study's findings underscore the pivotal role AI chatbots play in elevating user satisfaction and, in turn, predicting positive outcomes. These insights hold immense value for brand managers, offering a nuanced understanding of Indian online shoppers' behaviour. Furthermore, the study highlights the significant impact of e-WOM generated by AI chatbots within the online shopping domain, further solidifying their role as essential components of digital services in the contemporary landscape. As digital services continue to shape and define modern business operations, AI chatbots have emerged as critical facilitators in enhancing the satisfaction of digital users, making them indispensable for businesses seeking to thrive in the digital realm.

Keywords: AI chatbots, perceived enjoyment, perceived usefulness, ISS model, e-WOM

Introduction

Artificial intelligence (AI) has brought about transformative changes in how organisations operate and engage with their digital era customers (Jeon, 2018; Letheren *et al.*, 2020). One

http://doi.org/10.18080/jtde.v11n4.735

significant shift is evident in the realm of service systems, where AI-powered chatbots (Gkinko *et al.*, 2022; Prentice *et al.*, 2020) have revolutionised interactions between customers and businesses. It is essential to distinguish these chatbots from robotic automation processes (RBAs) (Hill *et al.*, 2015; Saboo *et al.*, 2016; Willcocks *et al.*, 2017). While RBAs respond to specific queries, AI chatbots exhibit adaptability, tailoring their responses to meet the ever-evolving needs and desires of customers. Across diverse industries, the implementation of AI chatbots has become a common strategy for catering to end users. These chatbots facilitate human–machine conversations through natural language (Sands *et al.*, 2020; Yu *et al.*, 2022). By harnessing AI tools, businesses can engage consumers and perform various tasks through machine learning (Araujo, 2018; Butt, Ahmad, Goraya *et al.*, 2021). In their roles, chatbots offer rapid responses sought by users and foster robust relationships between users and organisations (Chung *et al.*, 2018; Dwivedi *et al.*, 2021; Lin, 2015). AI conversational chatbots bring substantial value to both organisations and users by providing informative and entertaining interactions (Araujo, 2018; Radziwill *et al.*, 2017; Siala *et al.*, 2022).

Much research is available on the adoption of or intention to use chatbots (Ashfaq *et al.*, 2020; Przegalinska *et al.*, 2019); however, many companies are hesitant to implement such technologies because some consumers do not feel comfortable engaging with machines (Nguyen *et al.*, 2019; Willems *et al.*, 2019). But technology is available to make life more convenient regarding shopping (Butt, Ahmad, Muzaffar *et al.*, 2021; Chung *et al.*, 2018) and other services such as job applications (Collins *et al.*, 2021; van Esch *et al.*, 2020). Hence, it is assumed that AI chatbots will be engaged in the future to provide better services to the end user (Fotheringham *et al.*, 2022; Whitler, 2016; Y. Wang *et al.*, 2021). The research explains that AI chatbots prove helpful in enhancing usefulness and satisfaction (Ashfaq *et al.*, 2020). It is also stated that AI chatbots can engage customer and brand relationships and improve customer satisfaction (Chung *et al.*, 2018; Kubo, 2013). The benefits received after the use of technology helps the user to comprehend the experience involved with it (Fagan *et al.*, 2012; Wang, Butt, Zhang, Shafique *et al.*, 2021). Further, AI chatbots can also predict positive attitudes, satisfaction and intention to use such e-services (Adam *et al.*, 2020; Araújo & Casais, 2020; Xuequn Wang *et al.*, 2022). We understand that, with AI chatbots, the higher the engagement, the higher the consumers' satisfaction levels are. The potential of AI chatbots is limitless as they can perform according to a situation. Hence, organisations can engage human–chatbot interaction while increasing satisfaction and electronic word of mouth (e-WOM).

Studying AI chatbots within the context of Indian consumer behaviour in online shopping is of paramount importance. India's e-commerce sector has experienced exponential growth, making it crucial to understand how AI chatbots impact this expanding market. These virtual

http://doi.org/10.18080/jtde.v11n4.735

assistants have the potential to engage customers around the clock, offering personalised recommendations and cost-effective support. The current study focuses on understanding customer engagement using AI chatbots while online shopping. Hence, the study highlights the following research questions (RQs) — RQ1: Will consumers be satisfied with AI chatbots? And RQ2: Will AI chatbots help organisations attain positive e-WOM and continuous intention towards it (CINT)? The RQs addressed here will be answered by the results of this study. The studies on AI chatbots need to further focus on consumers' behavioural aspects and how to help organisations grow. There are many studies on AI chatbots, but more are required to understand the gap between consumer behaviour and AI technology regarding chatbots for online shopping. The satisfaction, CINT and e-WOM effects need to be better understood, and the current study will try to bridge this gap in light of previous knowledgeable studies. The present research framework will highlight the technology acceptance model (TAM), information systems success (ISS), AI chatbot engagement, AI chatbot satisfaction, attitudes, e-WOM, CINT and perceived enjoyment toward using AI chatbots. Large organisations such as WeChat, Amazon, Skype, Facebook, and eBay are already using AI chatbot services to cater to end-users' needs (Luo *et al.*, 2019; Stevens *et al.*, 2020). The future of chatbots is promising because of their functions due to AI tools (Ciechanowski *et al.*, 2019; Gupta *et al.*, 2020; Przegalinska *et al.*, 2019).

Investigating AI chatbots' influence can uncover insights into enhancing customer engagement, tailoring services to diverse cultural preferences, and improving trust and security perceptions in a country where online fraud concerns persist. Furthermore, analysing customer interactions with AI chatbots can provide invaluable feedback, illuminate emerging trends, and bolster competitive advantages in this dynamic and evolving marketplace. As India's online shopping landscape continues to evolve, research on AI chatbots can guide businesses in effectively navigating this promising terrain and to stay attuned to the shifting preferences and behaviours of Indian consumers. In the realm of comprehending CINT with AI chatbots, two robust indicators emerge: satisfaction and attitude (Ashfaq *et al.*, 2020; Butt *et al.*, 2023). Thus, in the pursuit of unravelling the ongoing intent of AI chatbot users and their e-WOM, it becomes imperative to explore their antecedents – satisfaction, attitude and engagement – in the context of the TAM and ISS theories. These theories, when juxtaposed with various AI-related variables, serve as the vital link, addressing the void elucidated in this study. These theories used with other AI aspect variables will also bridge this gap. The provision of superior service fosters brand loyalty, consequently nurturing positive e-WOM and satisfaction (Park & Lee, 2008). Attitude stands as another influential factor, exerting a strong influence on end-users' satisfaction with innovative technologies (Han *et al.*, 2014).

http://doi.org/10.18080/jtde.v11n4.735

Recent studies have shown that enjoyment is another essential factor in AI tools for satisfaction and CINT (Ashfaq *et al.*, 2020; Pillai *et al.*, 2020; Wang, Butt, Zhang, Ahmad *et al.*, 2021). Thus, the interplay of enjoyment and attitude takes centre stage, illuminating AI chatbot engagement as formidable predictors in shaping CINT and satisfaction within the realm of online shopping. The current study using ISS, TAM and other consumer behaviour aspects will bridge the gap, i.e., the AI relationship with consumer behaviour. The research framework focuses on understanding satisfaction effects on CINT and e-WOM of AI chatbot services in the shopping context. The study will help managers develop better consumer strategies regarding AI chatbots for shopping online. The higher quality of information and services will help consumers' satisfaction increase, which could lead to CINT and e-WOM (Ashfaq *et al.*, 2020; Kim *et al.*, 2018). The following parts of this study include the Literature Review, Methodology, Research Analysis, Discussion and Conclusion.

Research Framework and Hypothesis

AI chatbots – information systems success – (ISS)

The ISS model's information and service quality metrics were proposed by Delone *et al.* (2003). The ISS model predicts customer satisfaction with using technology; so it is vital to understand its information and service quality (DeLone *et al.*, 2016; Freeze *et al.*, 2019). A timely, accurate response to the end-user's needs and wants is considered to be information quality (Chung *et al.*, 2018; Yeoh *et al.*, 2016). Hence, we can predict that the AI chatbot's information quality (AIIQ) is paramount in e-commerce. AIIQ can predict the end-user's behaviour toward the CINT of AI-enabled chatbot services. Consumers require time and information to buy a product online, and the ISS model predicts users' behaviour toward technology usage (Santos, 2011; Yeoh *et al.*, 2010). AIIQ can provide such information accurately and quickly respond to satisfy the end user. It is stated that information quality is a critical component in services because it facilitates better-informed decisions (Adam *et al.*, 2020; Sharma *et al.*, 2019). Precise and relevant information can enhance an AI chatbot user's satisfaction.

The ISS model characterises service quality as the provision of timely responses to enquiries with a focus on individualised attention, thereby enhancing the satisfaction of end users (Kallweit *et al.*, 2014; Williams *et al.*, 2022). It is equally imperative to gain insight into consumer satisfaction and the sustained use of technology (Peng *et al.*, 2022; Setia *et al.*, 2013). AI chatbot service quality (AISQ) can predict consumers' positive behaviour toward satisfaction and its CINT. AISQ can also help organisations develop better end-user services through AI tools. Additionally, an organisation's strong reputation serves as a predictor of superior service, contributing to consumer satisfaction and continued intention (Sung *et al.*,

http://doi.org/10.18080/jtde.v11n4.735

2021; Veeramootoo *et al.*, 2018). Robust chatbot platforms designed to cater to consumers' needs and desires emerge as reliable predictors of both satisfaction and CINT. Service systems characterised by rapid responses and user-friendly interfaces play a pivotal role in cultivating trust in an organisation (Gao *et al.*, 2017; Kumar *et al.*, 2016; Leung *et al.*, 2022). Hence, it is reasonable to infer that AISQ holds the potential to assist organisations in crafting engaging human–computer interaction services within the domain of online shopping. We propose the following:

H1a: AIIQ positively influences AI chatbot satisfaction;

H1b: AISQ positively influences AI chatbot satisfaction.

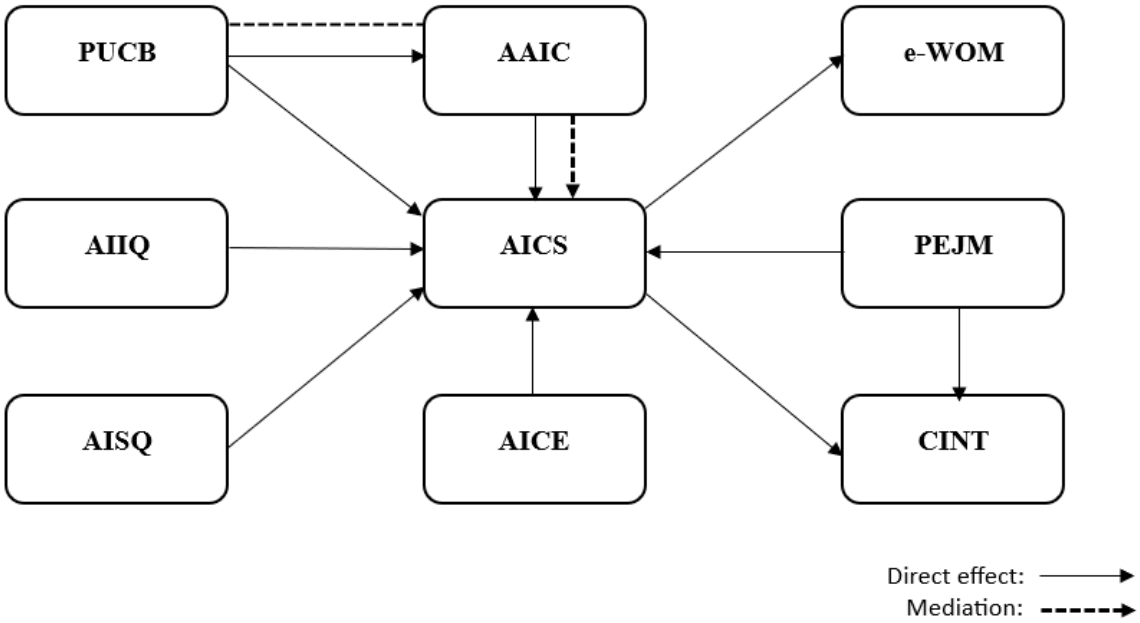
AI chatbot perceived usefulness (PUCB)

The technology acceptance model is well known among academicians and practitioners when discussing new technology. TAM dimensions of perceived ease of use and perceived usefulness (PUCB) are critical predictors in adopting technology services (Koul *et al.*, 2018; Manis *et al.*, 2019; Scherer *et al.*, 2019). The current study focuses on understanding the usefulness of AI chatbots in online shopping. The usefulness of technology is considered a benefit that can enhance the end user's experience (Amin *et al.*, 2014; Kawakami *et al.*, 2013; Tao *et al.*, 2018). PUCB has been used in previous studies as a strong predictor for understanding the satisfaction and CINT of a technology (Kapoor *et al.*, 2014; Manis *et al.*, 2019; Sánchez-Prieto *et al.*, 2017). Further, the dimensions of TAM predict a positive attitude toward the use of technology (J. B. Kim, 2012; Milberg *et al.*, 2021; Olsson *et al.*, 2013). Positive attitudes can also predict strong foundations for satisfaction (Ahmad *et al.*, 2022; Quet *et al.*, 2014; Suh & Youjae, 2006). Hence, PUCB can highlight the positive usage of AI chatbots in an online shopping context that may help organisations develop better strategies. The usefulness of technology can enhance the customer's satisfaction levels, leading to positive e-WOM and CINT. The use of AI chatbots in online shopping may improve such aspects. Figure 1 represents the conceptual framework of this study. It provides an overview of TAM and ISS theory impact on AI chatbot satisfaction. Attitude, enjoyment and engagement of AI chatbots also impact on satisfaction. We further assume that satisfaction of AI chatbots will have a positive impact on e-WOM and CINT to use such AI chatbot services. We propose the following:

H2a: PUCB positively influences attitude toward AI chatbots;

H2b: PUCB of AI chatbots positively influences AI chatbot satisfaction.

http://doi.org/10.18080/jtde.v11n4.735



Note: PUCB: Perceived usefulness of AI chatbot, **AIIQ**: AI chatbot information quality, **AISQ**: AI chatbot service quality, **AAIC**: Attitude towards AI chatbots, **AICE**: AI chatbot engagement, **AICS**: AI chatbot satisfaction, **PEJM**: Perceived enjoyment, **e-WOM**: Electronic word of mouth, **CINT**: Continuous intention

Figure 1. Conceptual framework

Attitude toward AI chatbots (AAIC)

Attitude is an individual's belief about a particular product or someone that may be favourable or unfavourable (Ajzen, 1991, 2001; Cheng *et al.*, 2021). A positive attitude can enhance consumers' satisfaction (Chou *et al.*, 2020; Suh & Youjae, 2006; X. Wang, M. J. Haque, *et al.*, 2021). Previous studies have focused on understanding the attitude's effect on satisfaction (Chiu *et al.*, 2021; Kissi *et al.*, 2020; Ye *et al.*, 2017). Hence, attitudes toward AI chatbots (AAIC) can enhance customer satisfaction. AAIC will further provide positive aspects of the behaviour of consumers in the online shopping context. It is further predicted that AAIC will positively mediate PUCB and AI chatbot satisfaction. As we have indicated, attitude positively impacts satisfaction and CINT (Cronin, 2010; Han *et al.*, 2014; Spielmann *et al.*, 2018). We can assume that AAIC will also play a positive role in direct and mediating effects. We propose the following:

H3a: AIIC positively influences AI chatbot satisfaction

H3b: AIIC mediates the relationship between the PUCB and AI chatbot satisfaction

AI chatbot engagement (AICE)

Technology engagement can also enhance consumers' satisfaction (Kang, 2019; Kosiba *et al.*, 2018). Brands are implementing tech-savvy strategies to attract customers. Novel technologies such as AI can impact on consumer satisfaction and loyalty toward the brand

http://doi.org/10.18080/jtde.v11n4.735

(Barry *et al.*, 2018; Gulati, 2019; Yusuf *et al.*, 2018). The engagement concept helps consumers develop positive beliefs about brand loyalty, awareness and satisfaction (Baker *et al.*, 2010; Jiménez-Barreto *et al.*, 2021; Van Doorn *et al.*, 2010). The use of AI chatbot engagement (AICE) in the current study will help us understand consumer behaviour toward such innovative technologies in online shopping. The engagement involves the customer's cognitive, emotional and behavioural aspects of brand loyalty and satisfaction (Bryce *et al.*, 2015; McLean *et al.*, 2019; Mende *et al.*, 2020). Engaging behaviour can lead to positive outcomes for consumers and the organisation (Tarute *et al.*, 2017). Hence, we can assume from the previous studies that the AICE may play a significant role in understanding the consumer's satisfaction with chatbots while shopping. A consumer's engagement with a brand's services leads to satisfaction and CINT (Du Plessis *et al.*, 2010; Hu *et al.*, 2021; Moriuchi, 2019). Therefore, the current research study of AICE will also provide the same valuable results as previous studies. We propose the following:

H4: AICE positively influences AI chatbot satisfaction.

AI chatbot satisfaction (AICS)

Previous studies have highlighted satisfaction as a strong predictor of CINT (Wu *et al.*, 2016) and e-WOM (Peddibhotla *et al.*, 2007; Suh & Wagner, 2017). Satisfaction for a consumer can include price, usefulness or benefit, time and other factors that can enhance their experience and expertise. Higher satisfaction levels lead to positive CINT toward using a technology (Ashfaq *et al.*, 2020; Asad Hassan Butt *et al.*, 2021; Sabharwal *et al.*, 2015). Hence, AICS will positively impact the CINT of such technology usage in shopping. Another factor that can play a crucial role in understanding consumer behaviour is a brand's positive e-WOM. If satisfaction is high, it may lead to positive e-WOM (Uslu, 2020; Yang, 2017). We argue that the AICS will positively impact consumers' e-WOM and CINT toward such services in the online shopping context. Hence, we propose the following:

H5a: AICS positively influences e-WOM;

H5b: AICS positively influences CINT.

Perceived enjoyment (PEJM)

Another factor that plays a crucial role in understanding consumers' behaviour toward innovative technologies is enjoyment (Kaufmann *et al.*, 2017; McGloin *et al.*, 2016). Perceived enjoyment (PEJM) can positively affect consumers' satisfaction and CINT toward the brand services, such as chatbots (Ashfaq *et al.*, 2020). The literature has established that enjoyment is a strong predictor of understanding consumer behaviour toward chatbot services regarding usage intention (Jang *et al.*, 2019; Xuhui Wang *et al.*, 2020). Using PEJM can enhance

http://doi.org/10.18080/jtde.v11n4.735

consumers' satisfaction and CINT in chatbot services (Chung *et al.*, 2018; Gursoy *et al.*, 2019; M. Park *et al.*, 2020). Other studies have revealed the importance of PEJM when adopting new technologies (Alalwan *et al.*, 2018; Lee *et al.*, 2019). Understandably, human–computer interaction, such as with AI chatbots, helps people to experience fun and enjoyment. Hence, the enjoyment of using a technology while shopping can impact on a consumer's satisfaction and continuous intention (Holdack *et al.*, 2022; Kuo *et al.*, 2017; Tung *et al.*, 2017). Therefore, we propose the following:

H6a: PEJM positively influences AICS;

H6b: PEJM positively influences CINT.

Methodology

A renowned online retailer in India, Flipkart, is featured in this study. Flipkart is an online shopping website with a 31.9% market share, and its rival Amazon is not far behind with a 31.2% market share (Chaudhary, 2019; Chopra, 2019). Flipkart currently has over 200 million registered users (Singh, 2020). In 2018, Flipkart launched its chatbot services on its website and WhatsApp (Das, 2018). The company is still working on AI-enabled chatbots by continuously improving them to then improve customer experience. The company even introduced a haggling chatbot to help the end user negotiate prices with its unique AI machine-learning tools (Das, 2018). Hence, the current study focuses on understanding the AI-enabled chatbot services employed by India's largest e-commerce website. India boasts a vastly sized market with the potential for exponential growth. Furthermore, there has been a notable surge in digital technology adoption, particularly in terms of smartphone usage and internet access. India's cultural diversity contributes to a multifaceted consumer base shaped by various cultural and regional influences. Additionally, it is important to note that the e-commerce sector in India is marked by intense competition.

The study is structured as a survey. Convenience sampling was used to gather the data from the Indian online shopping market. Indian marketing is extensive and will therefore provide useful information about local consumers. The questionnaire was floated online using different social media platforms in India, such as Facebook and WhatsApp. The questionnaire wasn't translated into the Hindi language as the literacy rate is high in India, and the consumers of technology services are aware of such services. Even though the sample participants were mindful of chatbot services, they were informed in the form of an introduction at the start of the questionnaire to provide their user experience with Flipkart's AI chatbot services while shopping. The items for PUCB, AIIQ, AISQ, and AICS were adapted from (Abdullah *et al.*, 2016; Ashfaq *et al.*, 2020). The items for AICE and AAIC were adapted

http://doi.org/10.18080/jtde.v11n4.735

from Moriuchi *et al.* (2020). The items for CINT were taken from Evanschitzky *et al.* (2015). The items for PEJM were taken from Pillai *et al.* (2020).

The total number of questionnaires returned was 581. Out of these, only 554 were recorded for further analysis. Some responses were found to be incomplete or appeared to be duplicated. Therefore, following a thorough screening process, only the responses that met the criteria were considered for inclusion in the Smart Partial Least Squares (PLS) analysis. The response rate was 95%. COVID-19 has completely changed the business environment and consequently organisations focus more on AI tools to provide better services. Hence, studying Flipkart from India allows us to understand the AI-enabled chatbot services while shopping online. The Indian population is enormous, which has led to more technological services being introduced to benefit end users. Therefore, the 554 responses will give us valuable insights into Indian consumers using AI-enabled chatbot services for shopping online. Table 1 represents the demographic profile of the respondents.

Table 1. Respondents' profiles

Features	Distribution	Frequency	%
Gender	Male	351	63.36
	Female	203	36.64
Age	21–25	133	24.01
	26–30	262	47.29
	31–35	117	21.12
	36–40	42	7.58
Education	High school	67	12.09
	Undergraduate degree	177	31.95
	Master's degree	281	50.72
	PhD degree	29	5.23
Occupation	Student	247	44.58
	Job	219	39.53
	Business	88	15.88

Research Data Analysis

Multicollinearity and common method bias

Using a variance inflation factor (VIF) provides a method to evaluate the multicollinearity issues in a model. Multicollinearity indicates the correlation between independent variables, and the existence of multicollinearity may contaminate a study's inferences. VIF values are much lower than the threshold of five, as shown in Table 2; therefore, this study is free from the problem of multicollinearity. Similarly, the common method bias (CMB) or common method variance is also a concern. However, the CMB's multicollinearity issue is related to the

http://doi.org/10.18080/jtde.v11n4.735

methodology, not the constructs or analysis method. We used Bagozzi *et al.* (1988) and Kock (2015) methods to assess the CMB problem. Similarly, another way to detect CMB is to apply Kock's full collinearity test: if the inner VIF value is lower than the five thresholds, the study is free from CMB (Kock, 2015).

Assessment of measurement model

Before testing a study's hypothesis, the researcher must test the reliability and validity of the data. Partial least squares structural equation modelling consists of two measurement models that assess the reliability and validity of data and constructs. The second model also tests a study's hypothesis (Hair *et al.*, 2019). Reliability can be assessed through the factor loadings, Cronbach's alpha average variance, and composite reliability. Cronbach's alpha and composite reliability indicate the internal consistency, factor loadings confirm the indicator reliability and content validity, whereas the average variance extracted is used to assess the convergent validity.

Table 2. Reliability and validity

Variables	Item code	Factor loadings	VIF
Attitude toward AI chatbots	α =0.807, rho_A=0.809, CR=0.886, AVE=0.721		
The use of AI chatbot for shopping is very good.	AAIC1	0.849	1.69
The use of AI chatbot for shopping is a smart decision to make.	AAIC2	0.843	1.795
I have a positive impression of using AI chatbot for shopping.	AAIC3	0.856	1.774
AI chatbot engagement	α =0.857, rho_A=0.857, CR=0.931, AVE=0.779		
The use of AI chatbot grabs my attention while shopping online.	AICE1	0.845	1.817
I felt involved in online shopping while using AI chatbot.	AICE2	0.92	3.01
The interaction with AI chatbot while shopping excited me.	AICE3	0.881	2.474
AI chatbot satisfaction	α =0.856, rho_A=0.865, CR=0.905, AVE=0.706		
I am satisfied with the use of AI chatbot while shopping.	AICS1	0.693	1.375
I am satisfied with the use of AI chatbot functions.	AICS2	0.839	2.199
I am satisfied with the information and service quality of AI chatbot.	AICS3	0.906	3.348
Overall, I am satisfied with the AI chatbot.	AICS4	0.905	3.24
AI chatbot information quality	α =0.852, rho_A=0.853, CR=0.901, AVE=0.695		

http://doi.org/10.18080/jtde.v11n4.735

Variables	Item code	Factor loadings	VIF
The AI chatbot provides me with clear information while shopping.	AIIQ1	0.827	2.11
The AI chatbot provides the information in a useful format.	AIIQ2	0.859	2.779
I get information on time through this AI chatbot.	AIIQ3	0.892	3.5
The information is sufficient for me through this AI chatbot.	AIIQ4	0.75	1.481
AI chatbot service quality	α =0.845, rho_A=0.849, CR=0.897, AVE=0.685		
The AI chatbot offers an appealing visual display.	AISQ2	0.783	1.87
The interface of AI chatbot gives a modern look.	AISQ3	0.873	2.36
The right solutions for my response were provided by AI chatbot.	AISQ4	0.888	2.661
It gave me a prompt response.	AISQ5	0.761	1.55
Continuous intention	α =0.892, rho_A=0.899, CR=0.933, AVE=0.824		
I strongly recommended others to use AI chatbot service.	CINT1	0.857	2.012
I frequently used the AI chatbot for shopping experience.	CINT2	0.931	3.744
I plan to continue using AI chatbot service in the future.	CINT3	0.933	3.671
Perceived enjoyment	α =0.914, rho_A=0.914, CR=0.939, AVE=0.795		
I enjoyed interacting with AI chatbot.	PEJM1	0.864	2.515
It was a pleasant way to shop with AI chatbot.	PEJM2	0.881	2.61
AI chatbot recommendation was pleasurable during shopping.	PEJM3	0.920	3.741
I was absorbed well in shopping with the use of AI chatbot.	PEJM4	0.899	3.104
Perceived usefulness of AI chatbots	α=0.878, rho_A=0.882, CR=0.925, AVE=0.804		
My effectiveness was enhanced by the use of AI chatbot.	PUCB1	0.891	2.414
My productivity was increased by the use of AI chatbot.	PUCB2	0.932	3.484
It was useful for me to do shopping with the AI chatbot.	PUCB3	0.865	2.281
e-WOM	α=0.898, rho_A=0.901, CR=0.936, AVE=0.831		
I shared my experience of AI chatbot.	e-WOM1	0.907	3.153
I spoke positively about the AI chatbot.	e-WOM2	0.934	3.921

http://doi.org/10.18080/jtde.v11n4.735

Variables	Item code	Factor loadings	VIF
I have recommended this AI chatbot shopping website to others.	e-WOM3	0.893	2.306

Note: α= Cronbach's alpha; CR= Composite reliability; AVE= Average variance extracted; rho_A= dependability of the composite scale

Discriminant validity

Discriminant validity evaluates how the constructs of studies differ from each other in the context of the same model (Fornell *et al.*, 1982). Fornell-Larcker and HTMT (Heterotrait monotrait) ratios are commonly used to assess the discriminant validity (Fornell *et al.*, 1981). With the Fornell-Larcker criterion, when the square root of AVE is compared with the inter-construct correlation, the AVE's square root must be more significant than the correlation. On the other hand, the HTMT ratio is another measure that uses the correlation between variables based on a Monte Carlo simulation. HTMT ratio must be lower than .85 and AVE's square root must be greater than the correlation values in the same column in the Fornell-Larcker criterion. All the values of the Fornell-Larcker criterion and HTMT ratio reported in Table 3 are according to the standards.

Table 3. Discriminant validity and model fit

	AAIC	AICE	AICS	AIIQ	AISQ	CINT	PEJM	PUCB	e-WOM	GOF	SRMR	NFI
Fornell-Larcker criterion (discriminant validity)												
AAIC	**0.849**											
AICE	0.427	**0.882**										
AICS	0.624	0.693	**0.84**									
AIIQ	0.555	0.652	0.667	**0.834**								
AISQ	0.19	0.512	0.444	0.35	**0.828**							
CINT	0.505	0.586	0.723	0.603	0.46	**0.908**						
PEJM	0.641	0.582	0.698	0.588	0.277	0.534	**0.891**					
PUCB	0.465	0.712	0.728	0.615	0.504	0.65	0.515	**0.896**				
e-WOM	0.435	0.704	0.585	0.557	0.395	0.532	0.551	0.578	**0.911**			
HTMT ratio (discriminant validity)												
AAIC												
AICE	0.511											
AICS	0.745	0.811										
AIIQ	0.668	0.76	0.783									
AISQ	0.223	0.596	0.523	0.411								
CINT	0.594	0.669	0.83	0.692	0.529							
PEJM	0.747	0.657	0.786	0.666	0.313	0.591						
PUCB	0.547	0.822	0.844	0.707	0.578	0.732	0.573					
e-WOM	0.504	0.799	0.661	0.633	0.449	0.591	0.606	0.644				
Model fit										**0.585**	**0.79**	**0.063**

Note: AAIC = Attitude toward AI chatbots; AICE = AI chatbot engagement; AICS = AI chatbot satisfaction; AIIQ = AI chatbots information quality; AISQ = AI chatbots service quality; CINT = Continuous intention; PEJM=

http://doi.org/10.18080/jtde.v11n4.735

Perceived Enjoyment; PUCB = Perceived usefulness of AI chatbots; e-WOM = e-Word of Mouth. The highlighted values within each construct correspond to the square root of the average variance extracted (AVE).

Additionally, Table 3 includes model fit indicators such as SRMR (standardised root mean square residual), NFI (normed fit index), and GOF (goodness of fit), offering insights into the overall model fit. Furthermore, a supplementary note below the table highlights the significance of the AVE square root in the context of the analysis.

Goodness of fit indices

The hypothesis was tested through structural equation modelling using SmartPLS. The study's model has acceptable model fit criteria; values of the fit indices are reported in Table 3. From the SmartPLS model fit index, we have used two values: SRMR and NFI. The threshold for SRMR is closer to 1 and for NFI the standard value must be below 0.08 (Hair *et al.*, 2019). Both values are according to the standard, indicating a good model fit. In addition to these criteria, the researcher has developed another global fitness index known as the goodness of fit index (GOF) (Tenenhaus *et al.*, 2004). This model's GOF value is 0.585, higher than the threshold of 0.36, confirming this study's global validation (see Table 3).

Hypothesis testing results

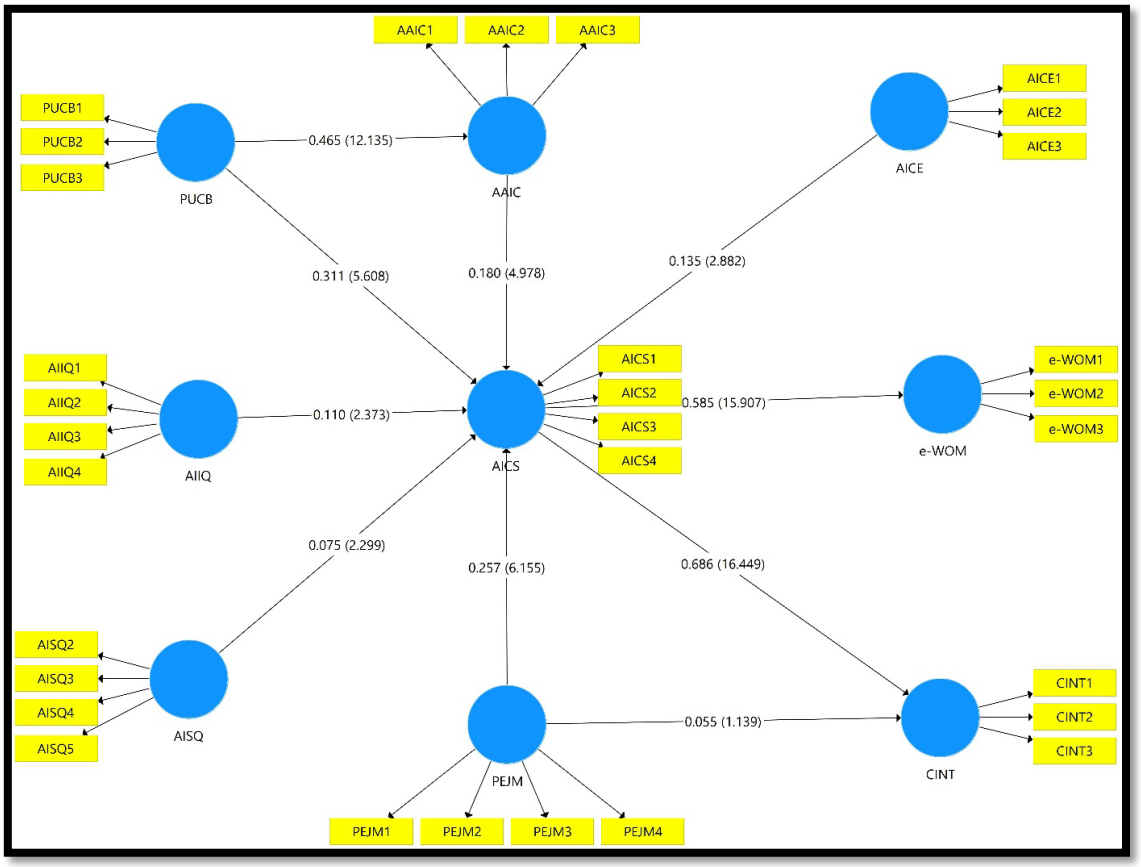
The proposed model has excellent and acceptable model fit indices, as reported above. Further, R square values indicate adequate explanatory power; R2 values are 0.217, 0.719, 0.525 and 0.342, respectively, as reported in Table 4. H1a and H1b postulate that AIIQ and AISQ positively affect AICS. As reported in Table 4, AIIQ is positively and significantly related to AICS (β=0.110, $p<0.05$), and AISQ also positively affects AICS (β=0.075, $p<0.05$). Therefore, H1a and H1b are supported. H2a and H2b propose a positive and significant impact of the PUCB on AAIC and AICS. Results shown in Table 4 indicate that these hypotheses have been proved. Hence, H2a and H2b are accepted based on empirical results. The testing for H3a and H3b shows that AAIC directly affects the AICS (β=0.180, $p<0.001$), and AAIC plays a mediating role between PUCB and AICS (β=0.084, $p<0.001$). Therefore, H3a and H3b are robustly accepted on empirical grounds. In H4, we proposed a positive and significant impact of AICE on AICS. Results reported in Table 4 support this hypothesis (β=0.135, $p<0.01$); therefore, H4 was accepted. Further results indicate that AICS has a positive impact on e-WOM (β=0.585, $p<0.001$) and on CINT (β=0.686, $p<0.001$). These relationships were proposed in H5a and H5b; thus, H5a and H5b have been supported. PEJM positively and significantly impacts AICS and CINT, as proposed in H6a and H6b. Results provided support for H6a (β=0.257, $p<0.001$), while H6b was rejected based on empirical results shown in Table 4 (β=0.055, $p>0.10$). The structural model of the data is shown in Figure 2.

http://doi.org/10.18080/jtde.v11n4.735

Table 4. Hypothesis tests

Hypothesis	Model variables	Beta coefficient (β)	P values	Decision
H1a	AIIQ → AICS	0.110	0.018	Accepted
H1b	AISQ → AICS	0.075	0.022	Accepted
H2a	PUCB → AAIC	0.465	0.000	Accepted
H2b	PUCB → AICS	0.311	0.000	Accepted
H3a	AAIC → AICS	0.180	0.000	Accepted
H3b	PUCB → AAIC →AICS	0.084	0.000	Accepted
H4	AICE → AICS	0.135	0.004	Accepted
H5a	AICS → e-WOM	0.585	0.000	Accepted
H5b	AICS → CINT	0.686	0.000	Accepted
H6a	PEJM → AICS	0.257	0.000	Accepted
H6b	PEJM → CINT	0.055	0.255	Rejected
Constructs	**R squared**			
AAIC	0.217			
AICS	0.719			
CINT	0.525			
e-WOM	0.342			

Note: AAIC = Attitude toward AI chatbots; AICE = AI chatbot engagement; AICS = AI chatbot satisfaction; AIIQ = AI chatbots information quality; AISQ = AI chatbots service quality; CINT = Continuous intention; PEJM = Perceived Enjoyment; PUCB = Perceived usefulness of AI chatbots; e-WOM = e-Word of Mouth



Note: AAIC = Attitude toward AI chatbots; AICE = AI chatbot engagement; AICS = AI chatbot satisfaction; AIIQ = AI chatbots information quality; AISQ = AI chatbots service quality; CINT = Continuous intention; PEJM = Perceived Enjoyment; PUCB = Perceived usefulness of AI chatbots; e-WOM = e-Word of Mouth

Figure 2. Structural model

http://doi.org/10.18080/jtde.v11n4.735

Discussion

AI-powered chatbot services serve a pivotal role in the realm of e-services, impacting both consumers and organisations (Moriuchi *et al.*, 2020; Pantano *et al.*, 2020). The current research framework has yielded promising results with respect to AI chatbot service satisfaction, continued usage intention, and e-WOM promotion. These findings carry significant implications for various theories and behavioural aspects. Evaluating AIIQ and AISQ demonstrates their critical role within the AICS landscape, corroborating prior research (Ashfaq *et al.*, 2020; Sangpikul, 2022). Furthermore, the perceived usefulness, benefits and overall attitude toward AI chatbots during shopping experiences can significantly enhance consumer satisfaction. The findings related to PUCB and AAIC are consistent with previous research studies (Amin *et al.*, 2014; Hess *et al.*, 2014). Moreover, these AI-driven chatbots have demonstrated their potential to enhance consumers' engagement with brand services, yielding positive outcomes. This underscores their role as catalysts for strengthening the bond between consumers and brands.

In our present research, AI chatbot services have demonstrated a remarkable capacity to actively engage consumers, thereby exerting a positive influence on the AICS landscape. This observation aligns harmoniously with prior research endeavours (Gangale *et al.*, 2013; Yusuf *et al.*, 2018), underscoring the consistency of these findings with established trends. Furthermore, our study elucidates the significant impact of AICS on consumers' intention to continue using chatbots (CINT). The results are indicative of consumers' satisfaction with AI chatbot services, as they express eagerness to persist in their usage and enthusiastically spread positive e-WOM about them. This trend aligns cohesively with the research conducted by (Yu *et al.*, 2022; Yusuf *et al.*, 2018). Lastly, our research findings concerning PEJM are in consonance with previous studies. While the data suggests that PEJM may not have a direct positive impact on CINT, it is worth noting that consumers may already be well acquainted with such services. Thus, their satisfaction remains intact, although they may not derive exceptional enjoyment from the experience. It is conceivable that a more extensive sample size could yield nuanced results, shedding further light on this aspect.

Theoretical contributions

The study's findings make significant contributions to the realm of AI chatbot usage theory. Firstly, the results underscore the expansion of the ISS model (Alahmari *et al.*, 2019; Delone *et al.*, 2003) and TAM theory (Manis *et al.*, 2019; Simay *et al.*, 2022) due to the incorporation of AI chatbots. The study's framework was meticulously crafted to illuminate the pivotal determinants of AI chatbots, encompassing user satisfaction, e-WOM propagation, and sustained usage intention. Secondly, the research integrates the notions of positive AICE (Hill

http://doi.org/10.18080/jtde.v11n4.735

et al., 2015) and PEJM (Ashfaq *et al.*, 2020). It extends the literature on the engagement aspect between consumers and organisations, enriching the existing literature concerning the engagement dynamics between consumers and organisations in the context of AI chatbots. Lastly, while numerous studies have explored chatbot adoption across diverse industries, few have delved into the realms of CINT and e-WOM within the sphere of AI-enabled chatbots for shopping. The study's findings serve to illuminate the distinctive role that chatbots equipped with AI tools play in the landscape of online shopping, offering fresh insights into this evolving domain.

The role of attitude is paramount, as it consistently yields positive outcomes, aligning with previous research findings (Sánchez-Prieto *et al.*, 2017; Suh & Youjae, 2006). The framework's results underscore the significance of AI-enabled chatbots in online shopping, as they effectively engage consumers through their utility and enjoyment factors. Consequently, this heightened engagement accelerates the adoption of these services, fostering deeper connections with a brand. As affirmed by earlier studies, consumer engagement holds the potential to enhance brand image and foster loyalty (Helme-Guizon *et al.*, 2019; McLean *et al.*, 2019). Moreover, the study recognises the pivotal role of e-WOM in the digital landscape. It is evident that satisfied consumers interacting with AI chatbots are more likely to contribute positively to e-WOM (Gkinko *et al.*, 2022; Uslu, 2020; Yang, 2017). In summation, the overall findings are distinctly favourable toward AI chatbots, substantially advancing the development of AI theory by shedding light on their pivotal role in enhancing engagement, satisfaction, and e-WOM within the realm of online shopping.

Practical contributions

The study's findings offer valuable insights and practical implications for managers across various domains. First, organisations should prioritise the development of factual information and service systems that ensure the timely delivery of accurate information. This is paramount, as the study predicts that the quality of AI chatbots' information and service delivery significantly influences customer satisfaction. Superior quality in these aspects can play a pivotal role in shaping more effective e-commerce business strategies. In today's COVID-19 environment, the importance of human–machine interaction is further underscored. Therefore, the establishment and enhancement of AIIQ and AISQ are imperative for the successful implementation of AI chatbots in online platforms.

Second, it is essential to acknowledge that innovative technologies like AI chatbots may elicit negative sentiments due to their inability to fully meet the needs and desires of consumers requiring human interaction. Hence, a balanced approach that combines human and machine interaction is recommended. By leveraging AI chatbots alongside human services employees,

http://doi.org/10.18080/jtde.v11n4.735

organisations can provide users with a digitally satisfying experience, fostering continued usage and positive e-WOM.

Third, the study underscores the pivotal role of enjoyment when predicting positive outcomes. Service benefits can be elevated to provide a sense of entertainment or enjoyment while in use. Therefore, retailers should consider incorporating gamification elements that engage consumers and deliver pleasure or joy during their interactions. Lastly, the ease of use and the provision of multiple benefits to end users should be central to the AI chatbots employed by different brands. Simplifying the user experience can have a positive impact on satisfaction, continued usage intention, and e-WOM. Thus, retailers should prioritise the development of user-friendly formats for AI chatbots. It is worth emphasising that AI chatbots distinguish themselves from RBAs by offering greater usefulness, enjoyment and engagement potential. These qualities contribute significantly to enhancing customer satisfaction, continuous usage intention, and positive e-WOM, making AI chatbots a valuable tool for businesses across industries.

Limitations

The study's results are helpful, but they still have limitations. First, the study's respondents were those who have experience using chatbots. For future reference, those respondents who haven't had any experience using AI chatbots could also participate. Technologies exist that are assisted or integrated with AI, such as augmented reality or virtual reality. These can also be used for future research. Second, ISS and TAM theories are well known, but some theories and variables can be incorporated for future studies, such as innovation diffusion theory, AI novelty, AI self-efficacy and technology anxiety. Further, perceived risk and trust can also play a significant part in future studies. Using different theories can provide a different perspective. Consumer culture theory can also perhaps be part of this future direction. Third, the sample comprised 554 respondents, which is good enough to highlight positive results in the framework. However, the Indian population is extensive, so a higher sample size would help to further understand AI chatbots in online shopping. Fourth, a comparative study can also play a key role in understanding AI-enabled chatbots. And last, combining front-line employees and AI chatbots within the real physical environment could be part of the future research.

Future directions

This study's insights offer valuable information for brand managers, enabling them to formulate comprehensive strategies for both online and offline platforms. In the rapidly evolving landscape of brand management, emerging technologies have a pivotal role. These

http://doi.org/10.18080/jtde.v11n4.735

technologies not only serve as effective customer attractors but also play a significant role in elevating the level of engagement between consumers and brands, fostering positive relationships. The integration of AI into brand operations presents a promising avenue in creating an amazing experience for the consumers. AI-driven systems have the capacity to assist consumers, tailoring recommendations based on their moods, attitudes and behaviours. This personalised approach not only enhances the consumer experience but also strengthens the bond between consumers and brands. Furthermore, brand managers can play a crucial role in enhancing employee engagement by providing training on the utilisation of AI. Empowering frontline employees to integrate AI into their sales processes can yield substantial benefits for both the company and its consumers. This synergy between human and AI-driven selling behaviours have the potential to optimise operations and further enhance the overall customer experience. In essence, the strategic incorporation of AI into brand management can lead to a win-win scenario, benefitting the company and its valued consumers.

Conclusion

The current human–machine interaction study was developed to understand consumers' satisfaction, CINT and e-WOM regarding AI chatbots. The use of such technologies is increasing, and many organisations are keen to further develop these services. The results' significance shows that consumers are willing to use these services and spread positive e-WOM. ISS and TAM have demonstrated that consumers find AI chatbots valuable and sound. The use of AI chatbots during online shopping can create immersive engagements for consumers, providing satisfaction, positive attitude and enjoyment. The results show that consumers are willing to develop a positive attitude toward using AI chatbots. Further, the brands or retailers could develop better strategies by introducing human services employees and AI chatbot integration to improve their services. Brands should integrate AI technology within online and offline environments to attract a customer base. AI chatbots can be of assistance not only to consumers but also to frontline employees. Therefore, it can be beneficial for companies to initiate integration of this technology to enhance both employee performance and consumer engagement.

References

Abdullah, F., Ward, R., & Ahmed, E. (2016). Investigating the influence of the most commonly used external variables of TAM on students' Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) of e-portfolios. *Computers in human behavior, 63*, 75–90. https://doi.org/10.1016/j.chb.2016.05.014

Adam, M., Wessel, M., & Benlian, A. (2020). AI-based chatbots in customer service and their effects on user compliance. *Electronic Markets, 31*(2), 427–445. https://doi.org/10.1007/s12525-020-00414-7

Ahmad, H., Butt, A., & Muzaffar, A. (2022). Travel before you actually travel with augmented reality–role of augmented reality in future destination. *Current Issues in Tourism, 26*(17), 2845–2862. https://doi.org/10.1080/13683500.2022.2101436

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2001). Nature and operation of attitudes. *Annual review of psychology, 52*(1), 27–58. https://doi.org/10.1146/annurev.psych.52.1.27

Alahmari, M., Issa, T., Issa, T., & Nau, S. Z. (2019). Faculty awareness of the economic and environmental benefits of augmented reality for sustainability in Saudi Arabian universities. *Journal of Cleaner Production, 226*, 259–269. https://doi.org/10.1016/j.jclepro.2019.04.090

Alalwan, A. A., Baabdullah, A. M., Rana, N. P., Tamilmani, K., & Dwivedi, Y. K. (2018). Examining adoption of mobile internet in Saudi Arabia: Extending TAM with perceived enjoyment, innovativeness and trust. *Technology in Society, 55*, 100–110. https://doi.org/10.1016/j.techsoc.2018.06.007

Amin, M., Rezaei, S., & Abolghasemi, M. (2014). User satisfaction with mobile websites: the impact of perceived usefulness (PU), perceived ease of use (PEOU) and trust. *Nankai Business Review International, 5*(3), 258–274. https://doi.org/10.1108/NBRI-01-2014-0005

Araujo, T. (2018). Living up to the chatbot hype: The influence of anthropomorphic design cues and communicative agency framing on conversational agent and company perceptions. *Computers in human behavior, 85*, 183–189. https://doi.org/10.1016/j.chb.2018.03.051

Araújo, T., & Casais, B. (2020). Customer acceptance of shopping-assistant chatbots. In *Marketing and Smart Technologies* (pp. 278–287): Springer.

Ashfaq, M., Yun, J., Yu, S., & Loureiro, S. M. C. (2020). I, Chatbot: Modeling the determinants of users' satisfaction and continuance intention of AI-powered service agents. *Telematics and Informatics, 54*, 101473. https://doi.org/10.1016/j.tele.2020.101473

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*, 74-94. https://doi.org/10.1007/BF02723327

Baker, V., Fowles, J., & Phillips, D. (2010). Difficult data: Boundary dynamics, public engagement and bridging technologies in a science/policy controversy. *East Asian Science, Technology and Society: An International Journal, 4*(4), 521–540. https://doi.org/10.1215/s12280-010-9143-0

Barry, J. M., & Graça, S. S. (2018). Humor effectiveness in social video engagement. *Journal of Marketing Theory and Practice, 26*(1-2), 158–180. https://doi.org/10.1080/10696679.2017.1389247

Bryce, D., Curran, R., O'Gorman, K., & Taheri, B. (2015). Visitors' engagement and authenticity: Japanese heritage consumption. *Tourism Management, 46*, 571–581. https://doi.org/10.1016/j.tourman.2014.08.012

Butt, A., Ahmad, H., Ali, F., Muzaffar, A., & Shafique, M. N. (2023). Engaging the customer with augmented reality and employee services to enhance equity and loyalty. *International Journal of Retail & Distribution Management, 51*(5), 629–652. https://doi.org/10.1108/IJRDM-04-2021-0165

Butt, A., Ahmad, H., Muzaffar, A., Ali, F., & Shafique, N. (2021). WOW, the make-up AR app is impressive: a comparative study between China and South Korea. *Journal of Services Marketing, 36*(1), 73–88. https://doi.org/10.1108/JSM-12-2020-0508

Butt, A. H., Ahmad, H., Goraya, M. A. S., Akram, M. S., & Shafique, M. N. (2021). Let's play: Me and my AI-powered avatar as one team. *Psychology & Marketing, 38*(6), 1014–1025. https://doi.org/10.1002/mar.21487

Butt, A. H., Ahmad, H., & Shafique, M. N. (2021). AI-Powered "Voice Recognition Avatar": A New Way to Play Games. *International Journal of Gaming and Computer-Mediated Simulations (IJGCMS), 13*(3), 1–17. https://doi.org/10.4018/IJGCMS.290305

Chaudhary, S. (2019). A Whooping $7 Billion On-Stake In India As Amazon Takes On Walmart-Owned Flipkart. Retrieved from https://eurasiantimes.com/a-whooping-7-billion-on-stake-in-india-as-amazon-takes-on-walmart-owned-flipkart/

Cheng, A., Baumgartner, H., & Meloy, M. G. (2021). Identifying picky shoppers: Who they are and how to spot them. *Journal of Consumer Psychology, 31*(4), 706–725. https://doi.org/10.1002/jcpy.1223

Chiu, Y.-T., Zhu, Y.-Q., & Corbett, J. (2021). In the hearts and minds of employees: A model of pre-adoptive appraisal toward artificial intelligence in organizations. *International Journal of Information Management, 60*, 102379. https://doi.org/10.1016/j.ijinfomgt.2021.102379

Chopra, K. (2019). Indian shopper motivation to use artificial intelligence. *International Journal of Retail & Distribution Management, 47*(3), 331–347. https://doi.org/10.1108/IJRDM-11-2018-0251

Chou, H. Y., Chu, X. Y., & Chiang, Y. H. (2020). What should we call this color? The influence of color-naming on consumers' attitude toward the product. *Psychology & Marketing, 37*(7), 942-960. https://doi.org/10.1002/mar.21351

Chung, M., Ko, E., Joung, H., & Kim, S. J. (2018). Chatbot e-service and customer satisfaction regarding luxury brands. *Journal of Business Research, 117*, 587–595. https://doi.org/10.1016/j.jbusres.2018.10.004

Ciechanowski, L., Przegalinska, A., Magnuski, M., & Gloor, P. (2019). In the shades of the uncanny valley: An experimental study of human–chatbot interaction. *Future Generation Computer Systems, 92*, 539–548. https://doi.org/10.1016/j.future.2018.01.055

Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management, 60*, 102383. https://doi.org/10.1016/j.ijinfomgt.2021.102383

Cronin, K. (2010). The "citizen scientist": reflections on the public role of scientists in response to emerging biotechnologies in New Zealand. *East Asian Science, Technology and Society: An International Journal, 4*(4), 503–519. https://doi.org/10.1007/s12280-010-9154-x

Das, S. (2018). Chatbots catching up in retail. Retrieved from https://www.indianretailer.com/magazine/2018/november/Chatbots-catching-up-in-retail.m120-4-1/

Delone, W. H., & McLean, E. R. (2003). The DeLone and McLean model of information systems success: a ten-year update. *Journal of management information systems, 19*(4), 9–30. https://doi.org/10.1080/07421222.2003.11045748

DeLone, W. H., & McLean, E. R. (2016). Information systems success measurement. *Foundations and Trends in Information Systems, 2*(1), 1–116. http://dx.doi.org/10.1561/2900000005

Du Plessis, R., Hindmarsh, R., & Cronin, K. (2010). Engaging across boundaries—emerging practices in 'technical democracy'. *East Asian Science, Technology and Society: An International Journal, 4*(4), 475–482. https://doi.org/10.1007/s12280-010-9157-7

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., . . . & Eirug, A. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

Evanschitzky, H., Iyer, G. R., Pillai, K. G., Kenning, P., & Schütte, R. (2015). Consumer trial, continuous use, and economic benefits of a retail service innovation: The case of the personal shopping assistant. *Journal of Product Innovation Management, 32*(3), 459–475. https://doi.org/10.1111/jpim.12241

Fagan, M., Kilmon, C., & Pandey, V. (2012). Exploring the adoption of a virtual reality simulation: The role of perceived ease of use, perceived usefulness and personal innovativeness. *Campus-Wide Information Systems, 29*(2), 117–127. https://doi.org/10.1108/10650741211212368

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, *18*(1). https://doi.org/10.1177/002224378101800104

Fornell, C., Tellis, G. J., & Zinkhan, G. M. (1982). *Validity assessment: A structural equations approach using partial least squares*. Paper presented at the Proceedings, American Marketing Association Educators' Conference.

Fotheringham, D., & Wiles, M. A. (2022). The effect of implementing chatbot customer service on stock returns: an event study analysis. *Journal of the Academy of Marketing Science, 51*, 802–822. https://doi.org/10.1007/s11747-022-00841-2

Freeze, R. D., Alshare, K. A., Lane, P. L., & Wen, H. J. (2019). IS success model in e-learning context based on students' perceptions. *Journal of Information systems education, 21*(2), 4. https://aisel.aisnet.org/jise/vol21/iss2/4

Gangale, F., Mengolini, A., & Onyeji, I. (2013). Consumer engagement: An insight from smart grid projects in Europe. *Energy Policy, 60*, 621–628. https://doi.org/10.1016/j.enpol.2013.05.031

Gao, L., & Waechter, K. A. (2017). Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation. *Information Systems Frontiers, 19*(3), 525–548. https://doi.org/10.1007/s10796-015-9611-0

Gkinko, L., & Elbanna, A. (2022). The appropriation of conversational AI in the workplace: A taxonomy of AI chatbot users. *International Journal of Information Management, 69*, 102568. https://doi.org/10.1016/j.ijinfomgt.2022.102568

Gulati, G. (2019). Importance Of Brand Engagement. Retrieved from https://www.gauravgulati.com/importance-of-brand-engagement/

Gupta, S., Leszkiewicz, A., Kumar, V., Bijmolt, T., & Potapov, D. (2020). Digital analytics: Modeling for insights and new methods. *Journal of Interactive Marketing, 51*(1), 26–43. https://doi.org/10.1016/j.intmar.2020.04.003

Gursoy, D., Chi, O. H., Lu, L., & Nunkoo, R. (2019). Consumers acceptance of artificially intelligent (AI) device use in service delivery. *International Journal of Information Management, 49*, 157–169. https://doi.org/10.1016/j.ijinfomgt.2019.03.008

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review, 31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Han, H., Baek, H., Lee, K., & Huh, B. (2014). Perceived benefits, attitude, image, desire, and intention in virtual golf leisure. *Journal of Hospitality Marketing & Management, 23*(5), 465–486. https://doi.org/10.1080/19368623.2013.813888

Helme-Guizon, A., & Magnoni, F. (2019). Consumer brand engagement and its social side on brand-hosted social media: how do they contribute to brand loyalty? *Journal of Marketing Management, 35*(7-8), 716–741. https://doi.org/10.1080/0267257X.2019.1599990

Hess, T. J., McNab, A. L., & Basoglu, K. A. (2014). Reliability generalization of perceived ease of use, perceived usefulness, and behavioral intentions. *MIS quarterly, 38*(1), 1–28. https://www.jstor.org/stable/26554866

Hill, J., Ford, W. R., & Farreras, I. G. (2015). Real conversations with artificial intelligence: A comparison between human–human online conversations and human–chatbot conversations. *Computers in human behavior, 49*, 245–250. https://doi.org/10.1016/j.chb.2015.02.026

Holdack, E., Lurie-Stoyanov, K., & Fromme, H. F. (2022). The role of perceived enjoyment and perceived informativeness in assessing the acceptance of AR wearables. *Journal of Retailing and Consumer Services, 65*, 102259. https://doi.org/10.1016/j.jretconser.2020.102259

Hu, Q., Lu, Y., Pan, Z., Gong, Y., & Yang, Z. (2021). Can AI artifacts influence human cognition? The effects of artificial autonomy in intelligent personal assistants. *International Journal of Information Management, 56*, 102250. https://doi.org/10.1016/j.ijinfomgt.2020.102250

Jang, Y., & Park, E. (2019). An adoption model for virtual reality games: The roles of presence and enjoyment. *Telematics and Informatics, 42*, 101239. https://doi.org/10.1016/j.tele.2019.101239

Jeon, C. (2018). The alpha human versus the Korean: Figuring the human through technoscientific networks. *East Asian Science, Technology and Society: An International Journal, 12*(4), 459–478. https://doi.org/10.1215/18752160-7218816

Jiménez-Barreto, J., Rubio, N., & Molinillo, S. (2021). "Find a flight for me, Oscar!" Motivational customer experiences with chatbots. *International Journal of Contemporary Hospitality Management, 33*(11), 3860–3882. https://doi.org/10.1108/IJCHM-10-2020-1244

Kallweit, K., Spreer, P., & Toporowski, W. (2014). Why do customers use self-service information technologies in retail? The mediating effect of perceived service quality. *Journal of Retailing and Consumer Services, 21*(3), 268–276. https://doi.org/10.1016/j.jretconser.2014.02.002

Kang, J.-Y. M. (2019). What drives omnichannel shopping behaviors? Fashion lifestyle of social-local-mobile consumers. *Journal of Fashion Marketing and Management: An International Journal, 23*(2), 224–238. https://doi.org/10.1108/JFMM-07-2018-0088

Kapoor, K., Dwivedi, Y., Piercy, N. C., Lal, B., & Weerakkody, V. (2014). RFID integrated systems in libraries: extending TAM model for empirically examining the use. *Journal of Enterprise Information Management, 27*(6), 731–758. https://doi.org/10.1108/JEIM-10-2013-0079

Kaufmann, R., Buckner, M. M., & Ledbetter, A. M. (2017). Having fun on facebook?: Mothers' enjoyment as a moderator of mental health and facebook use. *Health communication, 32*(8), 1014–1023. https://doi.org/10.1080/10410236.2016.1196513

Kawakami, T., & Parry, M. E. (2013). The impact of word of mouth sources on the perceived usefulness of an innovation. *Journal of Product Innovation Management, 30*(6), 1112–1127. https://doi.org/10.1111/jpim.12049

Kim, J. B. (2012). An empirical study on consumer first purchase intention in online shopping: integrating initial trust and TAM. *Electronic Commerce Research, 12*(2), 125–150. https://doi.org/10.1007/s10660-012-9089-5

Kim, S., Kandampully, J., & Bilgihan, A. (2018). The influence of eWOM communications: An application of online social network framework. *Computers in human behavior, 80*, 243–254. https://doi.org/10.1016/j.chb.2017.11.015

Kissi, J., Dai, B., Dogbe, C. S., Banahene, J., & Ernest, O. (2020). Predictive factors of physicians' satisfaction with telemedicine services acceptance. *Health informatics journal, 26*(3), 1866-1880. https://doi.org/10.1177/1460458219892162

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration (ijec), 11*(4), 1–10. https://doi.org/10.4018/ijec.2015100101

Kosiba, J. P. B., Boateng, H., Amartey, A. F. O., Boakye, R. O., & Hinson, R. (2018). Examining customer engagement and brand loyalty in retail banking. *International Journal of Retail & Distribution Management, 46*(8), 764–779. https://doi.org/10.1108/IJRDM-08-2017-0163

Koul, S., & Eydgahi, A. (2018). Utilizing technology acceptance model (TAM) for driverless car technology adoption. *Journal of technology management & innovation, 13*(4), 37–46. http://dx.doi.org/10.4067/S0718-27242018000400037

Kubo, A. (2013). Plastic comparison: The case of engineering and living with pet-type robots in Japan. *East Asian Science, Technology and Society: An International Journal, 7*(2), 205–220. https://doi.org/10.1215/18752160-2145117

Kumar, V., Dixit, A., Javalgi, R. R. G., & Dass, M. (2016). Research framework, strategies, and applications of intelligent agent technologies (IATs) in marketing. *Journal of the Academy of Marketing Science, 44*(1), 24–45. https://doi.org/10.1007/s11747-015-0426-9

Kuo, C.-M., Chen, L.-C., & Tseng, C.-Y. (2017). Investigating an innovative service with hospitality robots. *International Journal of Contemporary Hospitality Management, 29*(5), 1305–1321. https://doi.org/10.1108/IJCHM-08-2015-0414

Lee, J., Kim, J., & Choi, J. Y. (2019). The adoption of virtual reality devices: The technology acceptance model integrating enjoyment, social interaction, and strength of the social ties. *Telematics and Informatics, 39*, 37–48. https://doi.org/10.1016/j.tele.2018.12.006

Letheren, K., Russell-Bennett, R., & Whittaker, L. (2020). Black, white or grey magic? Our future with artificial intelligence. *Journal of Marketing Management, 36*(3-4), 216–232. https://doi.org/10.1080/0267257X.2019.1706306

Leung, E., Lenoir, A. S. I., Puntoni, S., & van Osselaer, S. M. J. (2022). Consumer preference for formal address and informal address from warm brands and competent brands. *Journal of Consumer Psychology, 33*(3), 546–560. https://doi.org/10.1002/jcpy.1322

Lin, T.-D. (2015). Theater as a site for technology demonstration and knowledge production: theatrical robots in Japan and Taiwan. *East Asian Science, Technology and Society: An International Journal, 9*(2), 187–211. https://doi.org/10.1215/18752160-2881956

Luo, X., Tong, S., Fang, Z., & Qu, Z. (2019). Frontiers: Machines vs. humans: The impact of artificial intelligence chatbot disclosure on customer purchases. *Marketing Science, 38*(6), 937–947. https://doi.org/10.1287/mksc.2019.1192

Manis, K. T., & Choi, D. (2019). The virtual reality hardware acceptance model (VR-HAM): Extending and individuating the technology acceptance model (TAM) for virtual reality hardware. *Journal of Business Research, 100*, 503–513. https://doi.org/10.1016/j.jbusres.2018.10.021

McGloin, R., Farrar, K. M., Krcmar, M., Park, S., & Fishlock, J. (2016). Modeling outcomes of violent video game play: Applying mental models and model matching to explain the relationship between user differences, game characteristics, enjoyment, and aggressive intentions. *Computers in human behavior, 62*, 442–451. https://doi.org/10.1016/j.chb.2016.04.018

McLean, G., & Wilson, A. (2019). Shopping in the digital world: Examining customer engagement through augmented reality mobile applications. *Computers in human behavior, 101*, 210–224. https://doi.org/10.1016/j.chb.2019.07.002

Mende, M., Salisbury, L. C., Nenkov, G. Y., & Scott, M. L. (2020). Improving financial inclusion through communal financial orientation: How financial service providers can better

engage consumers in banking deserts. *Journal of Consumer Psychology, 30*(2), 379–391. https://doi.org/10.1002/jcpy.1103

Milberg, S. J., Cuneo, A., Silva, M., & Goodstein, R. C. (2021). Parent brand susceptibility to negative feedback effects from brand extensions: A meta-analysis of experimental consumer findings. *Journal of Consumer Psychology, 33*(1), 21–44. https://doi.org/10.1002/jcpy.1282

Moriuchi, E. (2019). Okay, Google!: An empirical study on voice assistants on consumer engagement and loyalty. *Psychology & Marketing, 36*(5), 489–501. https://doi.org/10.1002/mar.21192

Moriuchi, E., Landers, V. M., Colton, D., & Hair, N. (2020). Engagement with chatbots versus augmented reality interactive technology in e-commerce. *Journal of Strategic Marketing, 29*(5), 375–389. https://doi.org/10.1080/0965254X.2020.1740766

Nguyen, Q. N., Ta, A., & Prybutok, V. (2019). An integrated model of voice-user interface continuance intention: the gender effect. *International Journal of Human–Computer Interaction, 35*(15), 1362–1377. https://doi.org/10.1080/10447318.2018.1525023

Olsson, T., Lagerstam, E., Kärkkäinen, T., & Väänänen-Vainio-Mattila, K. (2013). Expected user experience of mobile augmented reality services: a user study in the context of shopping centres. *Personal and ubiquitous computing, 17*(2), 287–304. https://doi.org/10.1007/s00779-011-0494-x

Pantano, E., & Pizzi, G. (2020). Forecasting artificial intelligence on online customer assistance: Evidence from chatbot patents analysis. *Journal of Retailing and Consumer Services, 55*, 102096. https://doi.org/10.1016/j.jretconser.2020.102096

Park, D.-H., & Lee, J. (2008). eWOM overload and its effect on consumer behavioral intention depending on consumer involvement. *Electronic Commerce Research and Applications, 7*(4), 386–398. https://doi.org/10.1016/j.elerap.2007.11.004

Park, M., & Yoo, J. (2020). Effects of perceived interactivity of augmented reality on consumer responses: A mental imagery perspective. *Journal of Retailing and Consumer Services, 52*, 101912. https://doi.org/10.1016/j.jretconser.2019.101912

Peddibhotla, N. B., & Subramani, M. R. (2007). Contributing to public document repositories: A critical mass theory perspective. *Organization Studies, 28*(3), 327–346. https://doi.org/10.1177/0170840607076002

Peng, C., van Doorn, J., Eggers, F., & Wieringa, J. E. (2022). The effect of required warmth on consumer acceptance of artificial intelligence in service: The moderating role of AI-human collaboration. *International Journal of Information Management, 66*, 102533. https://doi.org/10.1016/j.ijinfomgt.2022.102533

Pillai, R., Sivathanu, B., & Dwivedi, Y. K. (2020). Shopping intention at AI-powered automated retail stores (AIPARS). *Journal of Retailing and Consumer Services, 57*, 102207. https://doi.org/10.1016/j.jretconser.2020.102207

Prentice, C., Dominique Lopes, S., & Wang, X. (2020). The impact of artificial intelligence and employee service quality on customer satisfaction and loyalty. *Journal of Hospitality Marketing & Management, 29*(7), 739–756. https://doi.org/10.1080/19368623.2020.1722304

Przegalinska, A., Ciechanowski, L., Stroz, A., Gloor, P., & Mazurek, G. (2019). In bot we trust: A new methodology of chatbot performance measures. *Business Horizons, 62*(6), 785–797. https://doi.org/10.1016/j.bushor.2019.08.005

Quet, M., & Noel, M. (2014). From politics to academics: Political activism and the emergence of science and technology studies in South Korea. *East Asian Science, Technology and Society: An International Journal, 8*(2), 175–193. https://doi.org/10.1215/18752160-2416948

Radziwill, N. M., & Benton, M. C. (2017). Evaluating quality of chatbots and intelligent conversational agents. *arXiv preprint arXiv:1704.04579*. https://doi.org/10.48550/arXiv.1704.04579

Sabharwal, M., & Varma, R. (2015). Transnational research collaboration: expatriate Indian faculty in the United States connecting with peers in India. *East Asian Science, Technology and Society: An International Journal, 9*(3), 275–293. https://doi.org/10.1215/18752160-3141241

Saboo, A. R., Kumar, V., & Park, I. (2016). Using big data to model time-varying effects for marketing resource (re)allocation. *MIS quarterly, 40*(4), 911–940. https://www.jstor.org/stable/26629682

Sánchez-Prieto, J. C., Olmos-Migueláñez, S., & García-Peñalvo, F. J. (2017). MLearning and pre-service teachers: An assessment of the behavioral intention using an expanded TAM model. *Computers in human behavior, 72*, 644–654. https://doi.org/10.1016/j.chb.2016.09.061

Sands, S., Ferraro, C., Campbell, C., & Tsao, H.-Y. (2020). Managing the human–chatbot divide: how service scripts influence service experience. *Journal of Service Management, 32*(2), 246–264. https://doi.org/10.1108/JOSM-06-2019-0203

Sangpikul, A. (2022). Acquiring an in-depth understanding of assurance as a dimension of the SERVQUAL model in regard to the hotel industry in Thailand. *Current Issues in Tourism, 26*(3), 347–352. https://doi.org/10.1080/13683500.2022.2047163

Santos, G. (2011). Rethinking the Green Revolution in South China: technological materialities and human-environment relations. *East Asian Science, Technology and Society: An International Journal, 5*(4), 479–504. https://doi.org/10.1215/18752160-1465479

Scherer, R., Siddiq, F., & Tondeur, J. (2019). The technology acceptance model (TAM): A meta-analytic structural equation modeling approach to explaining teachers' adoption of digital technology in education. *Computers & Education, 128*, 13–35. https://doi.org/10.1016/j.compedu.2018.09.009

Setia, P., Setia, P., Venkatesh, V., & Joglekar, S. (2013). Leveraging digital technologies: How information quality leads to localized capabilities and customer service performance. *MIS quarterly, 37*(2), 565–590. https://www.jstor.org/stable/43825923

Sharma, S. K., & Sharma, M. (2019). Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation. *International Journal of Information Management, 44*, 65–75. https://doi.org/10.1016/j.ijinfomgt.2018.09.013

Siala, H., & Wang, Y. (2022). SHIFTing artificial intelligence to be responsible in healthcare: A systematic review. *Social Science & Medicine, 296*, 114782. https://doi.org/10.1016/j.socscimed.2022.114782

Simay, A. E., Wei, Y., Gyulavári, T., Syahrivar, J., Gaczek, P., & Hofmeister-Tóth, Á. (2022). The e-WOM intention of artificial intelligence (AI) color cosmetics among Chinese social media influencers. *Asia Pacific Journal of Marketing and Logistics, 35*(7), 1569–1598. https://doi.org/10.1108/APJML-04-2022-0352

Singh, M. (2020). Walmart's Flipkart makes local languages push to win small Indian cities and towns. Retrieved from https://techcrunch.com/2020/06/24/walmarts-flipkart-makes-local-languages-push-to-win-small-indian-cities-and-towns/#:~:text=Flipkart%20claims%20it%20has%20amassed%20more%20than%20200%20million%20registered%20users.

Spielmann, N., & Mantonakis, A. (2018). In virtuo: How user-driven interactivity in virtual tours leads to attitude change. *Journal of Business Research, 88*, 255–264. https://doi.org/10.1016/j.jbusres.2018.03.037

Stevens, H., & Haines, M. B. (2020). Tracetogether: pandemic response, democracy, and technology. *East Asian Science, Technology and Society: An International Journal, 14*(3), 523–532. https://doi.org/10.1215/18752160-8698301

Suh, A., & Wagner, C. (2017). How gamification of an enterprise collaboration system increases knowledge contribution: an affordance approach. *Journal of Knowledge Management, 21*(2), 416–431. https://doi.org/10.1108/JKM-10-2016-0429

Suh, J.-C., & Youjae, Y. (2006). When brand attitudes affect the customer satisfaction-loyalty relation: The moderating role of product involvement. *Journal of Consumer Psychology, 16*(2), 145–155. https://doi.org/10.1207/s15327663jcp1602_5

Sung, E. C., Bae, S., Han, D.-I. D., & Kwon, O. (2021). Consumer engagement via interactive artificial intelligence and mixed reality. *International Journal of Information Management, 60*, 102382. https://doi.org/10.1016/j.ijinfomgt.2021.102382

Tao, M., Nawaz, M. Z., Nawaz, S., Butt, A. H., & Ahmad, H. (2018). Users' acceptance of innovative mobile hotel booking trends: UK vs. PRC. *Information Technology & Tourism, 20*(1-4), 9–36. https://doi.org/10.1007/s40558-018-0123-x

Tarute, A., Nikou, S., & Gatautis, R. (2017). Mobile application driven consumer engagement. *Telematics and Informatics, 34*(4), 145–156. https://doi.org/10.1016/j.tele.2017.01.006

Tenenhaus, M., Amato, S., & Esposito Vinzi, V. (2004). *A global goodness-of-fit index for PLS structural equation modelling*. In XLII SIS Scientific Meeting. Padova: CLEUP, pp. 739–742.

Tung, V. W. S., & Law, R. (2017). The potential for tourism and hospitality experience research in human-robot interactions. *International Journal of Contemporary Hospitality Management, 29*(10), 2498–2513. https://doi.org/10.1108/IJCHM-09-2016-0520

Uslu, A. (2020). The relationship of service quality dimensions of restaurant enterprises with satisfaction, behavioral intention, eWOM and the moderator effect of atmosphere. *Tourism & Management Studies, 16*(3), 23–35. https://doi.org/10.18089/tms.2020.160303

Van Doorn, J., Lemon, K. N., Mittal, V., Nass, S., Pick, D., Pirner, P., & Verhoef, P. C. (2010). Customer engagement behavior: Theoretical foundations and research directions. *Journal of service research, 13*(3), 253–266. https://doi.org/10.1177/1094670510375599

van Esch, P., Black, J. S., & Arli, D. (2020). Job candidates' reactions to AI-Enabled job application processes. *AI and Ethics, 1*, 119–130. https://doi.org/10.1007/s43681-020-00025-0

Veeramootoo, N., Nunkoo, R., & Dwivedi, Y. K. (2018). What determines success of an e-government service? Validation of an integrative model of e-filing continuance usage. *Government Information Quarterly, 35*(2), 161–174. https://doi.org/10.1016/j.giq.2018.03.004

Wang, X., Butt, A. H., Zhang, Q., Ahmad, H., & Shafique, M. N. (2021). Intention to use AI-powered financial investment robo-advisors in the M-banking sector of Pakistan. *Information Resources Management Journal (IRMJ), 34*(4), 1–27. https://doi.org/10.4018/IRMJ.2021100101

Wang, X., Butt, A. H., Zhang, Q., Shafique, M. N., Ahmad, H., & Nawaz, Z. (2020). Gaming Avatar Can Influence Sustainable Healthy Lifestyle: Be like an Avatar. *Sustainability, 12*(5), 1998. https://doi.org/10.3390/su12051998

Wang, X., Butt, A. H., Zhang, Q., Shafique, N., & Ahmad, H. (2021). "Celebrity Avatar" Feasting on In-Game Items: A Gamers' Play Arena. *SAGE Open, 11*(2), 21582440211015716. https://doi.org/10.1177/21582440211015716

Wang, X., Haque, M. J., Li, W., Butt, A. H., Ahmad, H., & Shaikh, H. A. (2021). AI-Enabled E-Recruitment Services Make Job Searching, Application Submission, and Employee Selection More Interactive. *Information Resources Management Journal (IRMJ), 34*(4), 48–68. https://doi.org/10.1177/21582440211015716

Wang, X., Lin, X., & Shao, B. (2022). How does artificial intelligence create business agility? Evidence from chatbots. *International Journal of Information Management, 66*, 102535. https://doi.org/10.1016/j.ijinfomgt.2022.102535

Wang, Y., Zhang, M., Li, S., McLeay, F., & Gupta, S. (2021). Corporate responses to the coronavirus crisis and their impact on electronic-word-of-mouth and trust recovery: Evidence from social media. *British Journal of Management, 32*(4), 1184–1202. https://doi.org/10.1111/1467-8551.12497

Whitler, K. A. (2016). How artificial intelligence is changing the retail experience for consumers Retrieved from https://www.forbes.com/sites/kimberlywhitler/2016/12/01/how-artificial-intelligence-is-changing-the-retail-experience-for-consumers/?sh=7e9271610085

Willcocks, L., Lacity, M., & Craig, A. (2017). Robotic process automation: strategic transformation lever for global business services? *Journal of Information Technology Teaching Cases, 7*(1), 17–28. https://doi.org/10.1057/s41266-016-0016-9

Willems, T., & Graham, C. (2019). The imagination of Singapore's smart nation as digital infrastructure: Rendering (digital) work invisible. *East Asian Science, Technology and Society: An International Journal, 13*(4), 511–536. https://doi.org/10.1215/18752160-8005194

Williams, P., Escalas, J. E., & Morningstar, A. (2022). Conceptualizing brand purpose and considering its implications for consumer eudaimonic well-being. *Journal of Consumer Psychology, 32*(4), 699–723. https://doi.org/10.1002/jcpy.1324

Wu, H.-C., Ai, C.-H., & Cheng, C.-C. (2016). Synthesizing the effects of green experiential quality, green equity, green image and green experiential satisfaction on green switching intention. *International Journal of Contemporary Hospitality Management, 28*(9), 2080–2107. https://doi.org/10.1108/IJCHM-03-2015-0163

Yang, F. X. (2017). Effects of restaurant satisfaction and knowledge sharing motivation on eWOM intentions: the moderating role of technology acceptance factors. *Journal of Hospitality & Tourism Research, 41*(1), 93–127. https://doi.org/10.1177/1096348013515918

Ye, R., & Titheridge, H. (2017). Satisfaction with the commute: The role of travel mode choice, built environment and attitudes. *Transportation Research Part D: Transport and Environment, 52*, 535–547. https://doi.org/10.1016/j.trd.2016.06.011

Yeoh, W., & Koronios, A. (2010). Critical success factors for business intelligence systems. *Journal of computer information systems, 50*(3), 23–32. https://doi.org/10.1080/08874417.2010.11645404

Yeoh, W., & Popovič, A. (2016). Extending the understanding of critical success factors for implementing business intelligence systems. *Journal of the Association for Information Science and Technology, 67*(1), 134–147. https://doi.org/10.1002/asi.23366

Yu, S., Xiong, J., & Shen, H. (2022). The rise of chatbots: The effect of using chatbot agents on consumers' responses to request rejection. *Journal of Consumer Psychology*. https://doi.org/10.1002/jcpy.1330

Yusuf, A. S., & Busalim, A. H. (2018). Influence of e-WOM engagement on consumer purchase intention in social commerce. *Journal of Services Marketing, 32*(4), 493–504. https://doi.org/10.1108/JSM-01-2017-0031

An Analysis of the Optus National Outage and Recommendations for Enhanced Regulation

Mark A. Gregory
RMIT University

Abstract: On Wednesday, 8 November 2023 at about 4am, approximately 10 million Optus retail and 400,000 business customers lost network access as a result of the IP Core network shutdown. Optus stated that the cause of the network outage was a routine software upgrade that led to routing information updates from an international peering network causing key routers to disconnect from the network. This paper provides an analysis of the national outage, what information is needed to fully understand what occurred, and considers the lessons that might be learned.

Keywords: Telecommunications, Outage, Border Gateway Protocol, Internet Protocol Core Network, Resiliency

Introduction

On Wednesday, 8 November 2023 about 4.05am, Australia's second largest telecommunications company (Optus, 2023a), Optus, suffered a nationwide network outage that lasted more than 12 hours (Gregory, 2023a). At 4pm on the same day, Optus declared (Williams, 2023) the network outage had been resolved.

There were three key activities undertaken by Optus as the day unfolded (Optus, 2023a). The first was to identify and rectify the cause of the outage; the second was interacting with the Government and regulatory bodies; and the third was customer and media interaction.

In the days that followed, Optus' response to its stakeholders appeared uncoordinated, disorganised and chaotic — unsure of what information it should provide publicly (Haskell-Dowland *et al.*, 2023) and privately to Government and the regulators about what had occurred, what was being done to resolve the problem and how it would compensate customers affected by the outage.

http://doi.org/10.18080/jtde.v11n4.898

About three hours after the commencement of the national outage, Optus notified the Australian Communications and Media Authority (ACMA) that the network outage was "adversely affecting the carriage of emergency calls over the Optus network" (Optus, 2023a).

As a gesture of apology, on 9 November 2023, Optus indicated that it would provide eligible customers with 200GB of additional data as compensation (Optus, 2023c; Ainsworth, 2023). Media reports indicated that "customers were outraged" with the compensation offered by Optus. News.com.au reported that one customer had "shared a hack" that could be used by some affected customers to exchange the data for a plan charge (monetary) reduction (Whelan, 2023).

Attempting to explain the root cause of the outage, on 13 November 2023, in a media alert (Appendix), Optus suggested that the outage may have been partially due to failure in a third party "international peering network" (Optus, 2023b), which appears to have been the Singtel Internet Exchange (STiX), operated by Singtel, the parent company of Optus. On 16 November 2023, Singtel denied responsibility for the outage (Evans, 2023).

At a Senate hearing on 17 November 2023, an Optus representative stated: "We have applied the necessary protection to ensure that none of our peering partners could create a situation where a repeat of the outage could happen again" (Optus, 2023a).

Comparison with Meta Outage

On 4 October 2021, at about 15:40 UTC, routing announcements and withdrawals occurring from the Meta network, which hosts Facebook, WhatsApp and Instagram (collectively identified in this paper as Facebook), peaked leading to Meta's Domain Name System (DNS) servers going offline (Martinho & Strickx, 2021).

CloudFlare (2023a) describes the DNS as "the phonebook of the Internet". IBM (2023) describes DNS as the system that "makes it possible for users to connect to websites using Internet domain names and searchable URLs rather than numerical Internet protocol addresses. Rather than having to remember an IP address like 93.184.216.34, users can instead search for www.example.com".

It appears that the reason for Meta's DNS servers going offline was a problem related to Border Gateway Protocol (BGP) updates and announcements. Cisco (2023b) describes BGP as "the most scalable of all routing protocols. BGP is the routing protocol of the global Internet, as well as for Service Provider private networks. BGP has expanded upon its original purpose of carrying Internet reachability information, and can now carry routes for Multicast, IPv6, VPNs, and a variety of other data".

http://doi.org/10.18080/jtde.v11n4.898

The Facebook BGP updates and announcements for the period 14:00 UTC (01:00 AEDT) to 18:30 UTC (05:30 AEDT) on 4 October 2021 are shown in Figure 1.

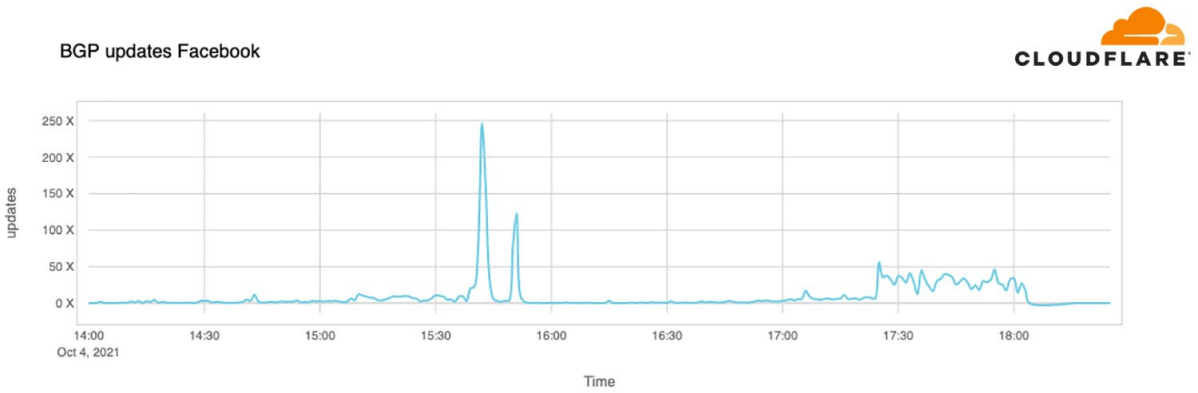


Figure 1. BGP Updates Facebook (Time: UTC) (Martinho & Strickx, 2021)

At 17:00 UTC (4am AEDT) on 7 November 2023, CloudFlare (2023b) reported a significant increase in BGP announcements from the Optus network, as shown in Figure 2, that led to the Optus routers disconnecting from its Core network due to "preset safety levels" (Gregory, 2023a).

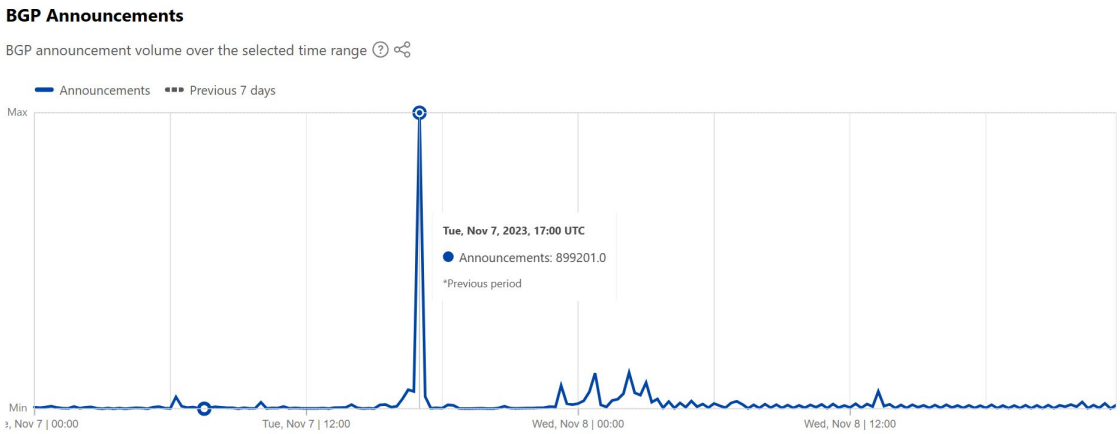


Figure 2. BGP Announcements Optus (Time: UTC) (CloudFlare, 2023b)

Network failures due to BGP are not uncommon, and incorrect BGP configuration will typically affect DNS and routers, followed by gateway and firewall devices. However, a central tenet of IP network routing protocols is the ability to offer multiple, diverse routing to ensure that events such as this one do not occur. To learn from this episode, it is critical that network operators like Optus develop contingency plans that minimise the impact of BGP routing failure in future. Optus has not clearly explained publicly how such a single software update failure could have resulted in such a widespread and protracted outage could occur.

The explanation provided by CloudFlare (Martinho & Strickx, 2021) of the Facebook outage provides a starting point for understanding what happened to Optus. A flood of BGP announcements can cause devices (DNS servers, routers, etc.) to disconnect, effectively bringing traffic flows to a halt.

http://doi.org/10.18080/jtde.v11n4.898

Internet Protocol Core Network

It has become clear that the Optus outage was the result of a fault in the "core network" (Haskell-Dowland *et al.*, 2023) that affected approximately 10 million retail and 400,000 business customers.

The Internet is complex, so most carriers, including Optus, use the concept of the "three layer network architecture" (Cisco, 2023a) to explain it. This abstraction splits the entire network into layers, as shown in Figure 3.

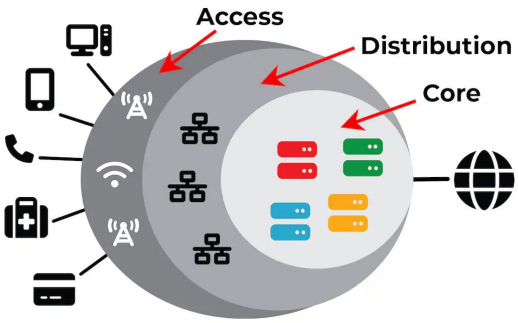


Figure 3. Three-layer Network Architecture. This architecture is just one of many different ways of describing complex networks. CC BY-SA (Gregory, 2023b)

The access layer

This layer consists of the devices you use to connect to the internet. They include the customer equipment, National Broadband Network firewalls and network termination devices, routers, mobile towers, and the wall sockets you plug into. Figure 4 shows an access network firewall, cable and mobile tower.

Figure 4. The access layer is what people interact with most often. CC BY-SA (Gregory, 2023b)

This layer generally is not interconnected, meaning each device sits at the end of the network. If you want to call a friend, for example, the signal would have to travel deeper into the network before coming back out to your friend's phone.

An outage in the access layer might only affect you and your local neighbourhood.

http://doi.org/10.18080/jtde.v11n4.898

The distribution layer

This layer interconnects the access layer with the core network (more on that later). Remember that the access layer regions are not connected to each other directly, so the distribution layer is the interconnecting layer. Another term for the interconnection cables is "backhaul". Backhaul is to the Internet like the main water pipes that travel between suburbs and towns are to a plumbing network. It is a bit more abstract but generally includes large switches in local exchange buildings, and the cabling that joins them together and to the core network.

Local exchange buildings, like the one shown in Figure 5, are being turned into network edge (Crozier, 2020) data centres to support distributed Cloud applications and services (Telstra, 2023a).

Figure 5. An exchange building in Bendigo, Victoria. Google maps, CC BY-SA (Gregory, 2023b)

The main purpose of the distribution layer is to route data efficiently between access points. An outage in this layer could affect whole suburbs or geographic regions.

The core layer

The core layer is the most abstract. It is the central backbone of the entire network and connects the distribution layers together and connects telecommunication carrier networks with the global network.

While physically similar to the distribution layer, with switches and cables, it is larger and much faster, contains more redundancy and is the location on the carrier's network where device and customer management systems reside. The carrier's operational and business systems are responsible for access, authentication and network security, traffic management, service provision and billing.

http://doi.org/10.18080/jtde.v11n4.898

Figure 6 shows a small section of a typical data centre, including infrastructure that is used to support and host Cloud applications and services.

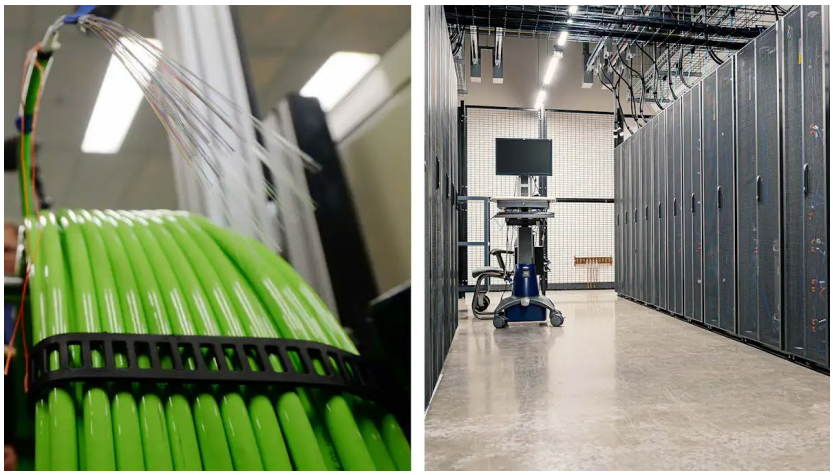


Figure 6. The core layer is abstract but includes fibre optic cables and datacentres. Pexels, Lukas Coch/AAP, CC BY-SA (Gregory, 2023b)

The core layer's primary function is volume and speed. It connects data centres, servers and the World Wide Web into the network using large fibre-optic cables.

An outage in the core layer can affect the entire country, as occurred with the Optus outage.

Why three layers?

A problem with networking is how to keep everyone connected as the network expands.

In a small network it may be possible to link everyone together but, as a network grows, this would be unwieldy (Gregory, 2023b), so the network is divided into layers based on function.

The three-layer model provides a functional description of a typical carrier network. In practice, networks are more complex, but we use the three-layer model to assist with the understanding of where equipment and systems are found in the network; e.g., mobile towers are in the access layer.

The core layer is designed to ensure that access-layer traffic coming from and going to the Internet or data centres is processed and distributed quickly and efficiently. Today, many terabytes of data moves through a typical carrier Core network daily.

A failure in the Core, caused by routers or DNS servers disconnecting, can affect an entire network. However, a central premise of the design of the Internet from the beginning has been to include multiple paths of core network redundancy to provide alternate routes for traffic to reach its destination if one or more primary routes has failed or becomes congested. When multiple routes of primary and redundancy pathways fail simultaneously, causing widespread outages, questions arise as to whether there may be fundamental flaws in the design of the core network architecture.

http://doi.org/10.18080/jtde.v11n4.898

When an upstream BGP gateway is updated and taken offline during the update process, downstream BGP gateways can be forced to move to an alternate upstream connection, and this can cause the BGP gateway to effectively reset its BGP routing table, generating a large spike in BGP announcements and updates. Firewall filter rules and policies should be in place to deal with spikes in BGP announcements and updates. Having a secondary upstream path that is already in place can ameliorate the impact of routing path changes.

Analysis

Information provided by Optus about the network outage does not provide a clear understanding of what occurred and why. Questions remain about the network design, redundancy and resilience.

The Optus outage appears to be the result of human error and not infrastructure failure nor a cyber incident. From what we know now, the Optus outage was preventable and has highlighted deficiencies in the Optus network design.

In this section, selected aspects of the Optus network outage will be discussed.

Critical infrastructure

The impact of the Optus outage was significant. The cost to customers and the nation is anticipated to be approximately $2 billion or more in economic activity.

The most important service to become unavailable was the Triple Zero (000) Emergency Call service (Bolger, 2023; Gregory, 2023a). Optus reported that 228 calls to the emergency call service were unable to be connected (Vidler, 2023).

This raises the question of whether Government should deem the IP Core networks of the three national carriers to be 'Critical Infrastructure'. By doing so the Government would ensure, through legislation, regulations, and cooperative network analysis amongst key industry players, that a similar outage would not happen again.

By deeming the three carrier IP Core networks to be Critical Infrastructure, the Government could require through regulations that there is more transparency, and improved reporting to the regulator, the Australian Communications and Media Authority (ACMA), on network design, management practices, redundancy and resiliency.

Recommendation 1. Government deem carrier networks to be Critical Infrastructure.

Recommendation 2. Government to introduce legislation and regulations regarding the minimum requirements for redundancy and resiliency of carrier networks.

http://doi.org/10.18080/jtde.v11n4.898

Network design and implementation

The Optus IP Core network outage appears to indicate that the Optus network is not sufficiently resilient. The cascading failure caused when the Core network routers disconnected appears to have caused the entire network to cease operation about 4.05am on Wednesday, 8 November 2023.

Optus has not released sufficient technical information for third parties to gain a clear understanding of its Core network architecture; however, it appears to be based on a centralised data centre with supporting edge data centres located around Australia. The centralised data centre is likely to host the key systems used for authentication, customer access, operations and billing. We gained an insight into this architecture when Optus indicated that it needed to send technical staff to sites to reset "100 devices in 14 sites across the country" (Williams, 2023).

In the Optus media release sent out on November 13 (Appendix), Optus states that it would "work with our international vendors and partners to increase the resilience of our network".

This raises questions:

1. Is Optus the design authority over its IP Core network?
2. Does Optus have sufficient engineering and technical staff supporting its networks?
3. What visibility is there that carrier Core networks are redundant and resilient?
4. What percentage of the technical and operational staff supporting the Optus IP Core network have accredited Australian Engineering or Computer Science qualifications and what percentage are on the National Engineering Register?
5. Is it appropriate for Singtel, the parent company of Optus, to have a direct involvement with the architecture or operation of the Optus Core IP network? Does this introduce a cyber-attack vector that is outside Australian jurisdiction?

Recommendation 3. Government to introduce regulations that provide minimum requirements for the control and operation of carrier networks.

Recommendation 4. Government to introduce regulations that provide minimum requirements for the competency of employees responsible for carrier networks.

Recommendation 5. Government to introduce regulations that specify the minimum requirements for carriers to maintain an Australian workforce that is responsible for the architecture, implementation and operation of carrier networks.

http://doi.org/10.18080/jtde.v11n4.898

Domestic mobile roaming

The loss of communications by Optus customers during the national network outage could have been reduced if emergency domestic roaming was available. Temporary domestic mobile roaming during an emergency is currently being investigated by Government (Rowland, 2023). The government ministers have tasked the Department of Infrastructure, Transport, Regional Development, Communications and the Arts and the National Emergency Management Agency to identify an emergency mobile roaming capability in collaboration with mobile carriers and to report back to Government by March 2024.

This activity comes after the Australian Competition and Consumer Commission (ACCC) completed an eighteen-month inquiry into the feasibility of temporary mobile roaming during an emergency. The ACCC concluded that it was "technically feasible" (ACCC, 2023). The outcome of the ACCC inquiry was unremarkable, as domestic mobile roaming occurs in many countries and across Europe.

In Australia, as in other countries, carriers are typically opposed to domestic mobile roaming as there is a perception that it reduces competition. In response to the Optus network outage, Telstra again reaffirmed its position that it is opposed to network sharing, even during an emergency (Telstra, 2023b). This position may have some merit, as Optus customers roaming onto the Telstra network during an emergency would significantly increase traffic demands on the Telstra network, likely causing significant network congestion (especially in regional areas) and potentially preventing Telstra customers from accessing the network, unless its entire regional network, or areas deemed to be high risk, were upgraded with additional capacity.

Importantly, domestic mobile roaming implemented with the carrier Core IP networks being traversed for device and customer authentication would not be a solution for the Optus network outage. In this scenario, the Optus customer devices would not be able to connect to another carrier's network.

Domestic mobile roaming implemented with a shared replicated authentication system to provide seamless domestic mobile roaming can be implemented. This would be a variation to Gateway Core Network, a version of active sharing that supports up to six network operators (3GPP, 2023). Arguments that the cost is prohibitive have not been tested publicly.

Domestic mobile roaming should have been introduced in Australia in 1997. Efforts to achieve this outcome are ongoing. There are many positive reasons for doing so, and no negatives other than the carriers being required to adopt an adjusted business model. In recent years the carriers have sold off large amounts of infrastructure, so the previous arguments about

http://doi.org/10.18080/jtde.v11n4.898

infrastructure being vital to competition are no longer sustainable. Unfortunately, new arguments that are equally unsustainable are now being put forward.

Implementing a shared replicated authentication system would be a secondary solution to ensuring that the carrier IP Core networks have appropriate redundancy and resiliency. However, with the light-touch regulatory environment currently in place in Australia, there is no transparency related to this matter.

Recommendation 6. Government launch a public inquiry into the technical implementation and cost for shared replication of device and user authentication.

Core IP network redundancy and resilience

The Optus network outage was surprising because Optus appears to indicate that the Core IP network does not have a design that is fully resilient. Redundant devices and routes may not exist or were inoperable; and separated control networks are not implemented or were inoperable. If any of these was indeed the case, then this highlights serious flaws in the Optus network design.

The requirement to send field technicians to sites to reset routers in those locations is surprising, as centrally controlled power solutions capable of initiating remote resets have been available for more than 30 years.

It should be anticipated that key network devices, such as DNS servers, routers, gateways and security appliances have their console ports connected to console servers that are connected to a separate protected control network.

It should be anticipated that key routers, DNS servers and other network devices have collocated redundant devices that are running the previous configuration to that running on the operational device. In the event of an outage due to a network software upgrade or misconfiguration, it should be possible for an intelligent network to disconnect the misbehaving device from the network and to bring up the redundant device before a catastrophic network outage occurs.

BGP is one of the original Internet protocols and, as such, there is considerable knowledge about how to implement BGP and to protect BGP appliances from flooding (update and announcements), hijacking, cyber attacks and other problems (Cisco, 2018, 2019).

This raises the question as to the suitability of the Optus IP Core network architecture and implementation. Whilst Optus has stated that it is taking steps to ensure that the outage will not occur again, what can be seen of the Optus IP Core network raises concerns that it is fragile and could be subject to the same or other failures in the future.

http://doi.org/10.18080/jtde.v11n4.898

Recommendation 7. Government regulate that independent Australian accredited registered engineers carry out annual audits of the carrier IP Core networks and provide reports to the regulator.

In Australia there is a requirement that the financial statements of most major corporations be audited annually, yet there appears to be a reluctance to audit Critical Infrastructure. The hands-off approach to regulation, also known as self-regulation, could leave the nation at risk of unwanted and unjustifiable outcomes.

Conclusions

It is reasonable to conclude that the Optus network was not fit for purpose leading to a national outage on 8 November 2023. A human error should not have been capable of bringing the entire Optus network down and the length of time taken to rectify the outage was excessive and required manual intervention at sites around the nation.

The extent of the problem is not fully understood and there is a need for Government to take action to ensure that similar failures to critical infrastructure do not occur in the future.

Government can improve legislation and regulation of critical infrastructure to ensure there are minimum requirements regarding transparency, redundancy, resiliency, accredited nationally registered employees, competency and network design and implementation practices. There is a need to introduce auditing of critical infrastructure and reporting.

The argument put forward by carriers that solutions are technically unfeasible and costly must be justified and balanced against the cost to customers, the nation and, more importantly, people imperilled by critical infrastructure failures.

References

3GPP. (2023). Network Sharing. Release 17. 3rd Generation Partnership Project. 9 November 2023. Accessed online https://www.3gpp.org/specifications-technologies/releases/release-17

ACCC. (2023). Regional mobile infrastructure inquiry 2022-23. Australian Communications and Consumer Commission. Australian Government. 23 October 2023. Accessed online https://www.accc.gov.au/inquiries-and-consultations/regional-mobile-infrastructure-inquiry-2022-23

Ainsworth, K. (2023). Optus offers customers 200GB of free data as compensation for nationwide outage. Australian Broadcasting Corporation. 9 November 2023. Accessed online https://www.abc.net.au/news/2023-11-09/optus-offers-customer-200gb-as-outage-compensation/103087168

Bolger, R. (2023). Optus outage prompts calls to force telcos to switch customers onto other networks when one fails. Australian Broadcasting Corporation. 8 November 2023.

http://doi.org/10.18080/jtde.v11n4.898

Accessed online https://www.abc.net.au/news/2023-11-08/optus-outage-roaming-customers-switch-to-networks-fail/103080582

Cisco. (2018). BGP Fundamentals. Cisco Press. 1 January 2018. Accessed online https://www.ciscopress.com/articles/article.asp?p=2756480&seqNum=5

Cisco. (2019). IP Routing: BGP Configuration Guide, Cisco IOS XE Gibraltar 16.11.x. Cisco. 25 September 2019. Accessed online https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bgp/configuration/xe-16-11/irg-xe-16-11-book.html

Cisco. (2023a). Cisco three-layer hierarchical model. Cisco. 17 November 2023. Accessed online https://study-ccna.com/cisco-three-layer-hierarchical-model/

Cisco. (2023b). Border Gateway Protocol (BGP). Cisco. 6 December 2023. Accessed online https://www.cisco.com/c/en/us/products/ios-nx-os-software/border-gateway-protocol-bgp/index.html

CloudFlare. (2023a). What is a DNS server? CloudFlare. 17 November 2023. Accessed online https://www.cloudflare.com/learning/dns/what-is-a-dns-server/

CloudFlare. (2023b). Routing Information from AS4804. CloudFlare. 17 November 2023. Accessed online https://radar.cloudflare.com/routing/as4804?dateStart=2023-11-07&dateEnd=2023-11-08

Crozier, R. (2020). Telstra's edge compute network to comprise 650 repurposed exchanges. Itnews. 31 November 2020. Accessed online https://www.itnews.com.au/news/telstras-edge-compute-network-to-comprise-650-repurposed-exchanges-555827

Evans, D. (2023). Optus parent company SingTel denies responsibility for outage. News.com.au. News Corp Australia. Accessed online https://www.news.com.au/technology/online/optus-parent-company-singtel-denies-responsibility-for-outage/news-story/4f3afcb0155f05c50a3f00e9c1ec4827

Gregory, M. A. (2023a). Optus has revealed the cause of the major outage. Could it happen again? *The Conversation*. 14 November 2023. Accessed online https://theconversation.com/optus-has-revealed-the-cause-of-the-major-outage-could-it-happen-again-217564

Gregory, M. A. (2023b). Explainer: what is the 'core network' that was crucial to the Optus outage? *The Conversation*. 9 November 2023. Accessed online https://theconversation.com/explainer-what-is-the-core-network-that-was-crucial-to-the-optus-outage-217375

Haskell-Dowland, P., Gregory, M. A., & Ahmed, M. (2023). Optus blackout explained: what is a 'deep network' outage and what may have caused it? *The Conversation*. 8 November 2023. Accessed online https://theconversation.com/optus-blackout-explained-what-is-a-deep-network-outage-and-what-may-have-caused-it-217266

IBM. (2023). What is DNS? IBM. 6 December 2023. Accessed online https://www.ibm.com/topics/dns

Martinho, C., & Strickx, T. (2021). Understanding how Facebook disappeared from the Internet. CloudFlare. 5 October 2021. Accessed online https://blog.cloudflare.com/october-2021-facebook-outage/

http://doi.org/10.18080/jtde.v11n4.898

Optus. (2023a). Submission to Senate Standing Committee on Environment and Communications. *Optus*. November 2023. Accessed online https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/OptusNetworkOutage/Submissions

Optus. (2023b). Media Alert: Update on Optus outage. Optus. 13 November 2023. (See Appendix)

Optus. (2023c). We're very sorry for the outage. Optus. 9 November 2023. Accessed online https://www.optus.com.au/notices/outage-response

Rowland. M. (2023). Government to scope emergency mobile roaming capability during natural disasters. Australian Government. 23 October 2023. Accessed online https://minister.infrastructure.gov.au/rowland/media-release/government-scope-emergency-mobile-roaming-capability-during-natural-disasters

Telstra. (2023a). Enhance your performance at the Edge. Telstra Corporation. 17 November 2023. Accessed online https://www.telstra.com.au/business-enterprise/products/cloud/solutions/telstra-edge

Telstra. (2023b). Submission to Senate Inquiry: Optus Network Outage. Telstra Corporation. 17 November 2023. Accessed online https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/OptusNetworkOutage/Submissions

Vidler, A. (2023). Hundreds of triple zero calls failed during Optus outage, CEO reveals while dodging questions over future. Nine.com.au. 17 November 2023. Accessed online https://www.9news.com.au/national/optus-ceo-kelly-bayer-rosmarin-to-face-senate-over-network-crash/d8786be0-7b81-420e-8b2c-3c87bd991670

Whelan, C. (2023). Optus outage compensation: Trick to turn 200GB data into cash. News.com.au. News Corp Australia. 15 November 2023. Accessed online https://www.news.com.au/technology/online/internet/optus-outage-compensation-trick-to-turn-200gb-data-into-cash/news-story/7a810d3972233a5b20cf051a8b8c96fb

Williams, T. (2023). Two weeks since the Optus outage, documents show backroom scrambling and urgent meetings occurred as the emergency played out. *ABC News*. 22 November 2023. Accessed online https://www.abc.net.au/news/2023-11-22/optus-outage-documents-behind-the-scenes-two-weeks-since/103130998

http://doi.org/10.18080/jtde.v11n4.898

Appendix

From: Optus Media Centre <media@optus.com.au>
Sent: Monday, November 13, 2023 1:14 PM
To: Optus Media Centre <media@optus.com.au>
Subject: [EXTERNAL] Media Alert: Update on Optus outage

Good afternoon,

Please find additional details below on the cause of last week's outage:

Optus Media Alert

We have been working to understand what caused the outage on Wednesday, and we now know what the cause was and have taken steps to ensure it will not happen again. We apologise sincerely for letting our customers down and the inconvenience it caused.

At around 4.05am Wednesday morning, the Optus network received changes to routing information from an international peering network following a routine software upgrade. These routing information changes propagated through multiple layers in our network and exceeded preset safety levels on key routers which could not handle these. This resulted in those routers disconnecting from the Optus IP Core network to protect themselves.

The restoration required a large-scale effort of the team and in some cases required Optus to reconnect or reboot routers physically, requiring the dispatch of people across a number of sites in Australia. This is why restoration was progressive over the afternoon.

Given the widespread impact of the outage, investigations into the issue took longer than we would have liked as we examined several different paths to restoration. The restoration of the network was at all times our priority and we subsequently established the cause working together with our partners. We have made changes to the network to address this issue so that it cannot occur again.

We are committed to learning from what has occurred and continuing to work with our international vendors and partners to increase the resilience of our network. We will also support and will fully cooperate with the reviews being undertaken by the Government and the Senate.

We continue to invest heavily to improve the resiliency of our network and services.

###

http://doi.org/10.18080/jtde.v11n4.898

Vale John Burke (1942–2023)

A Tribute to a Man who Contributed Much to Australian Telecommunications, TelSoc, and to All of his Communities

Jim Holmes
President, TelSoc

Abstract: John Burke was a long-term member of TelSoc, a member of the Editorial Advisory Board of this *Journal*, and Convenor of TelSoc's Broadband Futures Group. His sudden and unexpected death on 24 August 2023 was received with shock and great sadness by his colleagues in many fields, including in TelSoc and the ex-Telstra diaspora. This tribute focusses on John Burke's substantial contribution over a long period to the telecommunications sector, but provides some indication of the other work that he did over his 81 years for the various communities of interest of which he was part. John believed in the power of informed communities to take action to improve society in terms of equitable outcomes and opportunity, and persistently acted on that principle.

Keywords: John Burke, Obituaries, Australian telecommunications, First Nations, TelSoc

Introduction

Figure 1. John Burke in 2009 at Mallacoota

John Burke lived a full life and had an amazing capacity to pursue matters of public policy and community interest that he considered could deliver real and tangible benefits to communities and to society at large. It is this clear thread that runs through his life story, even though, as he admitted, his career paths were not clear to him when he started out or for some time later (Burke, 2022, p. 39).

http://doi.org/10.18080/jtde.v11n4.913

John saw his life and work as "episodic" (Burke, 2022, p. 39). The telecommunications episodes are the focus of this tribute, but other episodes provide a context within which to better appreciate the work that he did and his contribution. This tribute does not touch on some areas of John's rich and varied life, such as his work with communities involved in conservation and environmental sustainability. However, the pattern and the values that he espoused were consistent.

Early Life

John Philip Burke was born in Melbourne on 28 January 1942, and grew up in the beachside suburb of Sandringham. He was a serious student and leaned heavily towards mathematics and science in his academic orientation. He also leaned towards athletics and this was a major focus of his teenage years, through the Sandringham Athletics Club. John himself has noted that, between mathematics, science and athletics, he had little time or energy for other interests in those years. However, John's high achievements in athletics reflect his intense dedication to everything he did.

He was enrolled in a Science degree course at the University of Melbourne and studied there from 1959 to 1961. He majored in Pure Mathematics and the Theory of Statistics. In 1960, he was awarded the Dixson Scholarship for Pure Mathematics, a result that he attributed to a well-developed exam technique rather than superior insights into the subject (Burke, 2022, p. 38). He was invited to undertake an honours year in 1962, but he declined, because that course of action would lead to an academic career, which was not what he was seeking at that stage.

Instead, he joined IBM in London. But he soon returned to Melbourne to undertake further education to develop his capacity to become a teacher. He completed a Diploma of Education at the University of Melbourne and a Bachelor of Education at Monash University.

He also undertook post-graduate studies at Stanford University for a Master of Science degree on a Fullbright Scholarship. These studies, which consisted of considerable course work and a research assignment, would have resulted in a PhD had John completed them. His research field was in statistical techniques, with a minor discipline in computer science, a fast-developing field in those days. John found that there were fundamental limitations to computer-aided education. He says: "What it [the experience] gave me though was the understanding that, within the relationship of computer science and education, there was no developmental path for me, just one of critique" (Burke, 2022, p. 53). John's commitment to education was enhanced, but his commitment to computer-aided approaches diminished.

He returned to Australia and became a secondary teacher in Victoria for a while.

http://doi.org/10.18080/jtde.v11n4.913

The Malvern Learning Exchange

In 1971, John and his first wife, Kerry, moved to East Malvern. They were both heavily invested in the possibilities of community action to advance local community-based learning opportunities. Kerry was a lecturer in economics and had recently spent 18 months teaching in Japan.

In 1971, they started planning with friends and neighbours to take a major initiative in "de-formalised" education through what was to become the Malvern Learning Exchange, one of a number that were being established in Melbourne at that time (Neighbourhood Houses, 2022). The initiative was written up in *The Age* newspaper in December 1973:

> "They stocked a shop in Malvern with education books, toys, games, musical instruments, a card-index system and a small computer terminal for teaching purposes and typesetting. A roster of volunteer helpers was worked out.
>
> "At first the exchange worked by handling inquiries over the telephone or from people who dropped into the shop. Everyone they met was encouraged to fill out forms and become "resource people", listing their hobbies and interests and any skills they might be able to share with others" (Mathews, 1973).

The Age article records the wide diversity of people's interests at the time and the need to scale up the processing of matching interests and service providers:

> "Those whose wires crossed were put in touch with each other. But there were so many left over that it soon became necessary to establish a newspaper to gain a wider audience and to provide a forum for articles, ideas and discussions. The newspaper now [December 1973] appears monthly and has more than 400 subscribers throughout Australia, New Zealand and Papua New Guinea" (Mathews, 1973).

John noted that the first exchange was housed in a shop called the Lexicon Shop in High Street, Armidale (Burke, 2022, p. 61).

John's commitment and involvement in setting up the Malvern Learning Exchange is testimony to his persistence and to his determination to find practical means of implementing initiatives that will make a difference to the communities served. I especially mention this period of John's career because it was a forerunner to other similar initiatives and programs in which he later became involved.

The Learning Exchange had a long-term impact. Over 120 newsletters and articles were produced in the years to 1983. However, it struggled financially and barely made enough to

http://doi.org/10.18080/jtde.v11n4.913

keep going. There were various attempts to resuscitate it after John left, but it was finally closed in the mid-1980s (Burke, 2022, pp. 62–65).

Commission for the Future

The Commission for the Future was established by the Hawke Government in January 1985, and its creation was greatly encouraged by the then Minister for Science, Barry Jones MP.

> "It focussed on issues affecting the future including the predicament of youth, the ecology of health, sustainable environments, improving skills in Australia, technological change and law, management and work organisation, education futures, biotechnology, the information society, foreign affairs, the greenhouse effect, labour trends and population studies." (EOAS, 2011).

The Commission was contentious throughout its existence from 1985 to 1998, and was generally considered to be underfunded (EOAS, 2011). A more detailed assessment of the Commission's achievements and challengers by Richard Slaughter suggests that the Commission:

> "… attempted to carry out a wide range of projects and initiatives, many of which were intended to raise public awareness. But most projects were issues-based and it was not until rather late in the piece that standard futures methodologies were even contemplated. In this it differed from most other IOFs [Institutions of Foresight]. The initial selection of staff was dictated more by a political agenda (Jones was the Federal Minister for Science) than a professional one, and this coloured the nature of the organisation from the start. At no time thereafter did any full-time employee possess a background in FS [Future Studies]" (Slaughter, 1999, pp. 93–94).

This was the organisation that John joined in 1987 as a Deputy Director. His role within the Commission is unclear. However, from discussions with John in recent years, the author believes that his work was related to the future of education and to the planning process itself. He did attribute to his time with the Commission further development of his views about the rigour and integrity required if planning and related processes are to be effective and accountable. The downside, for John, appears to have been that the Commission was not gaining much traction and not providing the practical impact that he sought and achieved via the Learning Exchange. He left in 1988.

Telecom Australia and Telstra

John joined Telecom Australia in early 1989, taking up the position of Manager, Consumer Liaison and Policy Research, reporting to Ted Benjamin (and via him to Graeme Ward) in

http://doi.org/10.18080/jtde.v11n4.913

Telecom's Melbourne Headquarters. Due in part to the controversial proposal to introduce timed local calls, Telecom decided to establish a formal consultative process with consumer representatives. The first formal meeting of the Telecom Australia Consumer Council occurred in June 1989. Initially, representatives of ten consumer organisations met quarterly with Telecom senior managers. Under its formal structure, the Council was co-chaired by a senior Telecom executive and an elected consumer representative (Communications Law Centre, 1996). The Council evolved to the Telstra Consumer Consultative Council and operated until August 2009.

John's responsibilities included managing this consultative process. His knowledge of the community sector and his excellent collaborative style were instrumental in establishing the process and making it effective. One of the early engagements with consumers related to credit management and organisation responses to consumer hardship. John oversaw the establishment of the credit management working group, the first of a number of working groups which reported to the Consumer Council. There were significant improvements to Telstra's policies, products and services over time in this area.

Other benefits from this process included a continuing focus on people with disability and accessible telecommunications, product and service innovation, an affordability study, a pricing accord, raising awareness about public policy matters such as access to high-speed broadband, to name a few (Smith, 2000).

In 1991, John took up the position of Assistant Director, Business Planning, reporting to Graeme Ward, Managing Director, Corporate Strategy. There is no doubt from John's own observations then and later, confirmed by others who knew him at the time, that John found the process of corporate planning in a large and complex organisation to be stimulating, challenging and very frustrating. The need to compromise in order to move forward was not something that came easily to John, particularly when he was unable to engage directly with some of the higher levels of decision-making in Telstra.

Graeme Ward recalls:

> "I moved John to run the business planning process in the company to bring together Telstra's corporate plan both for internal consumption and to present to the Federal Government, as Telstra was 100% Government owned at that time. John worked closely with the late John Murphy to embed the overall company strategy into individual business unit plans across the company.
>
> "This role was extremely challenging given the size and complexity of the company and the often-competing objectives of the key stakeholders, being corporate Telstra—both Strategy and Finance—the business units and Government.

http://doi.org/10.18080/jtde.v11n4.913

> "John took on the role with his characteristic energy and collaborative style without shirking the challenge, working the issues and with the team produced credible corporate plans approved by the Telstra Board and acceptable to government" (Ward, 2023).

John resigned from Telstra in 1994, by which time he was the Group Manager, Business Planning, Telstra Corporate Strategy (Burke, n.d.).

Centre for International Research on Communication and Information Technologies (CIRCIT)

CIRCIT was set up in 1989 to provide independent research and education on information and communication services. The aim was to create new knowledge relevant to the community, industry and government, so as to increase the social and economic wellbeing of people in Australia and other parts of the world. It was established with funding from the Victorian State Government, Telecom Australia and other organisations.

John Burke took over as Director of the Centre for International Research on Communication and Information Technologies (CIRCIT) in 1994. This was a transitional time for CIRCIT as it moved from state government funding for its first five years to being independently funded. John kept CIRCIT operating through research funded by industry and the state government on a project-by-project basis, which was financially very challenging. In 1998, CIRCIT accepted RMIT's invitation to become part of the university. John Burke left CIRCIT in 2000. It closed down in 2001.

John's major contribution was to bring users, technologists, industry and policymakers together to talk to each other. Having worked with technologists, industry and policy makers, it was important for John that design and policy related to communication and information technologies led to effective solutions for everyday problems. His work with community organisations had focused on social justice and a fair society. This meant information and communication technologies had to work for all consumers, including the most marginal and vulnerable users.

CIRCIT under John Burke contributed towards an understanding of the use of information and communication technologies in the home, developing a monitoring framework for the effective use of online services, trust and electronic money, small business and electronic commerce, a design for the effective use of corporate email, and the multimedia strategy for the Victorian Government.

http://doi.org/10.18080/jtde.v11n4.913

This research contributed to CIRCIT and RMIT's participation in the Smart Internet Technology Cooperative Research Centre 2001–2008, followed by the Smart Services CRC 2008–2014. John's continued involvement with RMIT after he stepped down as Director, CIRCIT meant that he could help hone the users' perspective in the CRCs, which, by definition, brought together technologists, users, industry and policy makers.

As one of John's close associates at CIRCIT, Professor Supriya Singh, has observed:

> "It was not sufficient just to bring these diverse groups together. Conceptual frameworks and methodological approaches continued to differ. We needed a common language that went beyond disciplinary, industry and policy jargon. It was difficult to get people to speak plain English. Even when we succeeded by focusing on bridging concepts such as 'trust', 'design' and 'effective use', our initial questions were different. Though providers and policymakers are intensely interested in the way people use products and services, they start with questions about products and services. … It is a testimony to John Burke's emphasis on user-centred design and his ability to get people from diverse fields to work towards a fairer society, that researchers were able to work together on banking, electronic money and financial inclusion; security design and social and cultural practices; the users' perspective in digital rights management; trust, control and design; Pacific youth, digitising cultural collections and juvenile justice in New South Wales; and new media services" (Singh, 2023).

First Nations Issues

After he left CIRCIT in 2000, John became far more interested in issues of environmental sustainability and those affecting First Nations people. This in many ways was a continuation of his interest in inclusion and in ensuring that basic services and amenities were available to those who are marginalised or disadvantaged.

He wrote:

> "I joined Whitehorse Friends for Reconciliation in 2002 and was impressed by the work of people there – notably a weekend conference on Whitehorse Deliberates on Indigenous Issues, organised by Howard Tankey and Pam Morrison in particular, which brought over 100 Aboriginal and non-aboriginal members together for a very fruitful discourse.
>
> "Sid and Julia Spindler had established the Towards a Just Society Fund in the early 2000s. Various points of contact emerged with TJSF's activities, including the Fund's

http://doi.org/10.18080/jtde.v11n4.913

> support for Evonne Goolagong's establishment of a tennis program at Box Hill Secondary College. I also got more closely involved in the mid-2000s around the Fund's engagement with Worawa Aboriginal College at Healesville where I did some specific project work assisting them in planning and submissions" (Burke, 2022, p. 84)

In 2006, John was asked by Sid Spindler to attend a meeting of the Aboriginal Family Violence Prevention and Legal Service (FVPLS, now Djirra). This meeting was the start of a 10-year association between John and Djirra, and also with the national body (Burke, 2022, p. 85). John was instrumental in developing programs and strategic plans and in seeking funding from various levels of government and other sources.

When Sid Spindler became terminally ill, John took over as Chair of the Management Committee of the TJSF in 2016, and explored ways in which the Fund could be passed to an Indigenous-managed group to determine the allocation of philanthropic funds. "In 2018 TJSF broke new ground in Australian philanthropy when core funding totalling almost half a million dollars from TJSF and the estate of Les Dalton was used to establish Koondee Wonga-gat Toor-rong (KWT), Victoria's first Aboriginal and Torres Strait Islander-led philanthropic fund" (Richards, 2023)

TelSoc

In 2013, TelSoc (Telecommunications Association Inc., publisher of this *Journal*) and the *Journal* were both established in their present form following a period of amalgamation with the Australian Computer Society, which did not work out. John was invited to join the Editorial Advisory Board of the *Journal* in February 2019. He was known to many members of the Board from his work in Telstra and CIRCIT.

Together with others on the Board, John took the initiative to establish a group of volunteers who eventually formed themselves into the Broadband Futures Group within TelSoc. Their aim was to encourage government and industry to take the lead in developing a long-term plan for broadband communications and social and economic digital inclusion in Australia that would be transformative and overcome the short-term partisanship that had, at that time, characterised the sector for over a decade. John convened the Group, which met regularly before and during the COVID pandemic period, to develop a planning framework and proposal and to organise presentations and public discussions on various aspects of Australia's broadband experience and aspirations.

http://doi.org/10.18080/jtde.v11n4.913

Initially, events were in-person; then, at the outset of the lockdown period, they were hybrid, and, finally, they were conducted online. All of the events were well attended and most were the subject of articles in the *Journal*. They include:

- NBN Futures Forum: Encouraging Debate on NBN Ownership Models (Campbell & Milner, 2019);
- NBN Futures Forum: Realising the User Potential of the NBN (Campbell, 2019);
- NBN Futures Forum: Learning from International Experience (Campbell, 2020);
- NBN Futures Forum: Social and Economic Benefits of Broadband Networks – Telehealth and Digital Inclusion (Campbell *et al.*, 2020);
- NBN Futures Forum: A National Broadband Strategy for Australia (Holmes *et al.*, 2020);
- Broadband Futures Forum: Regional and Rural Broadband Access – City Standards in 10 years? (Campbell, 2021a);
- Broadband Futures Forum: The Rise of 5G and the NBN (Campbell, 2021b);
- Broadband Futures Forum: LEOs and how they differ from GEOs – OneWeb's plans in Australia and Competitor Differences (Pritchard-Kelly & Costa, 2022);
- Broadband Futures Forum: Affordability of Broadband Services (Campbell & Mithen, 2021);
- TelSoc Broadband Futures Forum: ABAC AgriTech Report (Waters & Koch, 2022);
- TelSoc Broadband Futures Forum: 5G Trends and Developments presented by Ericsson and Telstra (held online on 23 November 2021);
- Taking the Digital Economic Strategy (DES) to the next stage (held online on 17 March 2022);
- TelSoc Forum: Australian Broadband Advisory Council e-Health Report (held online on 22 March 2022); and
- Regional Connectivity and Shared Infrastructure: NSW and New Zealand (Adams *et al.*, 2022).

This represents a very full, diverse and rich body of work by many contributors, and John was the convenor and persistent facilitator of the initiative. He wanted to achieve a structured and serious discourse, both within TelSoc and with engagement with policy makers, community organisations and the industry, to ensure the widest possible involvement in making robust and enduring plans. He also wanted to ensure that plans, or proposals for plans, were not made once and forgotten about (often called "set and forget"). With his active participation, TelSoc made and published assessments of progress towards a national digital

http://doi.org/10.18080/jtde.v11n4.913

communications strategy at the end of 2021 (TelSoc BFG, 2021) and 2022 (TelSoc BFG, 2023), respectively.

A major step forward for John and TelSoc was in July 2022, when he and the author met with the then-recently appointed Minister for Communications, Michelle Rowland, in Melbourne, in order to have the Government take up the scoping of a national digital communications plan. The Minister was indeed receptive and her Department has now commenced industry consultations to see how the whole issue might best be taken forward. John participated in this work literally to the end of his life. The TelSoc Advocacy Working Group (successor to the Broadband Futures Group), comprising John, the author and Andrew Hamilton, were scheduled to meet with the Department the week following John's death. The meeting went ahead, but John was sorely missed, then as now.

Looking back on John Burke's extraordinary contributions, over a long period, to his various communities and to the sectors in which he worked, Emeritus Professor Trevor Barr summarised it thus:

> "John was a man of Integrity in both his personal and professional lives. For decades he was involved with the computer, telecommunications, and information industries, together with allied research and in public policy. He had a commendable approach by often asking this question — if we are living through an information revolution, who are the revolutionaries? Back in 1987, he summarized his philosophical position about the complex changes underway. He asked then: How many people know about these changes? Would everyone feel free to use these services? Are they easy to use? Are they affordable? (Barr, 1987). … These issues essentially guided his investigations during his multiple dimensional professional life — for the next fifty years!" (Barr, 2023).

Acknowledgements

The author deeply appreciates the contribution to this testament on John Burke's community and life's work from his family and many friends and colleagues. I am indebted to John Burke's family, and to Anna Burke, his daughter, in particular, for much material and for access to the manuscript that John prepared and shared with his children, (Jeremy, Anna, Sam, David and Sophie), which he named *From John to Family* (Burke, 2022). I acknowledge also the substantial assistance received from John's former colleagues, Trevor Barr, Graeme Ward, Margaret Portelli and Supriya Singh, and many others who assisted with their recollections and comments on John and his work. Trevor Barr, Graeme Ward and Margaret Portelli contributed on the period relating to Telecom Australia and Telstra. Margaret also contributed in relation to First Nations issues. Supriya Singh effectively wrote the material on CIRCIT.

References

Adams, P., Inglis, S., & Proctor, J. (2022). The Broadband Futures Forum: Regional Connectivity and Shared Infrastructure in NSW and New Zealand. *Journal of Telecommunications and the Digital Economy*, *10*(3), 1–13. https://doi.org/10.18080/jtde.v10n3.616

Barr, T. (ed.). (1987). *Challenges And Change: Australia's Information Society*. Oxford University Press, 1987. See chapter by Burke, J. P., The Impact of Technology.

Barr, T. (2023). Email from Professor Trevor Barr, now Emeritus Professor at Swinburne University in Melbourne, to the author dated 2 December 2023.

Burke, J. (n.d.). John Burke [author biographical statement]. Available at https://telsoc.org/journal/author/john-burke

Burke, J. P. (2022). *From John to Family* (unpublished). (Comment: this document was prepared by John Burke for his children. The author sourced the copy held by his daughter, Anna Burke. The document was prepared in recent years, and was presented to his children in 2022.)

Campbell, L. H., & Milner, M. (2019). NBN Futures Forum: Discussing the future ownership of Australia's National Broadband Network. *Journal of Telecommunications and the Digital Economy*, *7*(3), 1–9. https://doi.org/10.18080/jtde.v7n3.202. Held at RMIT, Melbourne, on 31 July 2019.

Campbell, L. H. (2019). The NBN Futures Forum: Realising the User Potential of the NBN. *Journal of Telecommunications and the Digital Economy*, *7*(4), 1–11. https://doi.org/10.18080/jtde.v7n4.228. Held at RMIT, Melbourne on 22 October 2019.

Campbell, L. H. (2020). The NBN Futures Forum: Learning from International Experience. *Journal of Telecommunications and the Digital Economy*, *8*(1), 49–57. https://doi.org/10.18080/jtde.v8n1.251. Held at RMIT, Melbourne, on 25 February 2020.

Campbell, L. H., Smith, A. C., & Brooks, P. (2020). The NBN Futures Forum: Social and Economic Benefits of Broadband for Digital Inclusion and Telehealth. *Journal of Telecommunications and the Digital Economy*, *8*(3), 18–32. https://doi.org/10.18080/jtde.v8n3.346. Held online on 18 August 2020.

Campbell, L. H. (2021a). The Broadband Futures Forum: Regional and Rural Broadband Access —City standards in 10 years? *Journal of Telecommunications and the Digital Economy*, *9*(2), 1–10. https://doi.org/10.18080/jtde.v9n2.400. Held online on 24 March 2021.

Campbell, L. H. (2021b). The Broadband Futures Forum: The Rise of 5G and the NBN. *Journal of Telecommunications and the Digital Economy*, *9*(3), 1–11. https://doi.org/10.18080/jtde.v9n3.432. Held online on 25 May 2021.

Campbell, L. H. and Mithen, J. (2021). The Broadband Futures Forum: Affordability of Broadband Services. *Journal of Telecommunications and the Digital Economy*, *9*(4), 127–137. https://doi.org/10.18080/jtde.v9n4.468. Held online on 25 August 2021.

Communications Law Centre. (1996). Telstra Consumer Consultative Council. (UNSW), *Communications Update*, *58*. Communications Law Centre (UNSW). Available at http://classic.austlii.edu.au/au/journals/CLCCommsUpd/1996/58.pdf. This publication provides a more detailed description of how the Telstra Consultative Consumer Council was structured and operated.

Encyclopedia of Australian Science and Innovation. (2011). Corporate Body: Commission for the Future (1985 - 1998). Available at https://www.eoas.info/biogs/A002176b.htm

Holmes, J. R., Burke, J. P., Campbell, L. H., & Hamilton, A. (2020). Towards a National Broadband Strategy for Australia, 2020-2030. *Journal of Telecommunications and the Digital Economy*, *8*(4), 192–269. https://doi.org/10.18080/jtde.v8n4.371. Held online on 24 November 2020.

Mathews, I. (1973). Learning exchanges provide the bridge to knowledge. *Education Age*, *Age*, Melbourne, 4 December 1973.

Neighbourhood Houses Victoria. (2022). Our history. Neighbourhood Houses Victoria. Available at https://www.nhvic.org.au/history. The neighbourhood house movement in Victoria had its origins in the late 1960s, and has grown in strength and diversity, indicating a demand for services and courses developed locally at the time and since.

Pritchard-Kelly, R., & Costa, J. (2022). Low Earth Orbit Satellite Systems: Comparisons with Geostationary and Other Satellite Systems, and their Significant Advantages. *Journal of Telecommunications and the Digital Economy*, *10*(1), 1–22. https://doi.org/10.18080/jtde.v10n1.552. Held online on 11 August 2021.

Richards, N. (2023). Vale John Burke. Australian Communities Foundation, 2 October 2023. Available at https://communityfoundation.org.au/about/news-and-media/vale-john-burke

Singh, S. (2023). Email to the author dated 15 December 2023. Professor Supriya Singh, formerly Deputy Director of CIRCIT and now Adjunct Professor, Department of Social Inquiry, La Trobe University, prepared the content and much of the text of the section on CIRCIT.

Slaughter, R. A. (1999). Lessons from the Australian Commission for the Future: 1986–98. *Futures*, *31*(1), 91–99. https://doi.org/10.1016/s0016-3287(98)00114-1

Smith, S. (ed.). (2000). *In the Consumer Interest – a selected history of consumer affairs in Australia 1945-2000*. Society of Consumer Affairs Professional in Business (Australia), Melbourne. It has a chapter entitled *Telecommunications: Consumers on the Line* that refers to the Telstra Consumer Consultative Council and John Burke.

TelSoc Broadband Futures Group. (2021). Assessing Australia's Progress Towards a National Broadband Strategy at December 2021. *Journal of Telecommunications and the Digital Economy*, *9*(4), 149–177. https://doi.org/10.18080/jtde.v9n4.472

TelSoc Broadband Futures Group. (2023). Assessing Australia's Progress towards a National Digital Communications Strategy at December 2022. *Journal of Telecommunications and the Digital Economy*, *11*(1), 29–43. https://doi.org/10.18080/jtde.v11n1.717

Ward, G. B. (2023). Private email from Graeme Ward to the author dated 26 October 2023.

Waters, P., & Koch, A. (2022). The Broadband Futures Forum: The Australian Broadband Advisory Council Agri-Tech Expert Working Group Report. *Journal of Telecommunications and the Digital Economy*, *10*(1), 23–33. https://doi.org/10.18080/jtde.v10n1.553. Held online on 21 October 2021.