



# Journal of Telecommunications and the Digital Economy

Volume 10, Number 4  
December 2022

Published by  
Telecommunications Association Inc.  
ISSN 2203-1693

© 2022 Telecommunications Associate, Inc. (TelSoc)

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 10, Number 4

December 2022

## Table of Contents

The Editorial Team	ii
<b>Editorial</b>	
Editorial: Building Trust in the Digital Economy Leith H. Campbell	iii
<b>Public Policy</b>	
Towards an Australian Digital Communications Strategy Michael de Percy, Leith Campbell, Nitya Reddy	1
Preserving Transparency and Integrity of Elections Utilising Blockchain Technology Abdallah Al-Zoubi, Mamoun Aldmour, Rakan Aldmour	24
<b>Digital Economy</b>	
Perceived Risk, Structural Assurance and Trust in Mobile Payments Afef Sahli Sassi, Hanene Hammami, Hajer Ben Lallouna Hafsia	41
<b>Telecommunications</b>	
Towards Optimization of Patients' Turnaround Time using Bluetooth Low Energy Based Solutions Ganes Raj Muthu Arumugam, Saravanan Muthaiyah, Thein Oak Kyaw Zaw	57
A Proposal for Dynamic and Secure Authentication in IoT Architectures Based on SDN Younes Abbassi, Hicham Toumi, El Habib Ben Lahmar	72
<b>Book Review</b>	
A History of Reshaping Australian Telecommunications: A Review of John Doyle's <i>Crossed Lines: Disruption, Politics and Reshaping Australian Telecommunications</i> Judith Brett	94
<b>Biography</b>	
David Piltz is Awarded the 2022 Charles Todd Medal Peter Gerrand, David Piltz	98
<b>History of Telecommunications</b>	
Marconi Wireless Telegraphy Trialled in Australia Simon Moorhead	103

## Editorial Team

### Managing Editor

Dr Leith H. Campbell, RMIT University

### Section Editors

Dr Frank den Hartog, University of New South Wales, Canberra  
(*Telecommunications*)

Dr Michael de Percy, University of Canberra (*Public Policy*)

Professor Payam Hanafizadeh, Allameh Tabataba'i University  
(*Digital Economy*)

Dr Jim Holmes, Incyte Consulting (*Book Reviews*)

Professor Peter Gerrand, University of Melbourne  
(*Biography; History of Telecommunications*)

### Board of Editors

Assoc. Professor Sultana Lubna Alam  
Deakin University, Australia

Professor Payam Hanafizadeh  
Allameh Tabataba'i University, Iran

Professor Abdallah Al Zoubi  
Princess Sumaya University for Technology,  
Jordan

\* Dr Jim Holmes  
Incyte Consulting, Australia & UK

\* Professor Trevor Barr  
Swinburne University, Australia

\* Mr Allan Horsley

\* Mr John Burke

Dr Maria Massaro  
Korea University, Republic of Korea

\* Dr Leith Campbell  
RMIT University, Australia

Professor Catherine Middleton  
Ryerson University, Canada

\* Mr John Costa

\* Dr Murray Milner  
Milner Consulting, New Zealand

Dr Frank den Hartog  
University of NSW, Canberra, Australia

Assoc. Professor Sora Park  
University of Canberra, Australia

\* Dr Michael de Percy  
University of Canberra, Australia

Mr Vince Pizzica  
Pacific Strategic Consulting, USA

\* Professor Peter Gerrand  
University of Melbourne, Australia

Professor Ashraf Tahat  
Princess Sumaya University for Technology,  
Jordan

\* denotes a member of the Editorial Advisory Board. The President of TelSoc is, *ex officio*, a member of the Editorial Advisory Board (if not otherwise a member).

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

# Building Trust in the Digital Economy

---

Leith H. Campbell  
Managing Editor

---

### Abstract:

This editorial comes in two parts: some remarks on government plans for the digital economy and the necessity of building trust; and a brief introduction to the papers in this issue.

**Keywords:** Government strategy, Trust, Editorial

## Government Leadership and Trust

The role of government and maintaining and supporting trust are themes that run through many of the papers in this issue. Government is called upon not just to regulate telecommunications and the digital economy, but also to provide leadership and direction in some areas.

When telecommunications was being transformed from a government-run near monopoly to a privately owned, competitive marketplace, there were some, perhaps, who thought it would be “set and forget”: governments could mainly stand aside, keeping just a light hand on the regulatory tiller to ensure fair competition. In Australia in 2009, this view was firmly set aside by the Commonwealth (federal) Government of the time deciding to create a wholly owned government business enterprise, NBN Co Ltd, which would establish and operate a wholesale only National Broadband Network (NBN), and to give it a near monopoly of high-speed access. It has been a matter of comment, debate and political contention ever since.

That such a move would be subject to debate and political scrutiny should come as no surprise: it was ever thus. This journal issue includes a review by Professor Judith Brett ([Brett, 2022](#)) of a new book by John Doyle on telecommunications “reform” in Australia up to the introduction of full competition. The book’s title, *Crossed Lines: Disruption, Politics and Reshaping Australian Telecommunications*, hints at the nature of the “reform” process. While politics plays a part, Professor Brett in her review expresses the view that “continuous

disruption [in telecommunications] is driven by relentless technological innovation to which politics has little choice but to respond” ([Brett, 2022](#), p. 97), a view undoubtedly supported by many readers of this *Journal*. Another case of a political response (in this case, Colonial politics) to technological change is described in the historical reprint ([Moorhead, 2022](#)) in this issue.

When Michelle Rowland, the Australian Minister for Communications, gave the Charles Todd Oration (a major event in the annual calendar of TelSoc, the publisher of this *Journal*), in October 2022, she indicated that she recognized the need both for enhancements to the NBN – that is, to the supply of broadband – and for building the capabilities of users and the inclusion of all in taking advantage of digital services – that is, the demand side.

The recently issued “Statement of Expectations” for NBN Co ([NBN Co, 2022](#)) by the Commonwealth Ministers for Communications and Finance is a step on the road to better supply. It is a more comprehensive document than its predecessor ([Australian Government, 2021](#)) and, while it sets expectations in many areas, it includes few real targets. It does, however, specify some peak download speeds: 1 Gbps availability for 90% of premises in the fixed-line footprint ([NBN Co, 2022](#), p. 2) and at least 50 Mbps busy-hour speed for Fixed Wireless Access (p. 4). We expect that NBN Co will define further targets and specific commitments, as it responds to the Government’s expectations.

The New Zealand Government, which seems to do well in this area, has recently issued “The Digital Strategy for Aotearoa [New Zealand]” ([NZ Government, 2022](#)). It sets out three themes – trust, inclusion and growth – the first two of which are primarily concerned with users and demand-side issues (while being underpinned by technological means). It sets out goals and measures in each area and it recognizes both challenges and opportunities. Importantly, it describes how the strategy will be put into action and how it will be adjusted as it progresses.

The New Zealand Government is right to emphasize trust. Trust is also identified as an important issue in another paper in this issue ([de Percy, Campbell & Reddy, 2022](#)) that provides an overview of both supply-side and demand-side initiatives in several countries. The New Zealand plan stands up well in comparison to the other strategies outlined in that paper.

The issue of trust also runs through other papers in this issue. Trust is an important aspect of mobile services for users ([Sahli Sassi, Hammami & Ben Lallouna Hafsia, 2022](#)); it must be supported by technology ([Abbassi, Toumi & Ben Lahmar, 2022](#)); and, in a democratic society, it is important that citizens trust the results of elections performed by digital means ([Al-Zoubi, Aldmour & Aldmour, 2022](#)).

Trust and inclusion will be major issues in the future. Governments will need to show leadership in these areas if they are to depend on digital services for their own interactions with their citizens – and if society is fully to benefit from the fast-expanding digital economy.

## In This Issue

We have a strong Public Policy section in this issue with two papers. *Towards an Australian Digital Communications Strategy: Lessons from Cross-Country Case Studies* summarizes initiatives in several countries to develop and execute a strategy for supporting the digital economy. *Preserving Transparency and Integrity of Elections Utilising Blockchain Technology* describes a proposal for security of election processes and results.

In the Digital Economy section, we have one paper, on the attitudes towards, and the requirements to support, *Perceived Risk, Structural Assurance and Trust in Mobile Payments*.

In the Telecommunications section, we publish two papers. *Towards Optimization of Patients' Turnaround Time using Bluetooth Low Energy Based Solutions* outlines a method for improving processes in hospitals. *A Proposal for Dynamic and Secure Authentication in IoT Architectures Based on SDN* looks at how to secure the Internet of Things.

We publish a review, *A History of Reshaping Australian Telecommunications: A Review of John Doyle's Crossed Lines: Disruption, Politics and Reshaping Australian Telecommunications*, of a book that will be of interest to many readers of the *Journal*.

In the Biography section, we record the speeches given when *David Piltz [was] Awarded the 2022 Charles Todd Medal*.

In the History of Telecommunications section, we reprint a “historical” paper from 2010 describing the *Marconi Wireless Telegraphy Trialled in Australia* in 1906.

As always, we encourage you to consider submitting articles to the *Journal* and we welcome comments and suggestions on which topics or special issues would be of interest.

## References

- Abbassi, Y., Toumi, H., & Ben Lahmar, E. H. (2022). A Proposal for Dynamic and Secure Authentication in IoT Architectures Based on SDN. *Journal of Telecommunications and the Digital Economy*, 10(4), 72–93. <http://doi.org/10.18080/jtde.v10n4.564>
- Al-Zoubi, A., Aldmour, M., & Aldmour, R. (2022). Preserving Transparency and Integrity of Elections Utilising Blockchain Technology. *Journal of Telecommunications and the Digital Economy*, 10(4), 24–40. <http://doi.org/10.18080/jtde.v10n4.626>

- Australian Government. (2021). NBN Co Limited—Statement of Expectations, 26 August 2021. Available at <https://www.infrastructure.gov.au/department/media/publications/nbn-co-limited-statement-expectations>
- Brett, J. (2022). A History of Reshaping Australian Telecommunications: A Review of John Doyle's *Crossed Lines: Disruption, Politics and Reshaping Australian Telecommunications*. *Journal of Telecommunications and the Digital Economy*, 10(4), 94–97. <http://doi.org/10.18080/jtde.v10n4.645>
- De Percy, M., Campbell, L., & Reddy, N. (2022). Towards an Australian Digital Communications Strategy: Lessons from Cross-Country Case Studies. *Journal of Telecommunications and the Digital Economy*, 10(4), 1–23. <http://doi.org/10.18080/jtde.v10n4.650>
- Moorhead, S. (2022). Marconi Wireless Telegraphy Trialled in Australia. *Journal of Telecommunications and the Digital Economy*, 10(4), 103–111. <http://doi.org/10.18080/jtde.v10n4.652>
- NBN Co. (2022). NBN Co Limited Statement of Expectations 19 December 2022. Available at <https://www.nbnco.com.au/content/dam/nbn/documents/about-nbn/policies/statement-of-expectations-2022.pdf>
- New Zealand Government. (2022). Te Rautaki Matihiko mō Aotearoa/The Digital Strategy for Aotearoa. Available at <https://www.digital.govt.nz/dmsdocument/237~the-digital-strategy-for-aotearoa/html>
- Sahli Sassi, A., Hammami, H., & Ben Lallouna Hafsia, H. (2022). Perceived Risk, Structural Assurance and Trust in Mobile Payments. *Journal of Telecommunications and the Digital Economy*, 10(4), 41–56. <http://doi.org/10.18080/jtde.v10n4.619>



# Towards an Australian Digital Communications Strategy

## Lessons from Cross-Country Case Studies

---

Michael de Percy  
University of Canberra

Leith Campbell  
RMIT University

Nitya Reddy  
University of Canberra

---

**Abstract:** In the early 21st century, governments developed national broadband plans to supply high-speed broadband networks for the emerging digital economy and to enable digital services delivery. Most national broadband plans are now focused on moving to ever faster networks, but there is a growing need to develop national digital communications strategies to focus on the demand-side of the broadband “eco-system”. In this paper, we outline the approaches adopted by the United States, Canada, the United Kingdom, Singapore, and Korea to assist in the development (or renewal) of Australia’s national broadband strategy, or, as we prefer, national digital communications strategy. The paper draws on the lessons learned from the case-study countries and the recent pandemic and considers some theoretical aspects of the broadband ecosystem. We conclude by suggesting a process to re-evaluate Australia’s national digital communications strategy as it rolls forward, and to incorporate recent international trends to develop demand-side policies to enable greater adoption and use of existing broadband infrastructure and digital services.

**Keywords:** Broadband connectivity, broadband demand, broadband supply, digital communications strategy, national broadband strategy

## Introduction

In the first decade of the 21st century, governments developed policies to enable residents to have improved access to broadband networks. In Australia, this trend was reflected in the successful 2007 federal election campaign by the Labor Party to support fixed broadband access to all premises, a policy that eventually led to the National Broadband Network (NBN)

provided by a government-owned company. At the same time, Mobile Network Operators (MNOs) were deploying ever more capable mobile broadband services. These deployments represent the *supply* side of a national broadband strategy.

In the second decade of the century and subsequently, attention has turned to the *demand* side of broadband. This is to ensure that all participants in the digital economy and digital society are able to use the broadband facilities that have been made available, driven by a range of social values, such as inclusion, fairness and equity. When TelSoc undertook an assessment of progress in Australia towards a national broadband strategy at the end of 2021 ([TelSoc Broadband Futures Group, 2021](#)), it found that there were some initiatives on the demand side but that they were generally of small scale and uncoordinated. Particularly after the COVID-19 pandemic, when online medical consultations and online education became widespread, it is no longer satisfactory to leave demand-side support to piecemeal solutions. A coherent, strategic approach is required for greatest effect ([ITU, 2022a](#)).

It is important to note at the outset that not all actions are in the hands of the government. Clearly, MNOs and other telecommunications-related companies and industry stakeholders have a major part to play in supplying broadband and digital services and in educating their customers on how best to use the facilities they provide. The role of government is assuredly to intervene directly in those places where the competitive market fails but also, more importantly, to define an overarching direction and set a policy that can offer guidance and can support ongoing investment by private companies. This is what we refer to as a national digital communications strategy.

This paper, then, looks at what has been undertaken in other jurisdictions and how effective these actions have been, in order to identify initiatives that could be undertaken in Australia as part of a national broadband strategy or, as we now prefer, a national digital communications strategy. The paper is arranged into four sections. The first section provides an overview of the policy approaches adopted by the case-study countries. The second section examines supply-side policies and the relevant outcomes on the basis of per capita take-up of broadband services. The third section considers demand-side policies and outcomes (where measurable) and the final section outlines an ongoing renewal process for an Australian national digital communications strategy based on the lessons learned from the case-study countries.

## Overview of the Case-Study Countries

All advanced economies and most countries have a “broadband plan” of some sort. Indeed, the ITU ([ITU & CISCO, 2013](#)) encourages all countries to do so. Australia could therefore draw inspiration from a wide variety of sources. We have selected case-study countries not just for

their direct relevance to Australia but also where innovative solutions have been implemented or where relevant challenges have been addressed. This section provides an overview of each of the case-study countries.

**The United States** is a rich and geographically diverse country in which there is a strong preference for private-sector solutions and a reluctance for government intervention. About 85% of US homes ([Martin, 2021](#)) have an Internet subscription. Nevertheless, the federal government has recognized that access to the Internet is an essential service and has identified unserved and underserved areas of the country ([FCC, 2010](#)). In recognition of the economics of broadband rollout, it has also identified “anchor institutions”, such as schools, hospitals, and government buildings, that should have high-speed Internet access. The interaction between the various levels of government in adopting these anchor institutions requires an interesting form of cooperative federalism, with federal leadership in broadband supply setting supply-side goals: a minimum of 100/50 (100 Mbps downstream towards end users; 50 Mbps upstream) broadband access to 100 million homes (about 82%) and at least 1 Gbps service to anchor institutions. On the demand side, it has recognized that affordability is not the only barrier to broadband take-up: a lack of digital skills or awareness can also limit access.

**Canada** is a geographically diverse country with responsibility for telecommunications divided between federal and provincial (state) governments and a dependence on private-sector initiatives. The emphasis has been on the provision of high-speed Internet services to rural areas, to match what is available in cities. There have been federal, provincial, and municipal initiatives, with the more populated provinces of Ontario ([Ontario Government, 2022](#)) and Quebec being particularly active.

**The United Kingdom** has a history of competitive mobile communications and an analytical and effective telecommunications regulator, Ofcom. The government and regulator have encouraged fibre access to homes and businesses over many years and the UK’s broadband supply strategy is focused on producing a 1Gbps service ([Hutton, 2022](#)). On the demand side, the government has recognized the need to encourage digital competence to address social, economic and equality gaps. It has also noted that trust is an important element in the decision to take up and use digital services ([Department for Digital, Culture, Media & Sport, 2022](#)).

**Singapore** is a country with a strong centralised government and an emphasis on economic development and international competitiveness. It views affordable broadband access as part of a “smart nation” development. On the supply side, it was one of the first nations to offer an affordable 1 Gbps service ([World Bank, 2018](#), p. 185). On the demand side, it has emphasised bringing low-income families and individuals online.

**South Korea** has used telecommunications technology as one mechanism for economic revival and development over the past 30 years. It established a world-leading mobile communications service through strong co-operation between the government and industry (industrial conglomerates). It then established widespread fixed Internet access through a variety of mechanisms. The continued co-ordination between government and advanced industries maintains South Korea as a high-tech nation. As a leader in broadband supply, it also is a place where social issues related to Internet usage first become apparent. Demand-side initiatives in municipal areas are helping residents to access digital government, transport, health, and financial services through hands-on assistance.

## Supply-Side Policies and Outcomes

In the early 2000s, most advanced economies focused on deploying infrastructure to provide access to broadband Internet services as a priority. While countries such as Korea and Canada, both early leaders in broadband supply, pursued deliberate strategies to bridge the digital divide, in other jurisdictions, digital literacy was, for the most part, a secondary matter to the provision of broadband infrastructure in the first decade of the 21<sup>st</sup> Century. Although the supply-side focus rested on a strategy of “build it and they will come” (ITU, 2012, p. 70), a focus on digital literacy posed a chicken-and-egg quandary for many administrations, with concern that supply and demand might be imbalanced one way or the other for long periods. As with most networked technologies, historical legacies and previous adoption patterns suggest there is no single optimally affordable way to deploy broadband networks: the variety of peculiarly local and national issues influence the type of technologies that have been or can be adopted and therefore the policy approaches that can be employed to stimulate further deployments.

Hughes’ (1993, p. 405) research into electricity systems in Germany, the US, and the UK found that local conditions resulted in distinct technological styles in each jurisdiction. Hughes defined these conditions that existed external to the technology as cultural factors: “geographical, economic, organizational, legislative, contingent historical, and entrepreneurial conditions... factors [that] only partially shape technology through the mediating agency of individuals and groups”. However, electricity systems are passive networks where users have limited choices about how the network is deployed or used, whereas modern communications systems provide suppliers and end-users with a variety of choices about the means of delivery and the use of the services. Rather than “cultural factors”, the various connectivity requirements of users tend to reflect particular circumstances which must be taken into account by policymakers if they are to enable greater take-up of a particular technological function or use of a service. The varieties of particular individual, organisational,

geographic, demographic, and infrastructure situations that policymakers may need to address (while attempting to predict the current and potential uses of communications technologies in such various conditions) might be better defined as the *varieties of particularism* that encapsulate the diverse circumstances in each case-study country.<sup>i</sup> These distinct varieties of particularism are evident in the approach adopted by each of the case-study countries in deploying broadband infrastructure.

There are many different ways of achieving highspeed connectivity, and previous technology decisions can influence the policy choices available in the present. For example, Canada's proximity to US television broadcast stations led to the deployment of community antennas that later evolved into coaxial cable networks capable of delivering broadband. This led to platform-based competition between coaxial cable and digital subscriber line (DSL) providers in Canada; a situation that did not occur in Australia on a large scale. Similarly, high-density housing in Korea enabled rapid deployment of fibre networks that could not be achieved in Canada, the US, and Australia due to the large, sparsely populated areas to be connected. Using the measure of broadband subscriptions per 100 inhabitants, Korea ranks first of the case-study countries (and sixth overall in the OECD<sup>ii</sup>) with 44.16 subscriptions per 100 inhabitants, with 87% of those subscriptions utilising fibre networks (see Figure 1). Canada, ranked second in the case-study countries for fixed-line broadband, has 41.48 subscriptions per 100 inhabitants but with 50% of those services delivered over coaxial cable. The UK ranks third of the case-study countries and has 74% of its 41.08 fixed-line subscriptions per 100 inhabitants delivered via DSL. While the US ranks fourth and has 61% of its 38.45 subscriptions per 100 inhabitants delivered via coaxial cable, it must be noted that the US has more fixed-line subscriptions overall than all the other case-study countries combined. Australia ranks fifth and, despite the NBN rollout occurring over the last decade, has only 23% of its 35.53 subscribers per 100 inhabitants connected via fibre. Singapore lags the other case-study countries in fixed-line broadband with 25.81 subscriptions per 100 inhabitants but is ranked first for mobile broadband subscriptions with 144 subscriptions per 100 people, reflecting the mobile connectivity that can be achieved within Singapore's land area of only 728.6 km<sup>2</sup> (see Figure 2).

There are other interesting statistics that suggest there is an element of supplementation, complementation, and substitution in fixed-line versus mobile subscriptions. For example, all of the case-study countries have surpassed 100 mobile subscriptions per 100 inhabitants except Canada. Canadian mobile subscriptions are notoriously expensive, with facilities-based rather than service-based competition keeping prices among the highest in the OECD ([Barnea, 2022](#)).

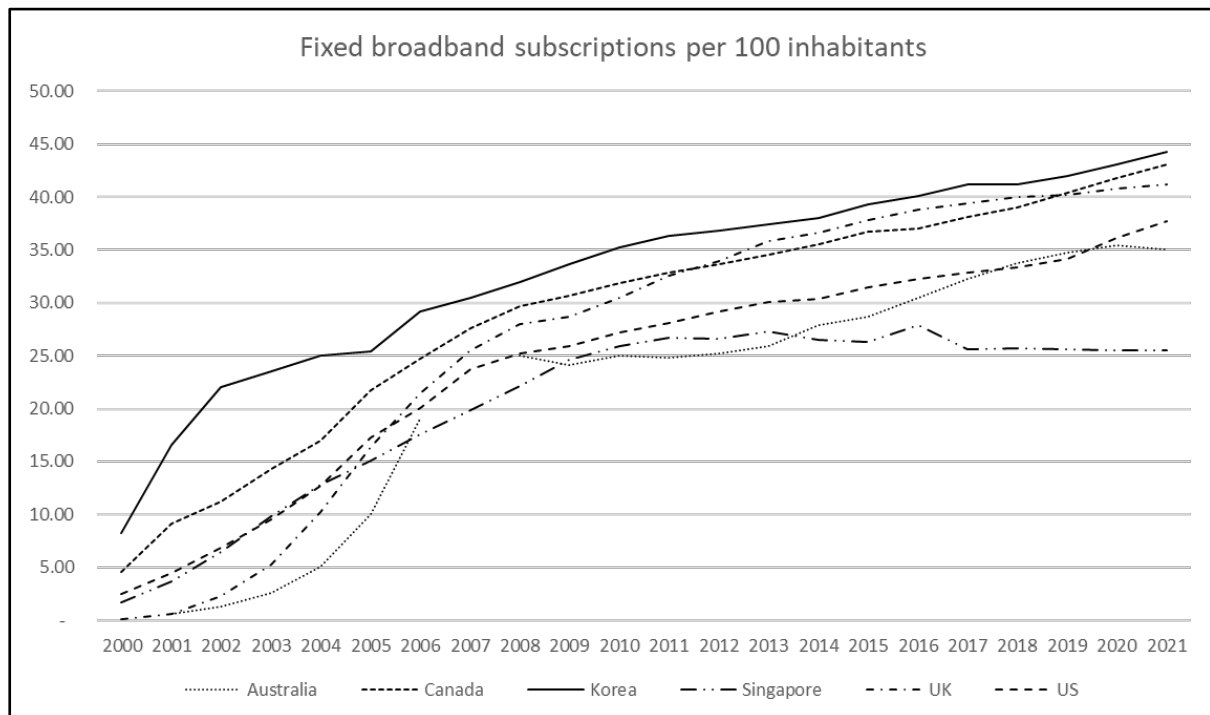


Figure 1: Fixed Broadband Subscriptions per 100 inhabitants (ITU, 2022b)

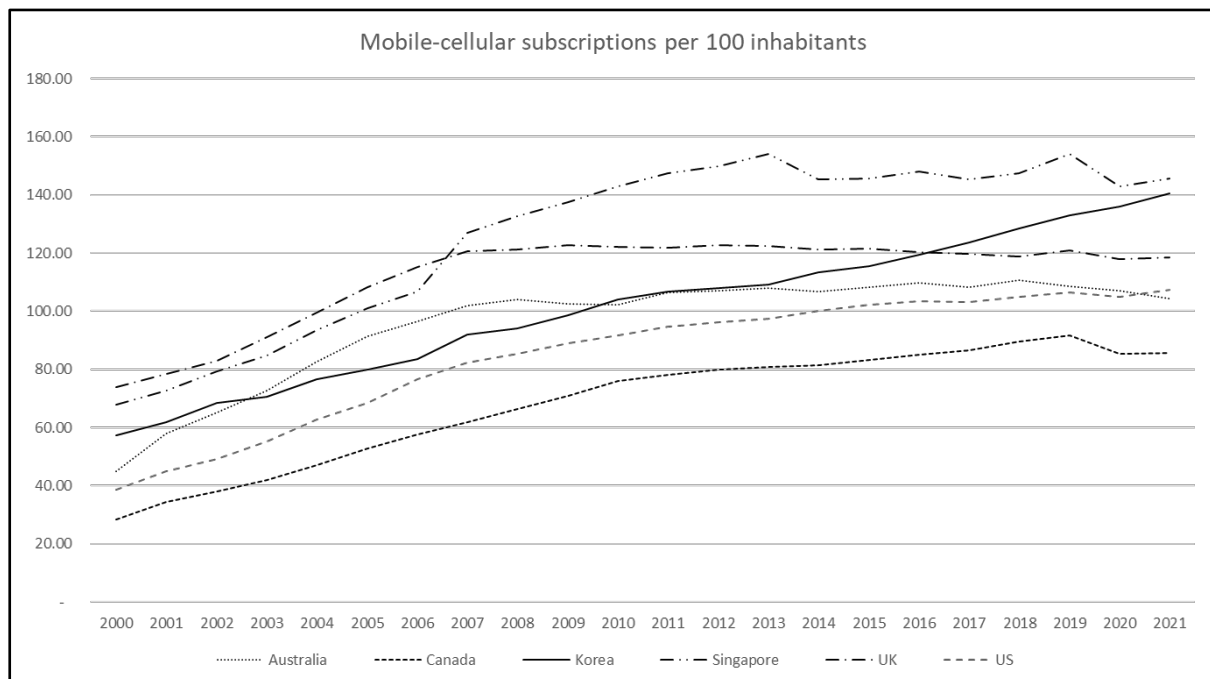


Figure 2: Mobile/Cellular Subscriptions per 100 Inhabitants (ITU, 2022b)

Korea was an early adopter and an early leader in broadband supply. However, the market-based philosophy adopted by Anglo liberal democracies contrasts sharply with that adopted by Korea, where policymakers:

...address all the components of the eco-system in an inter-connected fashion, generating incentives for broadband adoption in the areas of applications and services to follow through the build-up of broadband networks. Additionally, with support of a government research institute, the Korean Information Society

Development Institute (KISDI), policy makers in this country were able to develop and refine a broadband technology strategy based on rigorous economic analysis ([ITU, 2012](#), p. 71).

Korea's approach to deploying broadband and incorporating users early in the national broadband plan was key to addressing Korea's particular circumstances. For example, Korea is home to Samsung and LG, two major device manufacturers, with major research initiatives in next generation communications technologies focused on end-users, and a highly urbanised population with a large proportion living in apartment blocks, which makes it easier to connect subscribers to the broadband network than in large, sparsely populated countries like Australia, Canada, and the US. Koreans, generally, tend to be "tech-savvy" ([Budde, 2022](#)) and, led by the central government, have developed an over-arching strategy that began with the Korea Information Infrastructure project in 1995 ([Strand Consult, 2022](#)). However, government leadership has its limits once communications markets mature, with recent critiques of Korea's limited competition model forecasting higher prices in the near future ([Park & Nelson, 2021](#)).

Like Korea, Canada adopted a global leadership approach to the Internet (and later broadband) and, also from 1995, through the Information Highway Advisory Council (IHAC) and the policy leadership of then Minister for Industry John Manley, focused on "making Canada the most connected nation" ([d'Haenens & Proulx, 2000](#), p. 282). Industry Canada later developed IHAC into the Information Highway Applications Branch (IHAB) in Industry Canada to address areas where markets were not delivering broadband services. A key goal of IHAB was to develop "market aggregations" of local communities (including First Nations communities) to connect with various providers (including municipal and province-owned providers).<sup>iii</sup> The policy leadership was also implemented in the mandate of Canada's specialist regulator, the Canadian Radio-television and Telecommunications Commission (CRTC), and its policy aim of "regulatory forbearance" to restrict government interference in markets, while at the same time providing swift regulatory solutions to small service providers through an expedited complaints process where larger incumbent service providers were potentially conducting anti-competitive behaviour, especially in smaller communities where small-scale providers might otherwise deploy affordable or subsidised services that the incumbent service providers were reluctant to provide.

Over-arching this approach, according to many industry experts, the federal government focused on "facilitating, stimulating and legitimating" community involvement in the process of infrastructure deployment in areas of market failure (in areas where commercial incentives might be too weak or otherwise inappropriate for generating desired social, community and user outcomes) (see also Note iii). Alongside a technologically neutral approach, supported by



an independent municipal and provincial spirit stemming from constitutional arrangements that traditionally situated telecommunications powers with the provinces, local communities were able to develop broadband networks using a variety of technologies, including fibre, coaxial cable, and wireless. Canada was indeed an early leader in fixed broadband and, until recently, was first in the OECD rankings of the largest federated countries, yet Canada's penetration of mobile broadband has lagged Australia's (see Figures 1 and 2).

The US, largely responsible for the development of the Internet,<sup>iv</sup> is similar to Canada in that the embedded coaxial cable infrastructure remains the dominant network for broadband services. Similarly, Australia and the UK predominantly rely on DSL broadband services, reflecting the historical legacy of government ownership of the original telephone network and the absence of the pay-TV systems that dominated North America. Korea and Singapore, on the other hand, have some of the fastest fixed-line broadband speeds in the world and are both investing in 6G mobile technology and aiming to boost their fibre networks from 1 Gbps to 10 Gbps in the near future ([Low, 2022](#)).

## Framing a Technology Policy

There are some theoretical aspects of technology policy that must be addressed before considering the demand-side aspects of a national digital communications policy. Following on from Hughes' (1969) concept of *technological momentum*, a form of "soft" determinism that falls somewhere between *technological determinism* and *social constructivism*,<sup>v</sup> it can be said that "social development shapes and is shaped by technology" (Hughes cited in [Smith & Marx, 1994](#), p. 102). Technological momentum is therefore a "more complex concept than determinism or social construction" and it is also time dependent (Hughes cited in [Smith & Marx, 1994](#), p. 102). It can also refer to the:

...increase in the rate of: 1) the evolution of technology, 2) its infusion into societal tasks and recreations, 3) society's dependence on technology, and 4) the impact of technology on society" ([Dyer, 1995](#), p. 255).

Technological momentum, then, is a useful concept in explaining the evolution of broadband services in response to societal needs and the infusion of technology into how we live and work. In the analysis above, there are three groups of countries that have similar characteristics resulting from their cultural and historical trajectories. First, there is the North American model based on coaxial cable stemming from the deployment of cable networks well before the Internet was publicly available, combined with a blend of public, private, and community involvement in deploying broadband networks. Both Canada and the US lag the other case-study countries in mobile subscriptions, most likely resulting from issues of pricing. Second, the UK and Australia, with an historically government-owned Plain Old Telephone Service



(POTS) network with no competing platform, still rely on DSL. Although Australia and the UK have some fibre networks, the deployment of modern mobile networks has seen the take-up of mobile services in the UK and Australia surpass 100 subscriptions per 100 inhabitants. Third, Korea and Singapore, both formerly developing nations that have mobilised their collective efforts to bring greater standards of living and prosperity to their citizens in a matter of decades, have been able to deploy fibre networks and high-tech mobile networks, perhaps leap-frogging the embedded earlier technologies of the other case-study countries, no doubt helped by the high density housing on a small land area reducing the necessary investment when compared to Australia, Canada, and the US.

From the above analysis, three key issues emerge. First, those countries that focused on deploying fixed-line broadband services early on gained a significant advantage that was not readily overtaken by the other case-study countries. For example, Canada's early leadership in fixed-line broadband penetration continues to outpace Australia's, despite Australian taxpayers investing some \$44 billion in the NBN over the last decade (Baird, 2022). Second, solutions that take into account the varieties of particularism inherent in different jurisdictions, including political, economic, cultural, geographical, and historical conditions, *and the needs of users*, tend to result in better-connected populations. Third, a key role for government is not necessarily deploying publicly-owned infrastructure but for providing the leadership that *enables* the deployment of infrastructure, whether through policy incentives, regulatory forbearance or other measures that promote the involvement of all levels of the public, private, and civil society sectors in signalling demand or acting as anchor tenants for networks. The next section focuses on the most important component of the particular characteristics of a given jurisdiction, the users.

## Demand-Side Policies and Outcomes

Global COVID-19 lockdowns motivated an upsurge of digital interaction, encouraging government services, the health sector, educational institutions, and many employers to transition from traditional face-to-face to online interactions. Similarly, social distancing rules encouraged many families to commemorate births, funerals, marriages, graduations, birthdays, and other traditionally face-to-face events as online events using various digital platforms. It is interesting that the enabling technologies for online interactions on such a global scale were not *deterministic*, but rather *constructivist* in that social institutions adopted the technologies to adapt to pandemic restrictions (see Note **Error! Bookmark not defined.**). The motivated changes to the way we live and work resulted in an explosion of use of online interaction in all aspects of work and family life, in addition to streaming services adopted as a supplement for face-to-face entertainment activities (Weinschenk, 2020).

While demand for online interaction and entertainment increased the uptake of the gamut of digital services, it also exposed the importance of digital inclusion and demand-side policies to enable vulnerable groups, such as the elderly, to develop the digital literacy skills necessary to benefit from the available technologies ([Martínez-Alcalá et al., 2021](#); [Wheeler, 2020](#)). In advanced economies ([Muñoz-Najar et al., 2021](#), p. 24), the rapid uptake of pre-existing digital services during the pandemic suggests that, in addition to supply-side policies, there is considerable scope for making better use of existing services if appropriate demand-side policies can encourage more people to adopt these services. This section, then, discusses the relevant demand-side policies adopted by the case-study countries and the outcomes of these initiatives.

The demand for digital services during the pandemic highlighted institutional barriers that hinder the take-up of digital services. Indeed, the importance placed upon access to digital services resulted in initiatives to ensure ongoing supply of broadband services, particularly for those who could not afford the services as a result of income loss during the pandemic ([FCC, 2020](#)). Pandemic-related demand aside, institutional arrangements that may have previously been a barrier to take-up of digital services (such as the absence of subsidisation for telehealth consultations) were gradually removed as pandemic restrictions were applied in most jurisdictions.<sup>vi</sup> For example, justice systems enabled the use of electronic signatures and remote hearings ([Legg & Song, 2022](#)), and educational institutions that had previously only half-heartedly adopted online learning were forced almost overnight to move face-to-face classes and examinations completely online ([Muñoz-Najar et al., 2021](#)). Further, many legal, financial, and property services quickly adopted remote application and approval processes; and retail, food, and beverage firms adopted home delivery and other non-contact ways of buying and selling goods digitally. Again, most of these services were already available but the social and institutional arrangements had not kept pace with the available technologies ([UNCTAD, 2021](#)). Whether the post-pandemic era will perpetuate the “hybrid” way we live and work remains to be seen, but it is clear that many of the barriers to digital services were institutional rather than technological.

Pandemic-driven demand for digital services raised three key issues for accessibility, particularly for those who otherwise had avoided either using digital services or otherwise had no opportunity to develop digital skills. First, online health, medicine, financial, and government services are accessible for some, but not all residents. Elderly people and people with disabilities, for example, may find it challenging to navigate their way through digital services and often require hands-on assistance. Ng, Lim & Pang ([2022](#)) argue that the people who are least able to use online health, medicine, or government services and assistance may be those who require these services the most. The authors draw attention to the fact that “some

online services are accompanied by online guides, [but] these are not always easy to comprehend, especially for the less digitally or language literate” (Ng, Lim & Pang, 2022). To improve accessibility, the Singapore Government requested social service volunteers to step in and help their clients with booking appointments at clinics and employment agencies, and provide assistance with scanning, uploading and submitting online forms and documents. However, Ng, Lim & Pang (2022, pp. 7-8) highlight that, although these professionals can help the vulnerable, their “primary role is to provide social services and not technical support”. Therefore, to bridge this gap, the Singapore Government employed over 1,000 full-time professionals as part of the Digital Ambassadors initiative to provide one-on-one digital consultation. Furthermore, these ambassadors adopted an effective technique that categorised the targeted people into two groups: people who need additional support such as the elderly (Seniors Go Digital); and stallholders from food centres (Hawkers Go Digital) (Ng, Lim & Pang, 2022).

Not all accessibility programs were pandemic-driven. For example, over the previous decade, the UK’s “Get IT Together” program run by BT (formerly British Telecom) and “Go ON UK” program run by the Government Digital Service aimed to provide Internet access, skills training, and advice tailored to individual needs, in particular to the elderly, the disabled, and job seekers with no Internet access, and to do so in all four countries of the Kingdom and in the regions (Cabinet Office & Government Digital Service, 2014). These and other programs brought together the central and local governments with businesses and not-for-profit entities to provide a coherent and coordinated response to promoting digital inclusion. Similarly, in the US, the National Broadband Plan implemented by the Obama Administration considered policy interactions as part of an “ecosystem” approach to enabling “broadband capability”. The Plan focused on competition, efficient allocation and access to assets (such as spectrum, poles and wires, rights of way), and reform of laws, standards, and incentives to enable access in high-cost areas underserved by markets (FCC, 2010, p. xi). Further, the FCC’s (2022, p. 9) “ecosystem” approach to funding innovative programs to improve broadband capabilities complements markets by making all levels of government, tribal (Indigenous) organisations, educational, public service, and not-for-profit organisations and so on eligible for federal funding (see also Broadband Technology Opportunities Program, 2010). Nevertheless, the pandemic increased first-time digital customers in all sectors (including digital government services) at rates that, based on previous trends, might have taken years (SAS Institute, 2021).

Second, people require suitable devices (in addition to skills and a broadband subscription) to access digital services. For example, as online learning became the norm during the pandemic and students were obliged to participate, many institutions did not consider problems with access to devices in a low-income household, particularly those with more than one child

([Cain, 2021](#)). For example, pre-existing Singapore Government programs that enabled device ownership for low-income households were restricted to one laptop per household. These were subsequently amended to the “one device per learner” policy ([Ng, Lim & Pang, 2022](#)). Canadian school boards predominantly provide devices for students, but not generally to those in earlier stages of education. Some First Nations’ communities were forced to close schools altogether due to a lack of devices for students, many without home-based Internet connections. Even wealthier communities were affected by device shortages. For example, in January 2022, Ontario school boards, amid a shortage of devices, delayed the beginning of term to allow distribution, with some boards opting for a “one device per household” policy ([Alphonso, 2022](#)). Each case-study country has adopted a different approach to providing access to digital devices. For example, the US Government, under the Affordable Connectivity Program, provides low-income households with subsidised Internet connections (up to \$30 per month) and discounts on digital devices (up to \$100 per device), but only one per household ([The White House, 2022](#)).

Third, and given the swift uptake of digital services during the pandemic, cyber criminals have taken advantage of increased online users ([Dziedzic, 2022](#)) through hacking and identity theft, to the point where personal data has been ransomed in Australia. According to Rubinsztein-Dunlop *et al.* ([2022](#)), recent attempts by foreign criminal groups to ransom Australians’ personal data from the Optus and Medibank breaches are “only the tip of the iceberg”. Although a detailed assessment of cybersecurity is beyond the scope of this paper, for digital services to be advantageous, trust in the system and therefore its security are a major concern for any national digital communications strategy.

In the Australian context, there is a disconnect (that is not so evident in the other case-study countries) between the level of government responsible for telecommunications infrastructure (the Commonwealth) and the level of government responsible for most of the daily digital services that citizens access (the States and Territories). Most federal government digital services, such as taxation, social security, health, and veterans’ services, are currently operated through MyGov, whereas the various States and Territories and local governments have different platforms and approaches for licencing, registrations, and transport.

The NSW Government’s Service NSW app, for example, contains numerous services relating to an individual’s digital identity. Much like the leadership necessary to deploy broadband infrastructure, similar leadership is required to ensure digital services are delivered in a way that is most effective for users of the services. In NSW, the Hon. Victor Dominello MP holds the distinct portfolio of Minister for Customer Service and Digital Government. The Service NSW app has outclassed the Commonwealth’s attempt to establish the CovidSafe app during the pandemic, and, unlike the Australia Card in the Hawke Government era and recent

attempts to establish digital identities for Australian citizens, is now considered a world standard for digital government service delivery ([Bajkowski, 2022](#)). Importantly, Service NSW shopfronts provide an educative function by which a customer is assisted by staff to use the computer terminals to conduct their business. This level of service is replicated in regional areas where even services such as births, deaths, and marriages can be accessed on a regular basis via travelling Service NSW staff in purpose-built caravans who assist residents in regional and rural communities to access digital services that years previously required travel to large metropolitan centres like Sydney, Newcastle, or Wollongong.

From the analysis above, there are varieties of particularism that require bespoke solutions – there is “no one fits all” solution to the different needs of customers or the requirements of different cultures or jurisdictions. Even attitudes towards trust and privacy require different approaches and, oftentimes, coaching. The recent development of PayID functionality on mobile phones, for example, has changed the nature of socialising. Previously, many hospitality venues would not allow bill-splitting (typically due to the high cost of merchant fees), whereas digital services such as PayID enable customers to quickly and safely transfer funds between individuals in real time. Such advances suggest that an ecosystem approach, cognisant of the varieties of particularism and the momentum created between technology-driven services and socially constructed practices around the technology, requires an ongoing system of renewal that can adapt a national digital communications strategy to changing technologies and social practices. Governments can play a key role here in promoting the use of digital services and making proprietary services accessible through government-related transactions and other interactions with citizens and end-users. The next section, then, considers a conceptual renewal process for a national digital communications strategy.

## A Digital Communications Strategy Renewal Process

A broadband strategy lasting for 10 years cannot be just “set and forget”. A strategy should be re-evaluated periodically to ensure that it remains best positioned to deliver its aims. If it is not, it should be adjusted. In advanced economies, the shift in focus from infrastructure towards users is an important conceptual change in how we view broadband; hence, our preference for an Australian digital communications strategy (as opposed to a broadband strategy) that encompasses not only the deployment of infrastructure, but the opportunities for improvements in standards of living for users, including the most vulnerable in our societies.

One way to ensure that a strategy is periodically evaluated and adjusted as necessary is to put in place a *system* that provides regular feedback on the outcomes being achieved. In the case

of a national digital communications strategy, this involves tracking services, applications and users, as well as the availability and performance of broadband access networks.

Kim, Kelly & Raja (2010), in a report for the World Bank, think of this as an “ecosystem”. Their conception is presented in Figure 3. We can think of this as defining a broadband [re]evaluation cycle. As the authors say, a “broader conceptual framework leads to rethinking of the areas of focus for broadband policies and strategies” (Kim, Kelly & Raja, 2010, p. 16).

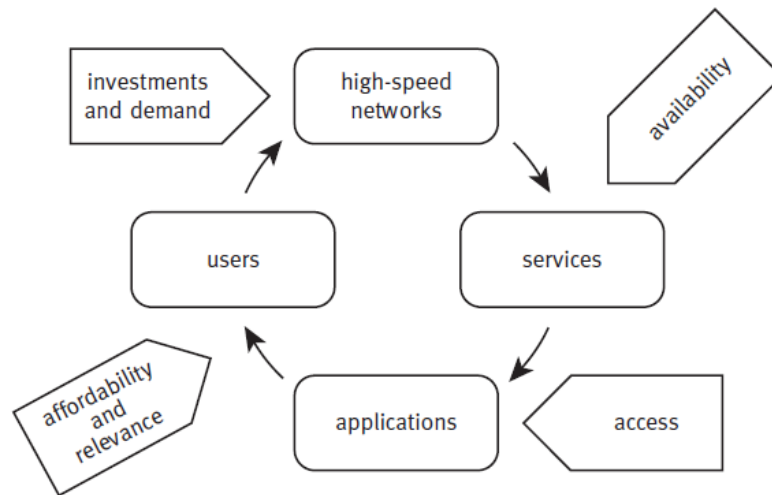


Figure 3. The Broadband Evaluation Cycle (Source: Kim, Kelly & Raja, 2010)

### High-speed networks

The focus in a national digital communications strategy has often been just on the availability and performance of high-speed networks and network access. This was, for example, the original conception of the NBN: provide network access to all premises in Australia at a specified minimum performance or better. But this, then, raises numerous questions. Should the network access really be provided to all premises? What about the ones which already have alternative access? At what level should the minimum performance be set? And why? These questions cannot be resolved without a wider understanding of the drivers for network availability. This is where an understanding of the broadband evaluation cycle is useful.

### Services

With greater availability of high-speed networks (both network access and high-speed long-distance transmission) comes greater availability of services. At the end-user level, services include IP connectivity and the attendant benefits of improved web browsing, cloud computing, access to corporate networks for remote working, and video streaming, for example. In addition, other services, not directly visible to end users, become economically feasible. Data centres can be built to supply vast data stores and computing facilities. Content Delivery Networks (CDNs), essentially private IP networks and data centres, can be deployed.



CDNs enable the mirroring of websites and storage of popular content nearer to end users, for example. All these generic services add greater capability and improved end-user performance to the underlying, high-speed, IP-based networks.

### Applications

Applications are built on and for high-speed networks and services. The more capable the networks and services, the more capable the applications. Social networking applications, for example, are able to synchronize content across many sites and users in near real time: this feature is built on high-speed networks and cloud computing. Banking applications are able to keep their customer data secure through public-key cryptography, secure firewalls and security features widely deployed in data centres. An important cluster of applications are those for e-government. The public sector is “a producer and user of digital content and applications – including those for education, health, culture, and economic activities” (Kim, Kelly & Raja, 2010, p. 25).

### Users

Users are people and other entities who use applications for interactions with businesses and government, or between themselves, or to upload content to or download content from the cloud. Users must be equipped with a suitable device, typically a computer or smartphone, for using applications, and a high-speed network access, either fixed or mobile, for interacting with other entities. In the end, a *national* communications strategy can only be considered successful if all citizens and residents are able to get access to and to use, effectively and efficiently, the applications they need to participate in the digital economy and digital society.

In periodically re-evaluating a national broadband strategy, the four participants – users, networks, services and applications – in the broadband development cycle need to be considered. A re-evaluation need not necessarily take in all aspects at once. The process is a *cycle*, meaning that identifying and overcoming a barrier to use in one aspect can lead on, around the cycle, to the development of greater capabilities in other areas.

### Re-evaluating a broadband strategy

Even in a country like Australia, where fixed and mobile broadband networks are well established, it is still worthwhile to ask periodically if they are achieving and maintaining appropriate support for the digital economy and digital society. For example, one might ask if the current take-up of fixed broadband – about 74% of households and businesses – is satisfactory. There may be operational barriers to connecting rental properties, for example, yet only if all rental properties come with a broadband access already in place will renters face

no physical barrier to taking up fixed broadband. The government could introduce incentives for landlords or tenants to install and use a fixed broadband connection.

The following subsections provide some notes on possible insights that could be obtained through periodic reviews.

### **Investments and demand**

While mobile broadband may be widely available, there is still a question if users are actually using the applications available. Some indirect data, like the distribution of monthly data volumes consumed by users, may indicate groups who are missing out through low cost, pre-paid plans with restrictive data limits. The distribution of data limits in actually used post-paid and pre-paid plans may also be informative. Of course, mobile service operators have extensive information on data usage and payments by their customers, but this information may not be made available either to government or publicly. Regulation on the industry to provide suitable customer data in an agreed form may be appropriate.

### **Availability**

Services are built on the availability of high-speed networks. For example, if only low-speed accesses are available in a certain area, then cloud computing will be severely restricted or non-functional in that area.

Evidence for the deployment of services may be gained from actual user data or may be found in business expansion or investment. For example, nine new data centres are being built in regional NSW in response to the expansion of the NBN and NSW government initiatives ([Adams, Inglis & Proctor, 2022](#)).

### **Access**

Applications need access to high-speed networks and the services they provide. Applications are built on the assumption of some level of access. If an application, such as a social-media platform, for example, depends on cloud computing and the cloud computing services are not readily available in an area, then the application will work less effectively or not at all in that area. Understanding what applications are popular and being used will give some information on what network and service capabilities are required. Customer complaints about the unavailability of an application or problems with using it will identify services or network capabilities that should be provided. The use of e-government applications can provide direct data for government.



## Affordability and relevance

If an application is not relevant to users, they will not use it. If an application should be relevant to a wide range of users (e.g., e-health records) and is not being used, then one needs to ask what barriers are stopping it being used. This could involve a lack of appropriate network or service support, or it may be due to access to the application being unaffordable.

On the other hand, popular applications, such as video streaming or 4K-quality television, may be affordable in some areas and not in others. This may indicate a mismatch between where the revenue is received and where investment costs are incurred. The apparent mismatch in revenues between “over-the-top” applications and telecommunications operators is an ongoing issue and is likely to be resolved only through government action or regulation. (The Australian government undertook to resolve a similar mismatch in advertising revenues between online news disseminators and newspapers ([Wilding, 2021](#))).

## Conclusion

TelSoc’s earlier focus on a pathway towards an Australian National Broadband Strategy was a necessary first step in supporting the ongoing enhancement and usage of the National Broadband Network. And, while there is still some way to go in terms of bringing this important infrastructure to all Australians, the pandemic proved that more needs to be done to enable citizens to take advantage of digital services. To that end, we recommend that future iterations of the strategy refer to an *Australian Digital Communications Strategy*, which is broader in scope than just broadband network development. This would bring Australia’s policy focus into line with the latest international thinking on broadband services being one part of an “ecosystem” approach, as outlined above.

One major challenge for an Australian Digital Communications Strategy is that many aspects of our daily lives are intertwined with three different levels of government. Health and education services, for example, and many identity-driven services, such as transport and recreational pursuits, are regulated by State governments. This means that any national strategy will require the co-operation of the States and local governments for it to be effective. Government financial support for telecommunications networks and associated accessibility programs under the authority of section 51(v) of the Australian Constitution tends to avoid direct support for State and local governments and community groups. This is in contrast with the US, where the focus is more on unserved and underserved communities in bringing digital services to the people.

Rather than a coordinated approach, the Republic of Korea provides a coherent approach that encourages action in the ecosystem, rather than trying to direct results as tends to be the case

in Singapore. The lessons from Canada point to an interesting combination of coherence and coordination that do not prevent local and provincial (state) initiatives from functioning, while at the same time coordinating actions where these intersect with the various jurisdictions.

Given the write-down of some \$31 billion of NBN recovery of capital costs at the time of writing (Baird, 2022), there is an opportunity to re-focus. The strategy needs to cover many moving parts and needs to involve and engage many diverse groups and stakeholders. Although this means the ecosystem is very complex, the strategy needs to be definite and certain. Although the semantics of rebadging the Australian Broadband Strategy as an Australian Digital Communications Strategy may seem petty stuff, we suggest that thinking beyond the NBN and adopting an ongoing process of renewal that encompasses all elements of the ecosystem in any strategic plan is key to our digital future. The most successful case-study countries examined in this paper all displayed policy leadership in adoption and use of digital communications technologies. An Australian Digital Communications Strategy provides the Australian government with an opportunity for such leadership.

## Acknowledgements

The authors wish to acknowledge the support of the University of Canberra and TelSoc for creating the opportunity for Nitya Reddy to participate in an industry-based internship as part of her university studies.

## References

- Adams, P., Inglis, S., and 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>
- Alphonso, C. (2022, 4 January). As online learning looms in Ontario, school boards face device shortages. *The Globe and Mail*. <https://www.theglobeandmail.com/canada/article-ontario-school-boards-face-device-shortages-as-online-classes-loom/> (Accessed 1 December 2022).
- Baird, L. (2022, 1 December). NBN writes off recovering \$31b invested to build network. *Australian Financial Review*. <https://www.afr.com/companies/telecommunications/nbn-writes-off-recovering-31b-of-government-investment-20221201-p5c2xv> (Accessed 2 December 2022).
- Bajkowski, J. (2022, 18 August). Dominello to dump politics, goes flat out on digital identity. *The Mandarin*. <https://www.themandarin.com.au/197373-dominello-to-dump-politics-goes-flat-out-on-digital-identity/> (Accessed 3 December 2022).
- Barnea, A. (2022, 2 April). Even after a decline in rates, wireless plans in Canada are still ridiculously expensive. *Toronto Star*. <https://www.thestar.com/business/opinion/2022/04/02/even-after-a-decline-in->

- [rates-wireless-plans-in-canada-are-still-ridiculously-expensive.html](#) (Accessed 3 December 2022).
- Broadband Technology Opportunities Program. (2010). *The Broadband Technology Opportunities Program: Expanding Broadband Access and Adoption in Communities Across America: Overview of Grant Awards*. Washington, DC: National Telecommunications and Information Administration. [https://www.ntia.doc.gov/files/ntia/publications/ntia\\_report\\_on\\_btop\\_12142010.pdf](https://www.ntia.doc.gov/files/ntia/publications/ntia_report_on_btop_12142010.pdf) (Accessed 1 December 2022).
- Budde, P. (2022). South Korea Telecoms Market Report: Telecoms, Mobile and Broadband - Statistics and Analyses. Sydney: Budde Comm. <https://www.budde.com.au/Research/South-Korea-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses> (Accessed 3 December 2022).
- Cabinet Office and Government Digital Service. (2014). *Policy Paper: Government Digital Inclusion Strategy*. London: Government of UK. <https://www.gov.uk/government/publications/government-digital-inclusion-strategy/government-digital-inclusion-strategy> (Accessed 30 November 2022).
- Cain, A. (2021, 17 April). Pandemic delivers lessons in online learning. *Australian Financial Review*. <https://www.afr.com/work-and-careers/education/pandemic-delivers-lessons-in-online-learning-20210412-p57ikx> (Accessed 1 December 2022).
- D'Haenens L. and Proulx, S. (2000). The Changing Stance of the Canadian Government in an Age of Globalization and Information. *International Communication Gazette*, 62(3-4), 281-299. <https://doi.org/10.1177/0016549200062003007>.
- Department for Digital, Culture, Media & Sport. (2022). *Policy Paper: UK Digital Strategy*. London: Government of UK. <https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy> (Accessed 30 November 2022).
- de Percy, M.A. and Batainah, H. (2021). Identifying historical policy regimes in the Canadian and Australian communications industries using a model of path dependent, punctuated equilibrium, *Policy Studies*, 42(1), 42-59. <https://doi.org/10.1080/01442872.2019.1581161>.
- Dyer, D. (1995). Too Much Too Fast: The Dangers of Technological Momentum. In Proceedings of the 1995 Annual National Convention of the Association for Educational Communications and Technology, Anaheim, CA. <https://eric.ed.gov/?id=ED383309> (Accessed 2 December 2022).
- Dziedzic, S. (2022, 4 November). Cybercrime reports jump as criminal gangs target families and businesses, cybersecurity agency says. *ABC News*. <https://www.abc.net.au/news/2022-11-04/cyber-crime-reports-jump-acsc/101612978> (Accessed 30 November 2022).
- Federal Communications Commission (FCC). (2010). *Connecting America: The National Broadband Plan*. Washington, DC: FCC Omnibus Broadband Initiative. <https://transition.fcc.gov/national-broadband-plan/national-broadband-plan.pdf> (Accessed 30 November 2022).

- Federal Communications Commission (FCC). (2020). *Keep Americans Connected*. Washington, DC: FCC Initiatives. <https://www.fcc.gov/keep-americans-connected> (Accessed 30 November 2022).
- Federal Communications Commission (FCC). (2022). *Notice of Funding Opportunity: Affordable Connectivity Outreach Grant Program*. Washington, DC: FCC. [https://www.fcc.gov/sites/default/files/acp\\_outreach\\_grant\\_program\\_nofo.pdf](https://www.fcc.gov/sites/default/files/acp_outreach_grant_program_nofo.pdf) (Accessed 1 December 2022).
- Hughes, T.P. (1969). Technological Momentum in History: Hydrogenation in Germany 1898-1933. *Past & Present*, August, 44: 106-132.
- Hughes, T.P. (1993). *Networks of Power: Electrification in Western Society, 1880-1930*. Baltimore: Johns Hopkins University Press.
- Hutton, G. (2022). Gigabit-broadband in the UK: Government targets and policy. London: House of Commons Library. <https://researchbriefings.files.parliament.uk/documents/CBP-8392/CBP-8392.pdf> (Accessed 1 October 2022).
- International Telecommunication Union (ITU). (2012, April). *The Impact of Broadband on the Economy: Research to Date and Policy Issues*. Geneva: ITU. [https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports\\_Impact-of-Broadband-on-the-Economy.pdf](https://www.itu.int/ITU-D/treg/broadband/ITU-BB-Reports_Impact-of-Broadband-on-the-Economy.pdf) (Accessed 30 November 2022).
- International Telecommunication Union (ITU). (2022a). *About Digital Services and Applications*. Geneva: ITU. <https://www.itu.int/en/ITU-D/ICT-Applications/Pages/about-ict-applications.aspx> (Accessed 1 December 2022).
- International Telecommunication Union (ITU). (2022b). *Statistics*. Geneva: ITU. <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx> (Accessed 2 December 2022).
- International Telecommunication Union (ITU) and CISCO. (2013). *Planning for Progress: Why National Broadband Reports Matter*. Geneva: Broadband Commission, ITU.
- Kim, Y., Kelly, T., & Raja, S. (2010). *Building Broadband: Strategies and Policies for the Developing World*. Washington, DC: World Bank. <https://doi.org/10.1596/978-0-8213-8419-0>.
- Legg, M. and Song A. (2021). The Courts, the Remote Hearing and the Pandemic: From Action to Reflection. *UNSW Law Journal*, 44(1), 126-166.
- Low, D. (2022, 19 September). Fibre broadband speeds to be boosted among upgrades to S'pore's digital connectivity. *Straits Times*. <https://www.straitstimes.com/tech/tech-news/fibre-broadband-speeds-to-be-boosted-among-upgrades-to-spores-digital-connectivity-josephine-teo> (Accessed 3 December 2022).
- Martin, M. (2021, 21 April). *Computer and Internet use in the United States: 2018: American Community Survey Reports*. Washington, DC: United States Census Bureau. <https://www.census.gov/library/publications/2021/acs/acs-49.html> (Accessed 30 November 2022).
- Martínez-Alcalá, C.I., Rosales-Lagarde, A., Pérez-Pérez, Y.M., Lopez-Noguerola, J.S., Bautista-Díaz, M.L., and Agis-Juarez, R.A. (2021). The Effects of Covid-19 on the

- Digital Literacy of the Elderly: Norms for Digital Inclusion. *Frontiers in Education*, 6: 1-19. <https://doi.org/10.3389/feduc.2021.716025>.
- Muñoz-Najar, A., Gilberto, A., Hasan, A., Cobo, C., Azevedo, J.P., and Akmal, M. (2021). *Remote Learning During COVID-19: Lessons from Today, Principles for Tomorrow*. Washington, DC: World Bank. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/160271637074230077/remote-learning-during-covid-19-lessons-from-today-principles-for-tomorrow> (Accessed 1 December 2022).
- Ng, I., Lim, S., and Pang, N. (2022). Making universal digital access universal: lessons from COVID-19 in Singapore. *Universal Access in the Information Society*, Apr 15, 1-11. <https://doi.org/10.1007/s10209-022-00877-9>.
- Ontario Government. (2022). Governments of Canada and Ontario announce more than \$56 million in new funding to bring high-speed Internet access to thousands more households. Press Release. Ottawa: King's Printer for Ottawa. <https://news.ontario.ca/en/release/1002061/governments-of-canada-and-ontario-announce-more-than-56-million-in-new-funding-to-bring-high-speed-internet-access-to-thousands-more-households> (Accessed 1 October 2022).
- Park, K.S. and Nelson M.R. (2021). Afterword: Korea's Challenge to the Standard Internet Interconnection Model. In Feigenbaum, E.A. and Nelson, M.R. (Eds.) *The Korean Way With Data How the World's Most Wired Country Is Forging a Third Way*. Washington, DC: Carnegie Endowment for International Peace.
- Rubinsztein-Dunlop, S., Hui, E., Curnow, S. and Nguyen, K. (2022, 28 November). Cyber black market selling hacked ATO and MyGov logins shows Medibank and Optus only tip of iceberg. *ABC News*. <https://www.abc.net.au/news/2022-11-28/cyber-black-market-shows-medibank-optus-hack-just-the-surface/101700974> (Accessed 3 December 2022).
- SAS Institute. (2021). Experience Disrupted: Is COVID-19 Continuing to Change Customer Behaviour? Cary, NC: SAS Institute. <https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/ebooks/en/experience-disrupted-is-covid-19-continuing-to-change-customer-behaviour.pdf> (Accessed 1 December 2021).
- Services Australia. (2022). *Changes to MBS Items*. Canberra: Australian Government. <https://www.servicesaustralia.gov.au/changes-to-mbs-items-during-coronavirus-covid-19-response?context=20#a1> (Accessed 1 December 2022).
- Sinnott-Armstrong, W. (1999). Some Varieties of Particularism. *Metaphilosophy*, 30(1/2), 1-12. <https://doi.org/10.1111/1467-9973.00108>.
- Smith, M.R. and Marx, L. (1994). *Does Technology Drive History? The Dilemma of Technological Determinism*. Cambridge: MIT Press.
- Strand Consult (2022, 12 November). South Korea takes the next step in global broadband leadership with the Network Free Ride Prevention Act. <https://strandconsult.dk/south-korea-takes-the-next-step-in-global-broadband-leadership-with-the-network-free-ride-prevention-act/> (Accessed 3 December 2022).



- 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>.
- United Nations Conference on Trade and Development (UNCTAD). (2021, 15 March). How COVID-19 triggered the digital and e-commerce turning point. Geneva: UNCTAD. <https://unctad.org/news/how-covid-19-triggered-digital-and-e-commerce-turning-point> (Accessed 1 December 2021).
- Weinschenk, C. (2020, 4 May). OpenVault: Pandemic Drives Almost a Year's Worth of Broadband Traffic Growth in the Span of a Couple of Weeks. *telecompetitor*. <https://www.telecompetitor.com/openvault-pandemic-drives-almost-a-years-worth-of-broadband-traffic-growth-in-the-span-of-a-couple-of-weeks/> (Accessed 30 November 2022).
- Wheeler, T. (2020, 27 May). 5 steps to get the internet to all Americans: COVID-19 and the importance of universal broadband. Washington, DC: Brookings Institution. <https://www.brookings.edu/research/5-steps-to-get-the-internet-to-all-americans/> (Accessed 1 December 2022).
- White House, The. (2022). Get Internet: Claim Your Affordable Connectivity Program Benefit. Washington, DC: The White House. [https://www.whitehouse.gov/getinternet/?utm\\_source=getinternet.gov](https://www.whitehouse.gov/getinternet/?utm_source=getinternet.gov) (Accessed 1 December 2022).
- 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>.
- World Bank. (2018). *Innovative Business Models for Expanding Fiber-Optic Networks and Closing the Access Gaps*. Washington, DC: World Bank.

## Endnotes

- <sup>i</sup> The term is borrowed from moral philosophy where it is used to explain a form of morality in which particular circumstances dictate particular approaches to morality, on a case-by-case basis, as opposed to a single moral principle that dictates all action (see [Sinnott-Armstrong, 1999](#)).
- <sup>ii</sup> OECD Broadband Portal, <https://www.oecd.org/digital/broadband/broadband-statistics/>.
- <sup>iii</sup> According to interviews with industry elites conducted by one of the authors in Canada in 2007.
- <sup>iv</sup> Through the Department of Defense's funding of ARPANET – the hardware – as opposed to the UK's claim to have developed the World Wide Web – the software – under the auspices of Tim Berners-Lee.
- <sup>v</sup> There are two key opposing theories of the interaction between human society and technology: *technological determinism*, where technology shapes human action; and *social constructivism*, where human action shapes technology ([de Percy & Batainah, 2021](#), pp. 43–44). Clearly, the pandemic revealed that societal needs prioritised the adoption of pre-existing online interaction technologies *en masse*, as opposed to the technologies being the driver for large-scale societal change. Technological

---

momentum sits somewhere between these two key theories, acknowledging that a theory that claims to both affirm and deny a particular phenomenon is tautological.

<sup>vi</sup> There are many examples of policies designed to keep people connected during the pandemic. These included enabling the Medicare Benefits Schedule for some telehealth consultations in Australia ([Services Australia, 2020](#)), and a raft of programs in the US through the Keep Americans Connected program ([FCC, 2020](#)). Whether such barriers will remain permanently removed in all jurisdictions remains to be seen.

# Preserving Transparency and Integrity of Elections

## Utilising Blockchain Technology

---

**Abdallah Al-Zoubi**

Princess Sumaya University for Technology, Jordan

**Mamoun Aldmour**

Staffordshire University, UK

**Rakan Aldmour**

Staffordshire University, UK

---

**Abstract:** Digital voting is increasingly important in both established and emerging democracies. Some of the advantages of digital voting are faster vote count and tabulation; accurate results; increased voters' participation and convenience; and effective handling of complex electoral system formats that require laborious counting procedures. However, transparency, credibility, and integrity concerns, as well as the limited possibility of recount, usually make traditional digital voting systems unpopular. Digital voting using blockchain technology, however, is safe, transparent, and immutable, which makes it a suitable choice for future decentralized voting systems. In particular, the Ethereum blockchain is proposed as an appropriate platform for the backbone of an e-voting system due to its widespread use, transparency, consistency and provision of smart contracts. Initial piloting on the implementation of a blockchain-based voting framework in Jordan shows promising results on its transparency and integrity by incorporating a space for representatives and observers to monitor the election procedure and results as an additional measure to ensure its efficiency and reliability. The uptake of the proposed system calls for further debate and dialogue amongst governments and people, especially in developing countries where democracy is still in its infancy.

**Keywords:** e-Voting System, Blockchain Technology, Ethereum Platform, Digital Applications.

## Introduction

Automatic voting systems are as old as democracy itself. An innovative method to safeguard against voter fraud while maintaining a sense of transparency using a ballot box containing a glass globe mounted in a frame was proposed by Samuel C. Jollie in 1858 ([Jones, 2009](#)). Early



voting machines consequently dispensed entirely with any form of durable ballot and, in so doing, they provided reasonable secrecy. The first pushbutton voting machine appropriate for use in a general election in the United States was introduced by Anthony Beranek in 1881, thereafter improved and suggested by Jacob H. Myers in 1892. Four types of e-voting systems have mainly dominated the landscape since: direct recording electronic (DRE) voting machines; optical mark recognition (OMR); electronic ballot printers (EBPs); and Internet voting, where votes are cast from anywhere and transferred to a central counting server. In fact, digital voting commenced in the early 1960s by utilizing punched cards and subsequently evolved from basic transmission of tabulated results to a full-function online voting process. The degree of automation varied from marking a paper ballot to a comprehensive system encompassing vote input and recording, data encryption and transmission to servers, and consolidation and tabulation of election results ([Abuidris et al., 2019](#)).

Estonia was the first country to fully implement an electronic voting system in local elections in 2005, and has since been legally bound to hold general elections using the Internet as a means of casting votes ([Tsahkna, 2013](#)). Today, there are over 34 countries which adapt and implement electronic voting in parliamentary elections, Pakistan being the latest when its National Assembly passed a bill approving electronic voting machine (EVM) voting as recently as November 2021. However, the main concerns with digital voting are security, privacy, trust, accuracy, and cost-effectiveness. Citizens worldwide are concerned about election security and integrity, particularly power interference, technical failure or mismanagement, hacking, fraud, forgery and unauthorised voting, as well as the manipulation of results ([Kshetri & Voas, 2018](#)). In addition, digital voting systems must comply with national and international standards and regulations. In fact, several countries, including Germany and Netherlands ([Loeber, 2014](#)), have abandoned e-voting in elections due to reliability issues, while others still endorse it ([Jain, 2019](#)). Certain voting machines are also prone to unexpected and inconsistent errors, making it difficult to ensure the authenticity, transparency and accuracy of results.

Kshetri and Voas proposed a blockchain-enabled e-voting system in 2013 that offers a solution to most of the existing problems of e-voting systems, as data is decentralised and distributed in a database shared by a peer-to-peer network. Every node in the network keeps a copy of voting data and stores it in blocks, which are chained together to make the ledger. The ledger may then be accessed by everyone in the network, thus ensuring the authenticity and transparency of voting data records. Blockchain-based voting may thus reduce fraud and increase accessibility over the Internet through computers and smartphones with encrypted-key and tamper-proof personal identification. Several blockchain-enabled voting systems have since been implemented with a variety of technologies and various degrees of uptake and success in several countries, including India, Russia, Malaysia, Colombia and Pakistan ([Jafar,](#)

[Aziz & Shukur, 2021](#); [Giraldo, Barbosa Milton & Gamboa, 2020](#); [Crowcroft, 2019](#); [Syed et al., 2019](#); [Sherman et al., 2019](#)). In fact, blockchain technology uptake is globally sweeping the financial, business and public administration landscape with a significant scale of adoption in applications at organisations and institutions, in addition to an expectation of a massive \$3.1 trillion worth of investments in the technology by 2030 ([Madaan, Kumar & Bhushan, 2020](#)).

In this paper, a blockchain voting system is proposed utilising the Ethereum platform, smart contracts, and supported by a decentralised database. The proposed blockchain system may offer citizens the opportunity to vote anonymously and transparently, to keep participants' records, and to ensure fraud-free results. A pilot experiment is designed to simulate an election in Jordan and to test its integrity and transparency with online presence of candidate representatives and worldwide independent observers to monitor the process and endorse its integrity.

## Blockchain Technology

Blockchain was first introduced in 2008 as a ledger to execute bitcoin transactions across a distributed network to provide a mechanism for remote nodes to reach consensus on the state of a ledger of information ([Hoiss, Seidenfad & Lechner, 2021](#)). Blockchain technology has actually moved over the years from the phase of inception to rapid development and practical applications. A blockchain actually consists of data blocks linked together in a sequential order forming a continuous chain of immutable records, which are permanent and tamperproof. The chain begins with a genesis block that records the first transactions. The block is also assigned an alphanumeric string called a hash, which it uses to create its own hash to link to the next block. Each block is given a number and contains data on transactions and a time stamp of the event, its own hash address and that of the previous block. Blockchain also uses a computational process called consensus to validate a block's authenticity before it can be added to the chain. The nodes on the blockchain network must agree to the hash of the new block by verifying its correct calculation. Consensus ensures that all copies of the distributed ledger are in the same state. Each computer in the network thus maintains a copy of the ledger to avoid a single point of failure ([Sheldon, 2021](#); [Jeyasekar, 2020](#)).

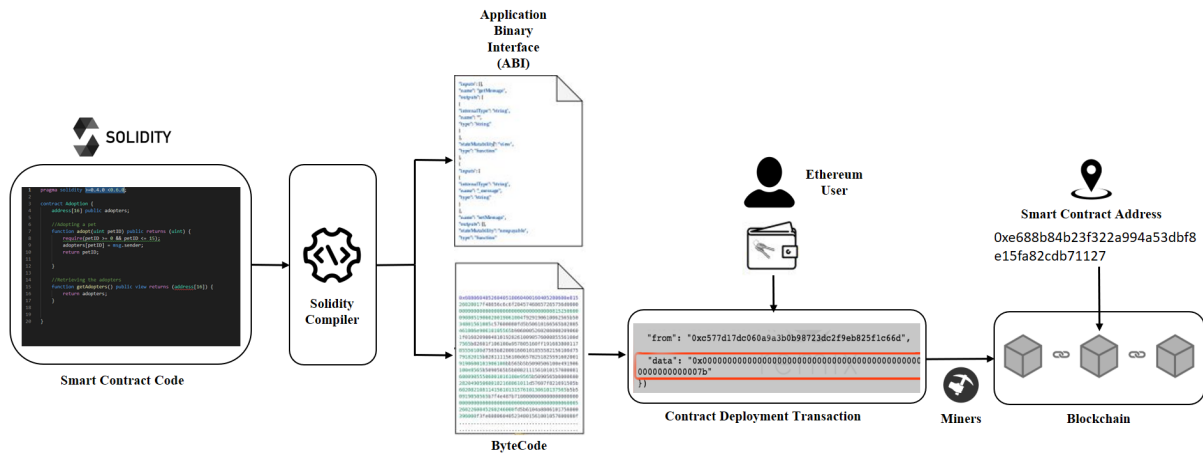
Blockchain is actually based on technologies that existed long before bitcoin appeared, such as the Merkle tree, which was proposed in 1979 to provide a data structure for verifying public records and digital signatures, and enabling multiple document certificates to live on a single block. In addition, mutually suspicious groups embody many of the elements of blockchain in the vault system established by David Chaum in 1979 to maintain and trust computer systems ([Sherman et al., 2019](#)). Actually, the vault system is a public record-keeping arrangement where group members follow private transactions that protect individual privacy through

physical security. The concepts of peer-to-peer (P2P) network and proof-of-work (PoW) to verify computational effort and deter cyberattacks also played an important role in the evolution of blockchain ([Vivek et al., 2020](#)). Recently, blockchain was introduced in electronic voting systems due to its attractive feature of end-to-end verification ([Hardwick et al., 2018](#); [Awsan & Othman, 2021](#); [Puneet et al., 2021](#); [Anggorojati, 2020](#)).

In 2014, Vitalik Buterin introduced the Ethereum platform as a decentralized open-source application with smart contract functionality, which extended the utilisation of blockchain technology beyond cryptocurrency ([Buterin, 2014](#)). Consequently, Ethereum provided developers with a platform for building decentralised applications in almost any field, utilising smart contracts that could be deployed to a live network because it is a secure, immutable, traceable and transparent platform. Ethereum has actually implemented smart contracts and provided developers with a means for application developments in many fields. Industries immediately began to recognise and explore the potential of blockchain and, as of the year 2014, the focus shifted from digital currency to the utilisation and development of blockchain applications beyond the financial landscape. The platform has actually attracted an active developer community that continues to this day. In fact, Ethereum network transactions exceeded 1 million per day in 2019, and consequently the Ethereum Foundation launched the Beacon Chain in preparation for Ethereum 2.0 ([Cortes-Goicoechea & Bautista-Gomez, 2021](#)).

The smart contract is a collection of code and data that resides at a specific address with a hash 66 characters long, and lives on the blockchain in an Ethereum-specific binary format called Ethereum Virtual Machine (EVM) bytecode, as shown in Figure 1. One may enter the address into a block explorer; like Etherscan, to see all of the transactions associated with the contract. A contract application binary interface or Arbitrary Binary Interface (ABI) is the standard way to interact with contracts in the Ethereum ecosystem, both from outside the blockchain and for contract-to-contract interaction. The smart contracts are deployed on Ganache, which only executes the byte-code representation. The ABI serves as an interface between two program modules. It defines how data structures and functions are accessed in machine code. When the compilation is successful, the smart contract can be deployed using a particular contract deployment transaction. When a transaction is executed, the contract can be referred to by its address, calculated as a hash function of the originating account and account nonce (number of transactions originated from an account). Consequently, the Ethereum user utilizes the address and ABI to interact with a smart contract. Hashing, a vital feature in blockchain operation, is the cryptographic process of converting an arbitrary input of variable size to an output of fixed size using a complex mathematical algorithm. Ethereum utilizes Keccak-256 hashing in a consensus engine called Ethash. Keccak-256 is part of the Secure Hash Algorithm (SHA)-3 standard released by the US National Institute of Standards and Technology (NIST)

in 2015, but with slightly different parameters than the current SHA-3. It generates a cryptographic hash function that yields a 160-bit hash value consisting of 40 hexadecimal characters.



### Figure 1. Blockchain Principle of Operation

There are two types of accounts in Ethereum, the first being an externally owned account (EOA), which is identified by a wallet address and controlled by a private key whose holder can transfer Ethers cryptocurrency and sign transactions. EOAs are linked to unique cryptographic key pairs, generated upon account creation. The public key address is used to reference the account, whereas the private key is used to sign a transaction before executing on the network to prove authenticity.

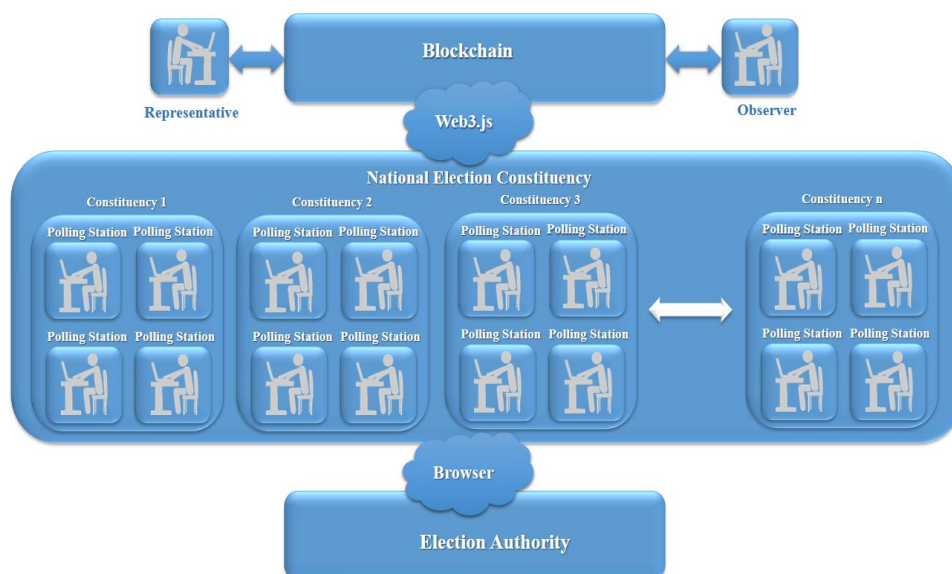
The second Ethereum account is, in fact, the smart contract, which may be considered an account controlled by its own code, or as an autonomous agent executed by the EVM, the core foundation and the main building blocks of any Decentralized Application (DApp). Once this code is deployed on the blockchain, the EVM will take care of running it as long as the conditions apply, and the contract may be publicly visited and viewed via its address with all associated transactions. Triggering functions in the smart contract can be performed from any account, as long as the address of the smart contract is known and the function caller has sufficient Ether to trigger it. A permissioned version of Ethereum exists, in addition to the public one, referred to as a private blockchain. In the public version blockchain, an EOA may send transactions to other addresses in the network using online explorers, such as Etherscan, while a central authority is needed to control and maintain its own ledger in the blockchain. In a country election process, for instance, a permissioned blockchain is usually preferred by governments in order to control the election process.

## System Architecture

Ethereum has found popularity as a platform in e-voting systems and many examples have been showcased in the past few years (Khoury *et al.*, 2018; Shukla *et al.*, 2018; Yavuz *et al.*,

2018; Rosasooria *et al.*, 2020; Park *et al.*, 2021). These focused on implementing Ethereum blockchain in e-voting systems governed by smart contracts to overcome problems associated with existing digital solution EVMs. Such platforms carry the promise of building trust among citizens on the transparency and openness of the election process, especially with the presence of a third party that monitors the validation, operations and procedures of voting, which is particularly important in emerging democracies.

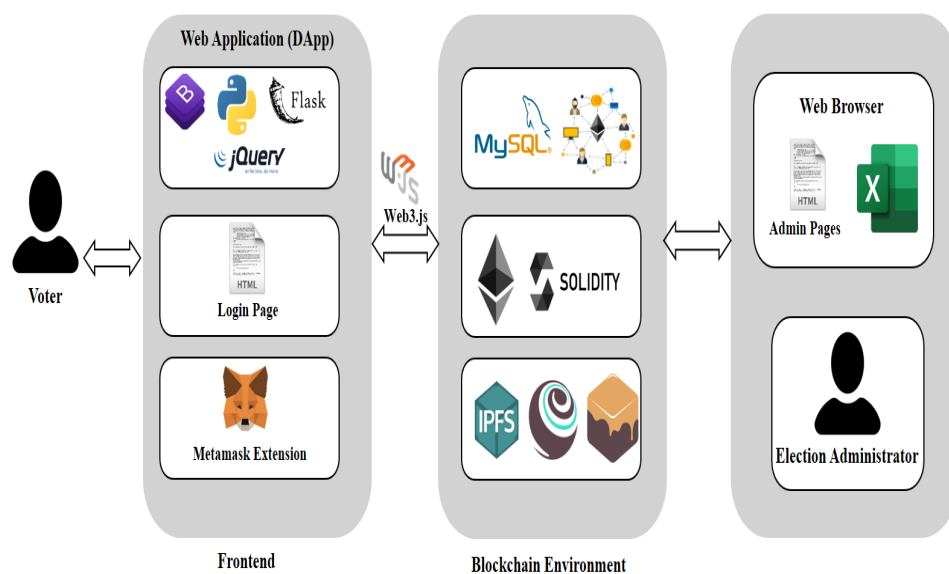
The proposed architecture of the blockchain system designed to run the voting process consists of four main blocks, namely the client side, front-end web application, blockchain environment and the administrator front-end. The Ethereum platform forms the backbone of the development blockchain environment that includes a Truffle suite (a development environment for smart contracts), as well as InterPlanetary File System (IPFS) and Remix, which are used to test the smart contracts functionality online and consequently host the decentralized web application. The layout of the proposed election landscape is shown in Figure 2, where a country, region, state or city is usually divided into districts or election constituencies, and each accommodates a number of polling stations. Every polling station is connected through the Internet to the blockchain using Web3.js libraries to allow for interaction with an Ethereum node using HTTP, IPC or Web Socket.



**Figure 2. Layout of the Proposed Election Landscape**

The voter at a certain polling station may access the voting system via an ordinary web browser by providing a unique national identification number. Once the vote is cast, the smart contract of the polling station automatically assigns the appropriate candidate a new count, and the process is repeated with each new voter in every polling station regardless of the constituency, as they all operate independently from each other using separate distinctive smart contract programming. Each smart contract of polling stations is assigned a transaction key address consisting of 42 characters, with a counter updated every 5 minutes. An observer, whether an

international or domestic electoral official assigned by the election authority or a specific representative of a candidate, may follow all transactions of one or more smart contracts directly on the Etherscan platform (<https://etherscan.io>), which provides real-time display of all transactions on the Ethereum blockchain. By simply selecting and filtering the smart contract address, the observer and representative monitor all transaction details, such as block number, transaction hash, method, age, value and fees. The platform also provides details on internal transactions within the smart contract, tokens and Ether transfers, analytics and comments. The same principle applies to any type of election, whether presidential, congressional, parliamentary, state assembly, municipality, or even limited scale student union elections at universities.



**Figure 3. Blockchain Voting System Architecture Overview**

In order to prepare the blockchain environment for the election process, as shown in Figure 3, Truffle is utilised to compile the smart contract, which is a set of protocols coded in Solidity to coordinate communication and to organize the flow of decisions amongst partners in the network (Ibrahim *et al.*, 2021). The Truffle framework actually allows migrating the smart contract to the local Ethereum blockchain utilizing default package manager for the JavaScript runtime environment Node.js (NPM). The smart contract necessary details and information, including its variables and functions, is migrated onto the blockchain in the form of an ABI file because of compilation. In fact, the ABI file helps connect the local Ethereum blockchain to the front end at the server side using web3.js. Simultaneously, Ganache, which is a local blockchain for rapid Ethereum distributed application development, is used across the entire development cycle to develop, deploy, and test decentralized applications (DApps) in a safe environment. Ganache actually initiates the local blockchain and provides the user with 10 accounts, each of which has a unique address that represents voters' access details in the actual election application. On the client side, the user and admin interfaces are hosted on the



election authority server using different programming languages, like HTML, Python, and JavaScript, while formatting is performed with a cascading style sheet (CSS). The user can access these pages using a web browser, supported by a MetaMask functionality, to connect to the Ethereum platform. Meanwhile, the admin interface is responsible for management of policies and rules, including uploading a candidate list Excel file to the smart contract to be stored in mapping arrays, in addition to assuming authority to view the results on the output pages. Furthermore, the client user interface utilises Ethereum accounts to invoke the smart contracts and then generates a dropdown menu form to select the candidate.

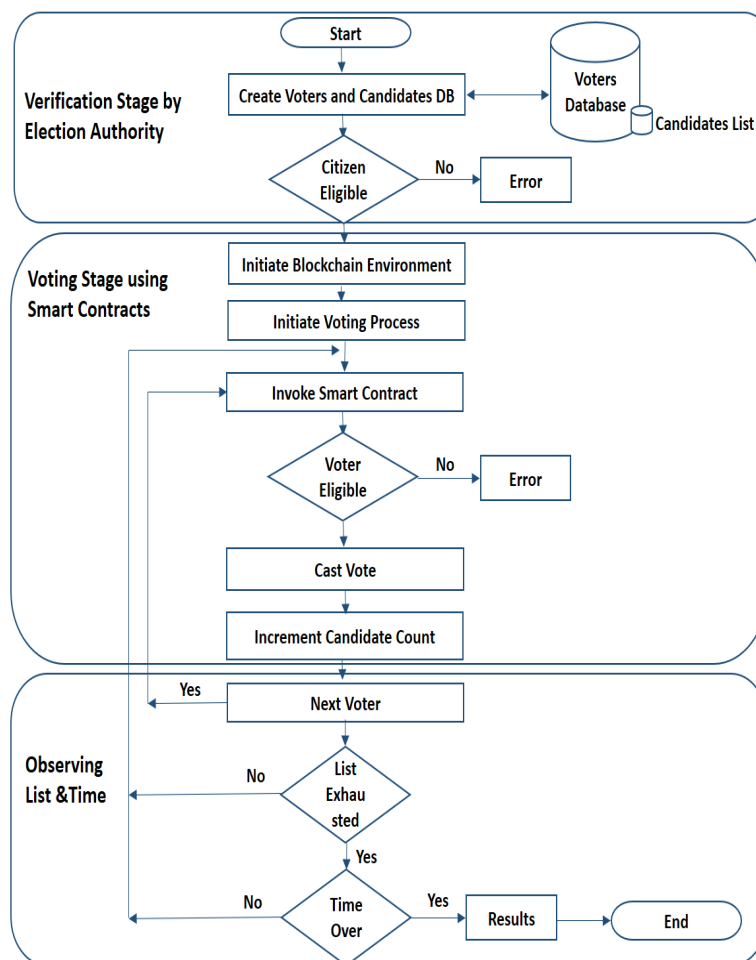
Election authorities usually initiate the voter registration stage. When an election starts, these appropriate authorities define a trusted list of individuals who are eligible to vote. This might require a database for an identity verification service to securely authenticate and authorize eligible voters by the Civil Authority Department. Using such a service is necessary for the requirement of secure identity verification and authentication: by default, when using a blockchain platform, for each eligible voter, a unique identity wallet is generated. The voter's registration process and identity verification are executed in advance prior to creating accounts. The ID card is used to verify the voter encrypted information. Consequently, the voter enters the application website with access details, including the national number that every citizen in the country is assigned. MetaMask will then ask the user to provide access information, including the private key generated by Ganache, and hence open the voting page in the form of the dropdown menu. Once the voting task is completed, MetaMask generates a sequence to move an Ether coin from the user to the smart contract address. Casting votes is performed by the smart contract that contains a function that verifies the authenticity of the voting, and then a vote count is incremented.

## Piloting the System

The flowchart in Figure 4 highlights the process of the voting application, which commences in initiating the blockchain environment to run locally on the desktop. The first step in the process is to read the data of the voting population from the server of the election authority by either uploading an Excel sheet containing all necessary details of each citizen, or reading it online directly by web service. In fact, election authorities should prepare the complete lists of voters months prior to election time. The voters' information includes details such as name, identification national number, sex, age, city and district. The list is uploaded to a secure MySQL database created by the admin at the election authority domain. An initial identity verification step is then launched based on the national identity number to check if the voter is included in the citizens list. A smaller candidate list is also created for each district

containing all competing individuals or parties according to the election registration mechanisms.

The blockchain environment is launched using the Truffle framework to interact with the local Ethereum network and deploy smart contracts onto the blockchain. Ganache, meanwhile, creates the 10 accounts in the trial version, in the form of a public hash key containing 42 hex characters, and a private hash key of 66 hex characters. The public key is assigned to the voter as an anonymous identity equivalent to the national identity number, while the private key is used to access the system the same way as a password does. The voter then receives an amount of the Ethereum currency in the form of a gas coin. The account then enables the voter to connect to the Ethereum platform, via MetaMask extension within the browser in the polling station, with the private key as the identifier. The voter is considered eligible if found in the citizens list; otherwise an error message is displayed.

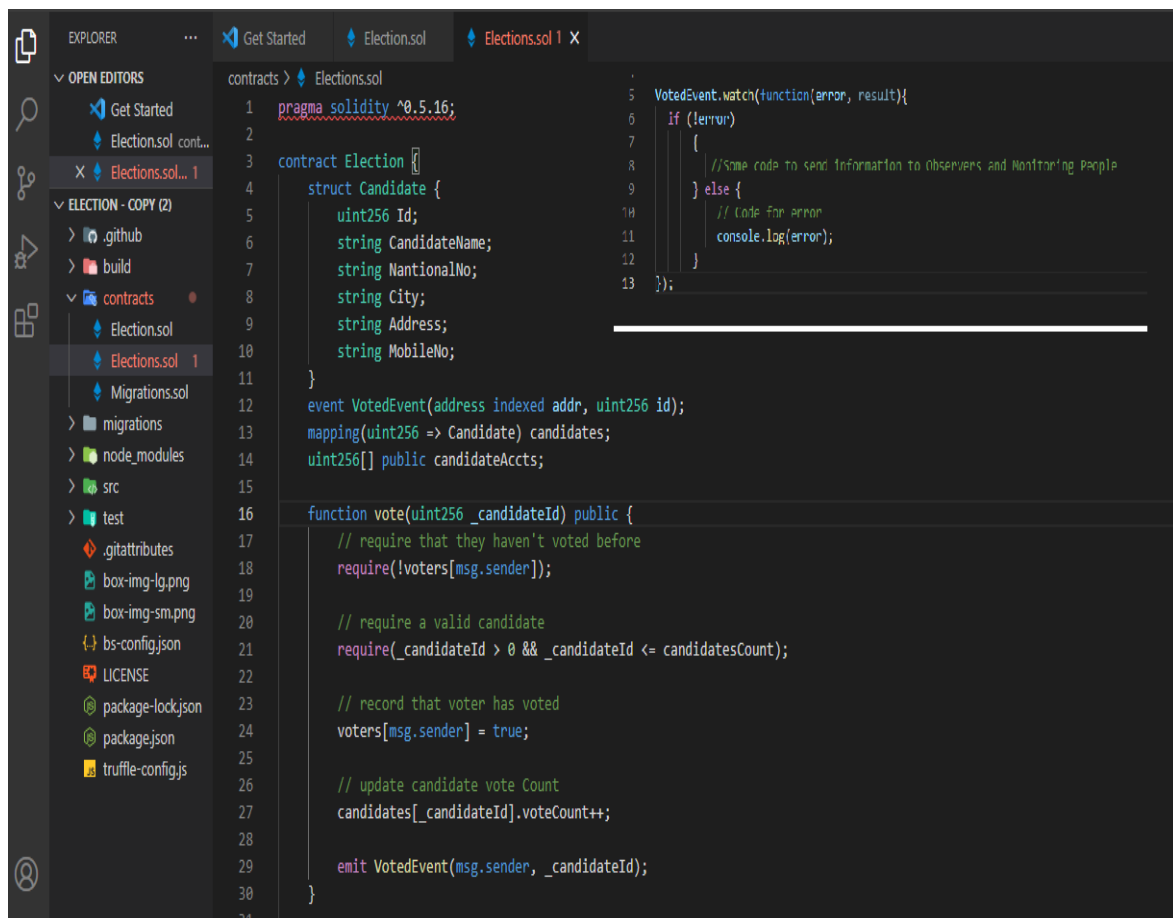


**Figure 4. Flowchart of e-Voting System**

The smart contract will also create a mapping array of the candidate list and stores it within its memory space, as shown in the example depicted in the screenshot of Figure 5. The details stored in the list pertain to the candidate data that consist of the names, IDs and vote counts. Once the voter accesses the blockchain election page in the user client side using the private



key, the smart contract will check the eligibility criteria, and whether the vote has been cast. The voter then casts the vote and the smart contract approves the transaction and increments the count for the corresponding candidate. The smart contract then waits for the next voter, repeats the process and checks if the list of voters is exhausted, and finally inspects if the time allocated for the election is over. Once over, the mapping array accumulates the results for each district, which may then be transferred to the IPFS location for proper recording and archiving using smart contract events that may be utilised to communicate back with the admin who invoked the contract in the first place.



```

1  pragma solidity ^0.5.16;
2
3  contract Election {
4      struct Candidate {
5          uint256 Id;
6          string CandidateName;
7          string NantionalNo;
8          string City;
9          string Address;
10         string MobileNo;
11     }
12     event VotedEvent(address indexed addr, uint256 id);
13     mapping(uint256 => Candidate) candidates;
14     uint256[] public candidateAccts;
15
16     function vote(uint256 _candidateId) public {
17         // require that they haven't voted before
18         require(!voters[msg.sender]);
19
20         // require a valid candidate
21         require(_candidateId > 0 && _candidateId <= candidatesCount);
22
23         // record that voter has voted
24         voters[msg.sender] = true;
25
26         // update candidate vote Count
27         candidates[_candidateId].voteCount++;
28
29         emit VotedEvent(msg.sender, _candidateId);
30     }
31
32     VotedEvent.watch(function(error, result){
33         if (!error)
34         {
35             //Some code to send information to Observers and Monitoring People
36         } else {
37             // Code for Error
38             console.log(error);
39         }
40     });

```

**Figure 5. Solidity Code of the Smart Contract**

In fact, events facilitate communication with the client through web3.js to obtain the value returned by the function to display in the user interface instead of the hash of the transaction, while the data passed is made available at the client side. In addition, every time an event is emitted, the data within the event is written into the blockchain logs, which are kept as a record of everything that happens within the contract, including the voter details and the candidates' vote count. The main features of events thus include the ability to log information and to trigger actions and return values to the invoking client. The example of the Solidity smart contract depicted shows the process when the Vote Function is invoked, in line 16. The event VotedEvent in line 12 is emitted, which returns the value of the voter account and candidate

ID defined in the struct candidate in line 4, back to the invoker and simultaneously logs both his/her address and value in the blockchain.

Transactions performed through Ethereum blockchain smart contract are grouped into blocks connected by a chain. A new block is not created until the previous block is completed and this is the vital step in the process as shown in Figure 6. The blocks are ordered chronologically, and each block contains a cryptographic hash of the previous block and applying the SHA-256 algorithm.

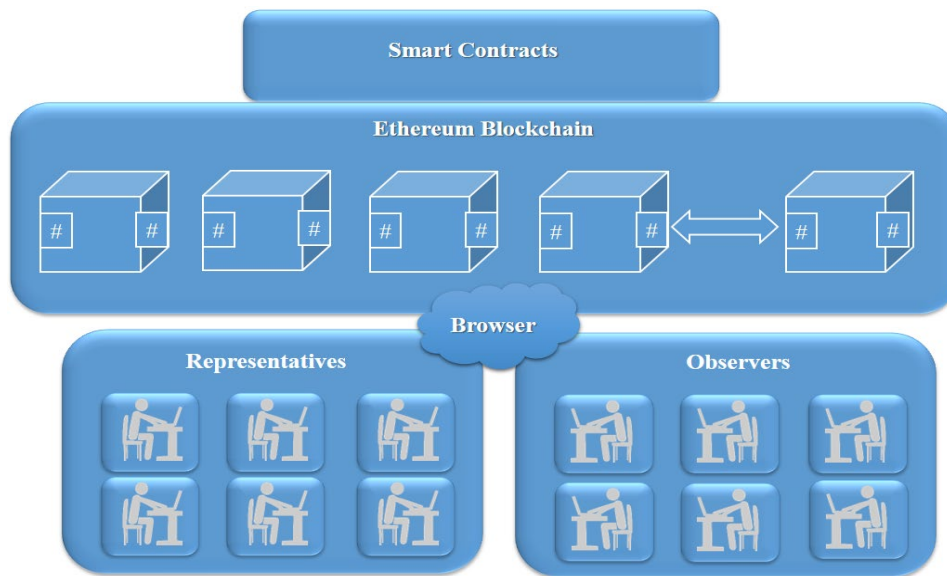


Figure 6. Observers' Role in the Blockchain Voting System

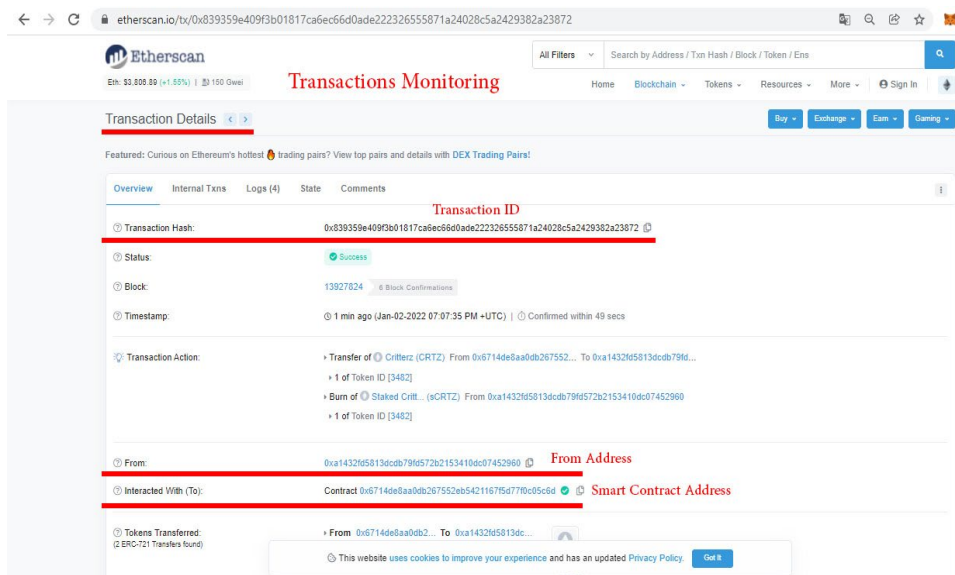


Figure 7. Etherscan View of Observers and Delegates

Observers assigned by the election authority and representatives of each candidate can subsequently monitor the election process by following the smart contract address in the Ethereum blockchain explorer at <https://etherscan.io/>, as shown in Figure 7. For each district, a vote is considered as a transaction by the smart contract. By following the transactions page,

which contains data such as transaction hash, method, block, age, value fee and sending end, the observers and representatives can keep a close eye on the process and take note of any irregularities that might occur. Observers and representatives may then report irregularities to the election authority to take appropriate action immediately by checking all transactions made at the concerned smart contract address.

Every user, however, can trace any transaction performed by voters given their address in the Etherscan. The privacy of the voting process may only be compromised if unauthorised personnel have access to the source code, or the ABI file is decompiled and the bytecode of the smart contract in the Etherscan is revealed. In this case, an additional cryptographic technique may be required if the secret ballot voting principle is compromised using the public Ethereum blockchain network.

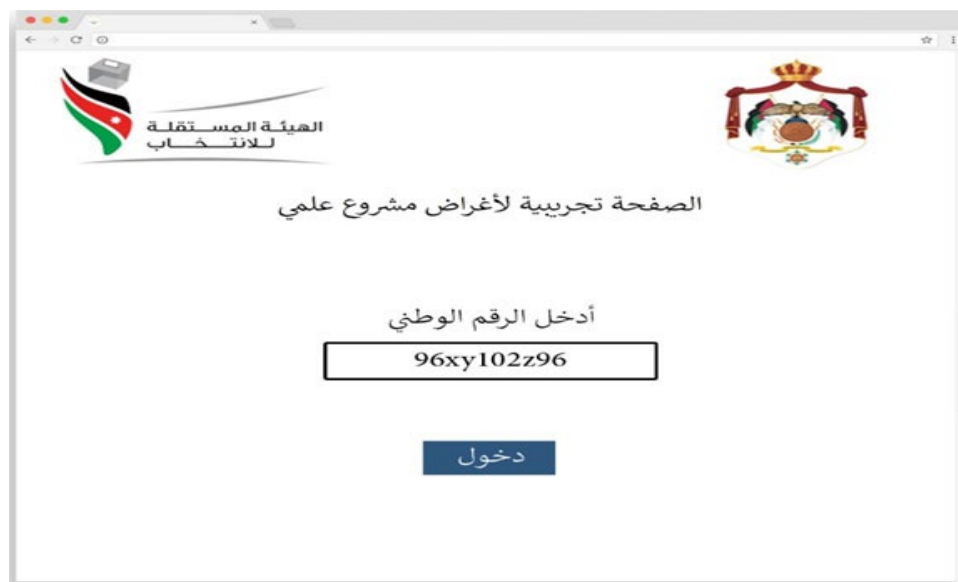
## Jordan Case Study

The political system in Jordan is parliamentary with a hereditary monarchy, as stated in the first article of the Constitution. The parliamentary system adopted is a bicameral national assembly of a Senate appointed by the King and a House of Representatives elected by citizens. Elections of various types and for different offices have been part of the political and public life in Jordan since 1929, when the first general election was conducted during the era of Transjordan. Local, municipality, decentralization, unions, and other forms of elections have continued ever since; however, parliamentary elections were halted after periods of turbulence and unrest in the region until 1989. An independent election commission (IEC) oversees all public elections and is the authority responsible for administering general and local polling processes. The IEC, in cooperation with the civil status department, prepares complete lists of voters in all districts and constituencies, months prior to election time. The commission may also seek the assistance of international observers to ensure accountable electoral management. This is a vital step to maintaining the credibility of elections and the transparency of electoral administration. The IEC thus follows specific executive instructions for the accreditation of international observers for the elections of parliament, as well as governorate and municipal councils, in order to provide an impartial and accurate assessment of the nature of election processes. International observers follow a detailed “code of conduct” to ensure that they respect the sovereignty of the host country, as well as the human rights and fundamental freedoms of its people, in addition to respecting the laws, authorities and bodies in charge of administering the electoral process.

Furthermore, the IEC reserves the power to approve the delegates or representative lists for individual candidates and political parties at the polling and counting centres for the general parliamentary and other elections. Delegates may enter the polling and counting centres and

monitor the process, with only one delegate assigned to each polling room, while the candidate has the right to monitor all polling stations and the results extraction centre, which is limited to the candidate without delegates. The IEC issues accreditation cards to delegates and publishes the names on the IEC website. In fact, the IEC administered a transparent voting process for the 2020 parliamentary elections and mobilized over 12,000 youths as volunteers, implemented COVID-19 health measures protecting voter safety, and provided accommodation to ensure equal access to polling stations for persons with disabilities in all municipalities, including 12 pilot highly accessible polling stations.

In 2016, the government introduced a smart ID card, containing information that includes 18 data fields, with the name in Arabic and English, gender, place of birth, area of residence, blood type, and a distinct citizen number consisting of 10 digits in use since 1992. The smart card embeds a chip that stores biometric data such as an iris scan and fingerprint, and designed to accommodate data on health insurance, tax, pension, and voting at later stages. The new ID card, in a credit card format, will reinforce the infrastructure required for digital signatures and make it possible to introduce new online services. The creation of the ID card has actually been a top priority of the country's e-government program as a reliable online infrastructure for access to present and future e-services. The e-government program has in fact been launched in 2002 to improve service delivery and increase the involvement of citizens with ICT, and consequently create a foundation for an e-voting system.



**Figure 8. Interface of the Voter Screen**

The proposed blockchain-based voting system is prototyped in one constituency for fictitious parliamentary elections in Jordan, which consists, according to the present election law, of 12 governorates, each allocated a certain number of seats, including gender, ethnic minority and special quotas. A number of seats are also allocated to a national list, totalling 130 parliamentary seats. The prototype is depicted for third district in the capital, selected as a

proof of concept. The demo page of the voter interface is shown in Figure 8, where the national ID is requested and entered. Access is then granted to the blockchain through the public key hash provided by the system. Figure 9 shows a snapshot of possible results for all candidates in that particular constituency.

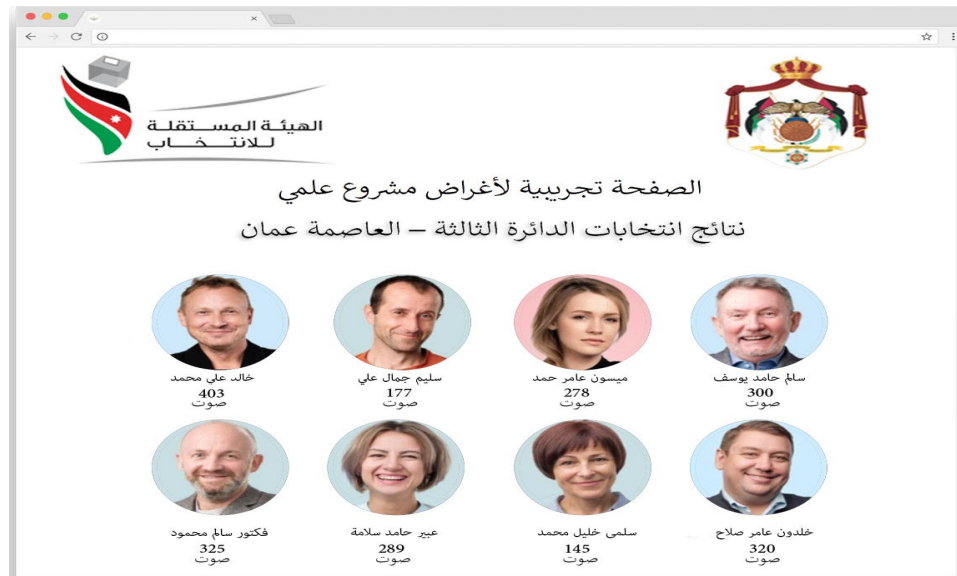


Figure 9. Interface of the Election Results

Almost all usual concerns regarding vote integrity and transparency have been raised, including the issue of assuring that votes have been counted as they were cast and not undetectably altered or discarded. However, a blockchain voting system running on a centralized network node with integrated biometric scanner has recently been developed in order to address the integrity of voters. This scheme allows data immutability while providing the user with security and control over their ballot. Recently, a blockchain based voting system (BBVS) has been proposed based on a private and centralized blockchain, using a Java development platform, implemented in a simulated environment, and then applied to parliamentary elections in Jordan. The BBVS applied a hierarchical election process, where a vote is cast at two levels, one for a group and the second for specific members within the group. A new algorithm has been introduced to maintain acceptable performance, both at the time of creating the blockchain for voters and candidates and at the time of vote casting (Malkawi, Yassein & Bataineh, 2021). Further research should address the challenges that blockchain brings in security, privacy, scalability and interoperability. Naturally, blockchain may not be appropriate for every application, and designers must evaluate its suitability before investing in its production.

## Conclusions

A pilot model for a proposed e-voting system based on blockchain technology, which runs on the Ethereum platform, utilises IPFS for data storage and manipulation, and deploys an

associated identity verification process, has been successfully implemented. The concept of smart contracts made programming the blockchain a smooth process that overcomes many of the limitations of conventional e-voting, such as a lack of transparency, security, trust or accuracy. The system may thus help in providing a reliable and secure voting process while reducing cost, saving time, and preserving the integrity of the election, whether it is local, regional or national, and regardless of its nature, being parliamentary, local authority, NGO or even private corporation. The system also promotes transparent democracy, which enables voters to easily cast their ballots from anywhere and consequently validate the final count.

The proposed model may be integrated further with identity authentication utilising artificial intelligence and machine learning algorithms for facial recognition, iris scanning or fingerprints. The advantage of the proposed system is its independence from traditional third-party involvement while maintaining integrity and transparency. Further improvements may be made to make the system versatile for elections at a large scale by integrating advanced identity authentication. The e-voting protocols may be improved further using different blockchain frameworks as well as real-time testing for large numbers of voters, in addition to increasing their confidence in the system.

## References

- Abuidris, Y., Hassan, A., Hadabi, A., & Elfadul, I. (2019). Risks and Opportunities of Blockchain Based on E-Voting Systems. 16<sup>th</sup> International Computer Conference on Wavelet Active Media Technology and Information Processing. <https://doi.org/10.1109/ICCWAMTIP47768.2019>.
- Anggorojati, D. P. (2020). Implementation and Evaluation of Blockchain Based e-Voting System with Ethereum and Metamask. International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS). <https://doi.org/10.1109/ICIMCIS51567.2020.9354310>
- Awsan, A. H., & Othman, E. A. (2021). Online Voting System Based on IoT and Ethereum Blockchain. International Conference of Technology, Science and Administration (ICTSA). <https://doi.org/10.1109/ICTSA52017.2021.9406528>
- Buterin, V. (2014). A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper 3(37), 2–1. Retrieved from [https://scholar.google.co.kr/citations?view\\_op=list\\_works&hl=en&hl=en&user=DL\\_PqgTAAAAAJ](https://scholar.google.co.kr/citations?view_op=list_works&hl=en&hl=en&user=DL_PqgTAAAAAJ)
- Cortes-Goicoechea, M., & Bautista-Gomez, L. (2021). Discovering the Ethereum2 P2P Network. 3<sup>rd</sup> Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 1–2. <https://doi.org/10.1109/BRAINS52497.2021.9569801>
- Crowcroft, B. S. (2019). Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access*, 7, 24477–24488. <https://doi.org/10.1109/ACCESS.2019.2895670>



- Giraldo, F. D., Barbosa Milton, C., Gamboa, C. E. (2020). Electronic Voting Using Blockchain and Smart Contracts: Proof of Concept. *IEEE Latin America Transactions*, 18(10), 1743–1751. <https://doi.org/10.1109/TLA.2020.9387645>
- Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K. (2018). E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *IEEE International Conference on Internet of Things, IEEE Green Computing, Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data*. <https://doi.org/10.1109/Cybermatics.2018.2018.00262>.
- Hoiss, T., Seidenfad, K., & Lechner, U. (2021). Blockchain Service Operations-A Structured Approach to Operate a Blockchain Solution. *IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) UK (Online)*. <https://doi.org/10.1109/DAPPS52256.2021>
- Ibrahim, M., Ravidran, K., Lee, H., Farooqui, O., & Mahmoud, Q. H. (2021). ElectionBlock: An Electronic Voting System using Blockchain and Fingerprint Authentication. *IEEE 18th International Conference on Software Architecture Companion (ICSA-C)*. <https://doi.org/10.1109/ICSA-C52384.2021.00033>
- Jafar, U., Aziz, M J. A., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors*, 21(17), 1–22. <https://doi.org/10.3390/s21175874>
- Jain, K. P. (2019). Decentralized E-Voting Portal Using Blockchain. *10<sup>th</sup> International Conference on Computing, Communication and Networking Technologies (ICCCNT)*. <https://doi.org/10.1109/ICCCNT45670.2019.8944820>
- Jeyasekar, S. K. (2020). A Competent and Accurate Blockchain based E-Voting System on Liquid Democracy. *Second Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS)*, 202–203. <https://doi.org/10.1109/BRAINS49436.2020.9223308>
- Jones, D. W. (2009). Early Requirements for Mechanical Voting Systems. *First International Workshop on Requirements Engineering for e-Voting Systems*. <https://doi.org/10.1109/RE-VOTE.2009.3>
- Khoury, D., Kfoury, E. F., Kassem, A., & Harb, H. (2018). Decentralized Voting Platform Based on Ethereum Blockchain. *2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*. <https://doi.org/10.1109/IMCET.2018.8603050>
- Kshetri, N., & Voas, J. (2018). Blockchain-Enabled E-Voting. *IEEE Software*, 35(4), 95–99. <https://doi.org/10.1109/MS.2018.2801546>
- Loeber, L. (2014). E voting in the Netherlands; past, current, future? *Journal Proceedings of the sixth international conference on electronic voting (EVOTE)*, 43–46.
- Madaan, L., Kumar, A., & Bhushan, B. (2020). Working Principle, Application Areas and Challenges for Blockchain Technology. *IEEE 9<sup>th</sup> International Conference on Communication Systems and Network Technologies (CSNT)*. <https://doi.org/10.1109/CSNT48778.2020.9115794>
- Malkawi, M., Yassein, M. B., & Bataineh, A. (2021). Blockchain Based Voting System for Jordan Parliament Elections. *International Journal of Electrical and Computer Engineering*, 11(5), 4325–4335. <http://doi.org/10.11591/ijece.v11i5.pp4325-4335>



- Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: from Internet voting to blockchain voting. *Journal of Cybersecurity*, 7(1). <https://doi.org/10.1093/cybsec/tyaa025>
- Puneet, Chaudhary, A., Chauhan, N., & Kumar, A. (2021). Decentralized Voting Platform based on Ethereum Blockchain. International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). <https://doi.org/10.1109/ICAECT49130.2021.9392580>
- Rosasooria, Y., Mahamad, A. K., Saon, S., Isa, M. A. M., Yamaguchi, S., & Ahmadon, M. A. (2020). E-Voting on Blockchain using Solidity Language. 3<sup>rd</sup> International Conference on Vocational Education and Electrical Engineering (ICVEE). <https://doi.org/10.1109/ICVEE50212.2020.9243267>
- Sheldon, R. (2021). A Timeline and History of Blockchain Technology. Retrieved from <https://whatis.techtarget.com/feature/A-timeline-and-history-of-blockchain-technology>
- Sherman, A. T., Javani, F., Zhang, H., & Golaszewski, E. (2019). On the Origins and Variations of Blockchain Technologies. *IEEE Security and Privacy*, 17(1), 72–77. <https://doi.org/10.1109/MSEC.2019.2893730>
- Shukla, S., Thasmiya, A. N., Shashank, D. O., & Mamatha, H. R. (2018). Online Voting Application Using Ethereum Blockchain. (2018). International Conference on Advances in Computing, Communications and Informatics (ICACCI). <https://doi.org/10.1109/ICACCI.2018.8554652>.
- Sliusar, V., Fyodorov, A., Volkov, A., Fyodorov, P., & Pascari, V. (2021). Blockchain Technology Application for Electronic Voting Systems. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2257–2261. <https://doi.org/10.1109/ElConRus51938.2021.9396400>
- Stein, R., & Wenda, G. (2014). The Council of Europe and E-voting: History and impact of Rec (2004)11. 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE). <https://doi.org/10.1109/EVOTE.2014.7001139>.
- Syed, T. A., Alzahrani, A., Jan, S., Siddiqui, M. S., Nadeem, A., & Alghamdi, T. (2019). A Comparative Analysis of Blockchain Architecture and its Applications: Problems and Recommendations. *IEEE Access*, 7, 176838–176869. <https://doi.org/10.1109/ACCESS.2019.2957660>
- Tsahkna, A.-G. (2013). E-voting: Lessons from Estonia. *European View*, 12(1), 59–66. <https://doi.org/10.1007/s12290-013-0261-7>
- Vivek, S. K., Yashank, R. S., Prashanth, Y., Yashas, N., Namratha, M. (2020). E-Voting Systems Using Blockchain: An Exploratory Literature Survey. Second International Conference on Inventive Research in Computing Applications (ICIRCA). <https://doi.org/10.1109/ICIRCA48905.2020.9183185>
- Yavuz, E., Koç, A. K., Çabuk, U. C., & Dalkılıç, G. (2018). Towards Secure E-Voting Using Ethereum Blockchain. 6<sup>th</sup> International Symposium on Digital Forensic and Security (ISDFS). <https://doi.org/10.1109/ISDFS.2018.8355340>

# Perceived Risk, Structural Assurance and Trust in Mobile Payments

---

Afef Sahli Sassi

University of Manouba

Hanene Hammami

University of Tunis El Manar

Hajer Ben Lallouna Hafsia

University of Manouba

---

**Abstract:** Mobile technologies have emerged as a new business phenomenon as a result of the increasing popularity of mobile devices and the proliferation of mobile technologies. A number of marketing research studies have focused on the identification of the background and consequences of mobile commerce, thus enabling m-commerce service providers to design appropriate marketing strategies. This paper's major contributions are the importance of trust in adopting mobile payments under the influence of perceived risk and structural assurance, as well as the identification of business-related factors that affect mobile trust. A quantitative study was carried out, with 175 valid auto-administered questionnaires collected and analysed using structural equations modelling. The analysis results indicate the positive effect of perceived risk and structural assurance in mobile trust on mobile payment adoption intention. It is important to raise managers' awareness of preserving the security of services in order to develop mobile trust. Also, to reduce the perceived risk associated with mobile financial transactions, managers need to provide basic insurance for customers in order to defend their transactions in the event of fraud or a particular problem.

**Keywords:** Trust; mobile payment; perceived risk; structural assurance; intention to adopt.

## Introduction

M-commerce is distinguished from traditional E-commerce by its user interface and associated risks, ubiquity, interactivity, location services and usage habits (Wang, Ou & Chen, 2019). To develop mobile commerce, merchants, financial intermediaries and

telecommunications operators have joined forces to propose a new mobile payment offer; this is the m-payment. In recent years, mobile payments have become widely accepted due to their dependable and efficient transaction services ([Huang, Wang & Wang, 2020](#)). However, there are a variety of factors that affect the adoption of mobile payments ([Liébana-Cabanillas et al., 2018](#)). The literature review indicates that trust remains “as a prerequisite for the success of e-commerce sites” ([Chouk, 2005](#)). Several studies did not integrate it until lately and they have emphasized the role of the characteristics of the merchant site in the development of trust. Other research has focused on the study of brand trust ([Chaudhuri & Holbrook, 2002](#); [Gurviez & Korchia, 2002](#)). Thus, there is still little work on trust in the mobile payment setting ([Srivastava, Chandra & Theng, 2010](#); [Xin, Techatassanasoontorn & Tan, 2013](#)); and those that have identified antecedents to trust in electronic payment (TEP) and trust in mobile payment (TMP) do not always share the same results. This research is interested in identifying the factors related to business characteristics that are most explanatory of mobile trust.

In the current context, the study of the conceptual and empirical framework of mobile trust in the development of mobile commerce is a captivating area of research. It is then crucial to understand how consumers develop their mobile trust and adopt the mobile payment service in a developing country like Tunisia. Thus, the objectives of this investigation are threefold:

- 1- Succeed in mobile payment under the mobile trust effect;
- 2- Identify business-related factors that affect mobile trust;
- 3- Examine the impact of trust on mobile payment adoption intention.

This paper explores the importance of trust in adopting mobile payment under the effect of perceived risk and structural assurance. Expected search results can supplement existing literature and provide new perspectives on payment-related factors. This research is structured as follows: first, a literature review on trust constructs, explanatory factors and mobile payment adoption intention, and the relationship between these constructs is conducted. Secondly, the article presents the research methodology used and the instrument chosen for data collection. Finally, the analysis of the results is presented followed by a discussion and managerial implications on the mobile payment service.

## Literature Review

### Trust in mobile payment

While the number of retail banks offering mobile banking services has increased significantly, consumer adoption remains very low. Trust is one of the key issues identified by researchers ([Sawadogo et al., 2022](#)). Understanding the impact of mobile services on purchase intentions has become critical ([Zhani, Mouri & Ahmed, 2022](#)). Consumer trust was considered to be one

of the most important predictors of mobile adoption, as it is a key determinant of success. ([Rana et al., 2019](#)). It has been defined as the willingness of one party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the client, regardless of the first party's ability to monitor or control that other party.

In fact, several authors have synthesised trust, in a traditional context ([Guibert, 1999](#); [Guibert et al., 2009](#); [Rousseau et al., 1998](#)) and even online ([Chouk, 2005](#)). They have shown the complication of this concept, where it is difficult to propose an exact definition because of the multiplicity of dimensions to be considered ([Wang & Emurian, 2005](#)). Indeed, trust is difficult to observe and measure directly ([Hwang & Kim, 2007](#)). The study of trust is undergoing a real evolution since it has several facets: cognitive, affective, emotional and behavioural ([Chouk, 2005](#); [McKnight, Choudhury & Kacmar, 1995](#)) and is used in different fields such as psychology, sociology and marketing.

Furthermore, Jarvenpaa, Tractinsky & Vitale ([1999](#)), Veijalainen ([2007](#)) and Pavlou ([2003](#)) emphasise the notion of vulnerability that impacts on online trust. This vulnerability increases the fragility of the client who can be exploited by the other party in the exchange. In line with this idea, several researchers ([Bart et al., 2005](#); [Bermeo Giraldo et al., 2021](#); [Hwang & Kim, 2007](#)) have shown the importance of trust in different transactions and its role in reducing uncertainty and perceived risks. It is in this context that we thought it appropriate to conclude this section with the emergence, through our readings, of a new concept, named 'mobile trust'.

## Perceived risk and trust

Eastin ([2002](#)) has shown empirically that perceived risk negatively influences the adoption of online banking. This same result has been confirmed in other research, where it has been shown that the more risk the consumer perceives, the less likely they are to adopt the service ([Bauer, Falk & Hammerschmidt, 2006](#); [Yousafzai, Pallister & Foxall, 2009](#)). Malaquias & Hwang ([2016](#)) concluded that there is a direct negative effect between perceived risk and trust in mobile banking as it lowers their average level.

On the other hand, ([Tournois & Cheikho, 2015](#)) studied in depth all possible interactions between perceived risks in m-banking on customers' trust in their bank in the mobile context. They attest to the positive influence of perceived risk on trust in the mobile context.

In 2009, Lee revisited the six risk dimensions, replacing "physical risk" with "security risk" because it is inadequate for the virtual world. It is in this context that we pose the following hypothesis:

**Hypothesis 1:** Perceived risk has a positive influence on trust in mobile payments.

H1.1. Perceived risk has a positive influence on benevolence.

H1.2. Perceived risk has a positive influence on integrity.

H1.3. Perceived risk has a positive influence on competence.

## Structural assurance and trust

Structural assurances can be considered among the legal dispositions (laws, guarantees, and regulations) provided by the institutional environment to protect the security of transactions.

In the context of mobile commerce, Xin, Techatassanasoontorn & Tan (2013) expose the positive effect of structural assurances on consumer trust. M-payment services give rise to problems of vulnerabilities and data leakage. Therefore, in order to build trust in mobile payment and to close the reliability and security gaps of this payment method, users can rely on structural assurances (Srivastava, Chandra & Theng, 2010).

In this same context, Srivastava, Chandra & Theng (2010) and Zhou (2011) have shown that structural assurance as an institution-based trust mechanism can effectively enhance user trust and decrease perceived risk in online transactions. In this sense, we confirm the positive effect of structural assurance on trust in mobile payments. Hence the following hypotheses are given:

**Hypothesis 2:** Structural assurance has a positive influence on trust in mobile payment.

H2.1. Structural assurance has a positive influence on benevolence.

H2.2. Structural assurance has a positive influence on integrity.

H2.3. Structural assurance has a positive influence on competence.

## Trust and mobile payment adoption

Lack of trust is seen as a barrier to consumer adoption of the technology (Dounia & Fatine, 2020). Since mobile payment is a relatively new innovation, consumers may have uncertainties about their technology and operating environment (Srivastava, Chandra & Theng, 2010).

Extending this logic to the mobile payment context, several researchers (Xin, Techatassanasoontorn & Tan, 2013) show that trust in mobile payment has a positive effect on consumers' intentions to adopt mobile payment.

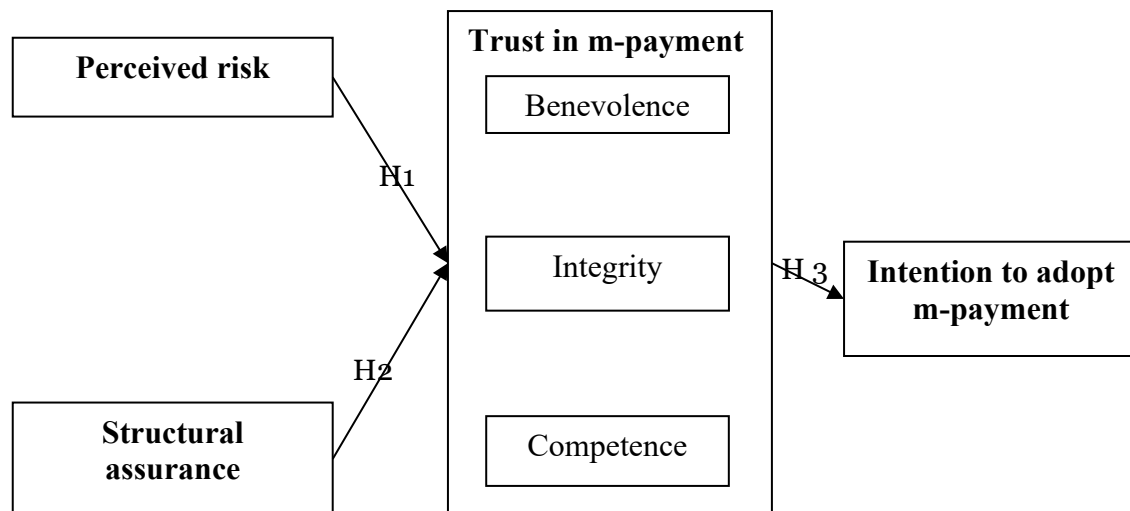
It is in this context that we pose the following hypothesis:

**Hypothesis3:** Trust in mobile payment has a positive influence on intention to adopt mobile payment.

H3.1. Benevolence has a positive influence on intention to adopt mobile payment.

H3.2. Integrity has a positive influence on intention to adopt mobile payment.

H3.3. Competence has a positive influence on intention to adopt mobile payment.



**Figure 1. Research model**

## Material and Methods

### Measuring instruments

To empirically measure the effect factors and test the model presented above, we chose the questionnaire survey as a data collection instrument. The constructs are measured by scales from the literature (Table 1). These scales have been adapted to the context of the present research “mobile payment”. In this research, the dependent variable “trust in m-payment” is measured according to a three-dimensional scale (benevolence, integrity and competence) inspired by Hwang & Kim (2007) and also the variable “perceived risk” is measured according to a three-dimensional scale (performance risk, security risk and financial risk) inspired by Lee (2005).

**Table1. Measurement scales**

Variable	Scale items		Authors
Perceived risk	Perceived performance risk	The performance of the Ooredoo mobile payment system server may be affected by slow download speeds, blocking or maintenance. Ooredoo’s mobile payment system server may malfunction and perform incorrect operations.	Adapted from Lee (2005)
	Perceived safety risk	I would not feel completely safe providing personal information via the Ooredoo mobile application (MobiCash). By using mobile payment via the Ooredoo mobile application (MobiCash), I am afraid that other people will have access to my account. I don’t feel safe sending important information via Ooredoo’s mobile applications (MobiCash, Mobiflouss).	

Variable	Scale items		Authors
	Financial risk	When transferring money via the Ooredoo mobile application (MobiCash), I am afraid of losing money because of careless mistakes (mistakes in the account number or in the amount). When there are transactional errors, I fear that I will not be reimbursed by Ooredoo.	
Structural assurance	Ooredoo offers enough guarantees to make me feel comfortable using MobiCash. I am confident that Ooredoo's legal structures effectively protect me from the problems of mobile technology. I am convinced that the safeguards in the mobile technology sector are secure for using MobiCash. In general, mobile technology provides a robust and secure environment for using MobiCash.		( <a href="#">Srivastava, Chandra &amp; Theng, 2010</a> )
Trust in mobile payment	Benevolence	I expect Ooredoo's m-payment system to have good intentions towards me. I expect Ooredoo's m-payment intentions to be benevolent. I expect Ooredoo's m-payment system to work in my interest.	(Hwang & Kim, 2007)
	Integrity	The promises made by Ooredoo's m-payment system seem reliable. I don't doubt the honesty of Ooredoo's m-payment. I expect Ooredoo's m-payment to deliver on its promises.	
	Competence	Ooredoo's m-payment system understands the market in which it operates. Ooredoo's m-payment system knows all about financial products. Ooredoo's m-payment system knows how to provide an excellent service.	
Intention to adopt mobile payment	I intend to use MobiCash in the future. I will be using MobiCash frequently in the coming months. I would strongly recommend others to use MobiCash.		( <a href="#">Xin, Techatassa nasoontorn &amp; Tan, 2013</a> )

## Choice of study area

To carry out our survey, we used a popular application known by Tunisians, the “MobiCash” service of the Tunisian telephone operator “Ooredoo”: “this is a new-easy to use payment method which is thoroughly secure. It grants you both, mobile money and mobile payment transfer”.

## Sampling and data collection

The validation of the conceptual framework was carried out using a quantitative data collection method, based on a survey of Ooredoo mobile payment users. The data was collected using an online questionnaire. A total of 200 questionnaires were completed, of which 25 were removed from the database due to incomplete or contradictory answers. A total of 175



questionnaires constituted the final sample. We have used the Likert 5-point semantic scale, ranging from “strongly agree” to “strongly disagree”. According to Touzani & Driss (2007), this scale is the most adapted to the Tunisian context.

However, in order to respect the notion of representativeness of the sample, we took into consideration socio-demographic criteria such as age, gender, educational level and income.

Our sample consists of 61.5% of men and 38.5% of women, the majority (39%) belong to the age category (20-35 years) and almost 95% have a university education and have been subscribing to Ooredoo.

## Results

A two-stage analysis was conducted. Exploratory factor analysis follows confirmatory factor analysis.

In order to conduct the exploratory factor analysis, the results obtained show that Cronbach's alpha is acceptable ( $>0.7$ ), KMO (Kaiser–Meyer–Olkin test) is acceptable ( $>0.5$ ), Bartlett's test is significant ( $>0.000$ ) and the explained variance is good (Abraouz Chakir 2020 ; Tritah & Daoud, 2021). All these results are presented in Table 2.

**Table2. Result of the principal component analysis**

Constructs/Dimensions	KMO	Bartlett Test Significance	Explained Variance %.	Cronbach's $\alpha$
Perceived risk	0.563	828.924; $p=0.000$		
R. of performance dimension			31.728	0.766
R. of safety dimension			23.193	0.750
R. financial dimension			23.178	0.899
Structural assurance	0.818	622.160; $p=0.000$	70.505	0.860
Confidence in payment	0.760	1987.878; $p=0.000$		
Benevolence dimension			39.105	0.911
Integrity dimension			25.631	0.917
Competence dimension			18.029	0.838
Intent to adopt mobile payment	0.636	340.104; $p=0.000$	70.370	0.776

For the confirmatory factor analysis, we used the structural equation method (SEM) using the Smart PLS.3 (Partial Least Squares) to test the hypotheses and estimate our structural model. The results obtained show that the construct reliability is good; hence the Cronbach alpha and composite reliability are acceptable, which is above the acceptable value of 0.70, indicating that the internal consistency is confirmed. Convergent reliability is tested by the average variance extracted (AVE) and the recommended threshold is 0.5 (Table 3). Discriminant validity is assessed by three methods (Gold, Malhotra & Segars, 2001; Henseler, Ringle & Sarstedt, 2015). First, the Fornell-Larcker test when  $\sqrt{AVE} > R$  (Fornell & David, 1981);

second, the Cross-loading technique ([Chin, 1998](#)) when Cross-loadings < Loadings; and, third, examination of the correlation ratio HTMT, also called the Heterotrait-Monotrait matrix when  $HTMT < 0.90$ . Hence, the discriminant validity is confirmed. We have noted that, thanks to the reliability and validity of the measurement scales selected, the quality of our measurement model is satisfactory.

**Table3. Result of the factor analysis**

Built	Reliability of construction		Convergent validity
Constructs/Dimensions	Cronbach Alpha > 0.7	Composite reliability > 0.7	Average variance extracted > 0.5
Perceived risk			
R. performance dimension	0.766	0.878	0.785
R. of safety dimension	0.752	0.856	0.655
R. financial dimension	0.899	0.952	0.909
Structural assurance	0.860	0.905	0.704
Trust in mobile payment			
Benevolence dimension	0.912	0.944	0.850
Integrity dimension	0.918	0.948	0.859
Competence dimension	0.848	0.877	0.763
Intent to adopt mobile payment	0.787	0.876	0.703

## Structural model assessment

The structural model, also known as the “internal model”, presents all the hypothetical relationships between the latent variables ([Hair et al., 2014](#)). Thus, the evaluation of the structural model makes it possible to empirically test the set of hypotheses put forward and to evaluate the predictive power of the model on the basis of indicators and statistical estimates.

First, the assessment of the predictive validity is based on the coefficient of determination  $R^2$  (R Squared) and the Stone-Geisser  $Q^2$  coefficient ([Fernandes, 2012](#)). The value of these two coefficients lies between 0 and 1 ([Wetzels, Odekerken-Schröder & Van Oppen, 2009](#)). Both indices are significant.

Secondly, the evaluation of the goodness of fit of the structural model is based on the goodness of fit (GOF > 0.36) according to Wetzels, Odekerken-Schröder & Van Oppen (2009), and the Standardized Root Mean Square Residual (SRMR < 0.08). An SRMR value of less than 0.08 generally indicates good model fit according to Hu & Bentler (1999). Our results demonstrate the acceptability of the SRMR index. It is 0.006 for the saturated model and 0.006 for the radiating model. The acceptability of the GOF index is shown by its value of 3.860; which confirms the good quality of adjustment of the model.

## Analysis result of structural model

The quality of the global model being good, the convergent and discriminant validity being verified, an estimation of the structure model that reproduces the relationships between the latent constructs is necessary in order to test the research hypotheses through a bootstrapping procedure and significance (at the 5% significance level). The estimation of the different relationships represented in the model is carried out by examining the standardized path coefficients ( $\beta$ ) or correlation coefficients and the student t-values after bootstrapping. Indeed, bootstrapping allows the stability of the PLS estimate to be verified (Chin, 1998), and this procedure is recommended as a solution for a small sample size.

A company factor constitutes a guarantee for consumers and therefore reinforces consumer confidence. The results obtained show that trust in mobile payment is affected by perceived risk (H1) and structural assurance (H2). Furthermore, mobile trust positively influences mobile payment adoption intention (H3). The test results are summarised in Table 4.

**Table4. Test of business-related factors on mobile trust**

Assump tions	Relations	B (Path Coefficient)	T Student	p-Value	Conclusion
H1	Perceived risk -> Mobile trust				
H1.1	RP -> Benevolence	0.019	2.317	0.047	Confirmed
H1.2	PR -> Integrity	0.017	0.226	0.819	Rejected
H1.3	PR -> Competence	-0.069	0.952	0.299	Rejected
H1.4	RS -> Benevolence	0.092	1.650	0.098	Confirmed
H1.5	RS -> Integrity	-0.084	1.004	0.288	Rejected
H1.6	RS -> Competence	0.000	0.001	0.999	Rejected
H1.7	RF -> Benevolence	0.112	2.139	0.025	Confirmed
H1.8	RF -> Integrity	0.082	1.343	0.201	Rejected
H1.9	RF -> Competence	-0.060	1.073	0.288	Rejected
H2	Structural assurance -> Mobile trust				Confirmed
H2.1	Assurance -> Benevolence	0.244	4.620	0.000	partially Confirmed
H2.2	Assurance -> Integrity	0.134	1.996	0.046	Confirmed
H2.3	Assurance -> Competence	-0.022	0.425	0.671	Rejected
H3	Trust -> Intent to adopt				
H3.1	Benevolence -> Intention	0.039	0.954	0.341	Rejected
H3.2	Integrity -> Intent to adopt	-0.026	0.640	0.522	Rejected
H3.3	Competence -> Intention	0.705	27.834	0.000	Confirmed

## Discussion

The result of this study showed that hypothesis H1 was confirmed. As a result, the postulated link between perceived risk (performance risk, security risk and financial risk) and trust in mobile payment (benevolence, integrity, competence) is partially validated. This finding is in line with the work of Aldás-Manzano *et al.* (2009). Thus, the higher the performance risk, the higher the benevolence. This high level can be explained by the context of m-payment, which is focused on virtual transactions through a wireless network. This is why this service is perceived as vulnerable and may face problems related to mobile networks and technology. “This mode of transaction may not work as advertised, and therefore it does not provide the desired benefits” (Chaix & Torre, 2015).

Moreover, the greater the security risk, the greater the benevolence. Also, the participants interviewed are concerned about the security and risks of virtual transactions. For example, in order to carry out transactions via the mobile phone, they have to give personal and confidential information such as their credit card number and the payment code. This type involves the risks of fraud, financial loss and hacking when using m-payment. For the interviewees, this risk increases, as they do not have a written proof of the transactions made and they are afraid that their data will be hacked and their bank accounts will be stolen.

Hypothesis H2 was confirmed. The results showed that the relationship between structural assurance and mobile trust is partially confirmed. This relationship is consistent with previous work (Srivastava, Chandra & Theng, 2010; Xin, Techatassanasoontorn & Tan, 2013). Some work shows that structural assurance can be an antecedent of trust as it covers users against risks, hacks and interceptions of information (McKnight & Norman, 2002). Structural assurance means that there are adequate technological and legal structures to ensure the security of payments. Compared to online payments, mobile payments embedded in wireless networks may be more vulnerable to hackers’ attacks and information interception. In addition, viruses may exist in mobile terminals. These problems will affect the security of the account and the money. Thus, if there are sufficient structural assurances such as certification and regulation to ensure the security of payments, users can build their trust in mobile payments. It should be noted that structural assurance has the greatest positive and significant impact on mobile trust. The more protective regulations and safeguards the company has, the more confident the consumer is to adopt the mobile payment service (Chaix & Torre, 2015).

The link between mobile confidence and adoption intention is significant, which is consistent with the literature (Srivastava, Chandra & Theng, 2010; Xin, Techatassanasoontorn & Tan, 2013). Lack of consumer trust is observed as a barrier to the adoption of the new technology. Since m-payment is a new mode of transaction, it can create a degree of uncertainty for users

regarding their technology and operational environment ([Srivastava, Chandra & Theng, 2010](#)). As such, the presence of trust is paramount in the decision to adopt mobile payment. Previous studies on e-commerce and m-commerce consistently demonstrate that trust has a positive relationship with technology adoption intention ([Gefen, Karahanna & Straub 2003](#); [Srivastava, Chandra & Theng, 2010](#)). Extending this logic to the mobile payment context, Xin, Techatassanasoontorn & Tan ([2013](#)) found that consumers' level of trust in mobile payment has a positive effect on their intention to adopt the service.

A new theoretical concept "mobile trust" has been developed in this research. "It reflects mobile users' trust in transactions conducted on their mobile phone." This definition can be used to provide a theoretical foundation for future research.

Following that, our findings added to the work of Chandra *et al.* ([2010](#)) and Xin, Techatassanasoontorn & Tan ([2013](#)), who established perceived reputation, perceived opportunism, and perceived risk as predictors of trust in mobile payment. We improved both perceived safety and structural assurance.

Furthermore, the choice of the Tunisian context, where mobile payment adoption is low or non-existent, is novel. As a result, it is crucial to encourage Tunisians to register for and use regular mobile payment services. When compared to previously used products and services, the adoption of mobile payment represents a significant shift in customer behaviour.

## Conclusions/Recommendations

The aim of the present research was to examine how three firm-related factors, knowledge, perceived risk, and structural assurance, affected user trust in the context of mobile payments. According to the findings, trust positively influences mobile payment adoption intention. Furthermore, perceived risk and structural assurance influence mobile trust significantly.

The research revealed the company-related factors, such as perceived risk and structural insurance. As a result, in order to correct the limitations of the mobile payment system, such as illegal downloading, content loss, a lack of safety, hackers, an absence of authentication, a total absence of a monitoring system, and so forth, the primary role of professionals is to code any mobile payment transaction to be 100% safe and protected.

In light of the importance of structural assurance as a key factor in mobile trust, the government and the Central Bank must strengthen the institutional environment by enacting regulations and laws that protect user confidentiality and identification, as well as protection against uncertainty, fraud, and the risk of using new technology.

Greater efforts are required to ensure:

- Sensitizing mobile service providers to the importance of service security in order to foster mobile trust.
- Holding communication campaigns, mobile payment demonstrations, mode of employment distribution, and benefit distribution to reduce perceived risk associated with mobile financial transactions.
- Providing clients with assurances to protect their transactions in the event of fraud or a specific problem, as well as to reduce their hesitation when making mobile payments.
- Establishing a legal framework that, on the one hand, protects mobile transactions and consumer interests while, on the other hand, boosts competition by incorporating, for example, new players in order to expand electronic commerce.
- Incorporating customer experience into the design of mobile phones in order to make them more accessible and performant to different types of customers (Generation X, Generation Y, etc.).
- Encouraging telecom operators to invest in mobile technologies in order to make transactions faster (mobile application download, mobile payment, etc.) and to ensure network availability.

However, the evolution of m-commerce remains a problem for some countries, particularly Tunisia, because m-payment is limited to domestic transactions.

One limitation of this study is that it did not include demographic variables, such as age, gender, income, and socio-professional category, which can influence trust in mobile payments, nor individual and mobile app factors that can affect mobile trust. Notwithstanding these limitations, the study suggests that future research can provide a better understanding of these variables' roles in the context of mobile payment. This would be a fruitful area for further work.

The findings of this study have a number of important implications for future practice. It is therefore necessary to raise the awareness of mobile payment stakeholders to preserve the security of services in order to develop mobile trust. In this sense, it is imperative to launch communication campaigns, mobile payment demonstrations, distribution of instructions for use and benefits, etc. to reduce the perceived risk associated with financial transactions on mobile phones. As a result, managers need to put in place assurance for customers to defend their transactions in case of fraud or other problems.

## References

Abraouz, F. Z., & Chakir, K. (2020). Adéquation entre entrepreneuriat coopératif et développement durable, Étude des aspects coopératifs dans la région Souss-Massa.



*Revue Internationale des Sciences de Gestion*, 3, 2. <https://revue-isg.com/index.php/home/article/view/252>

- Aldás-Manzano, J., Lassala-Navarré, C., Ruiz-Mafé, C., & Sanz-Blas, S. (2009). Key drivers of internet banking services use. *Online Information Review*. <https://doi.org/10.1108/14684520910985675>
- Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing*, 69(4), 133–152. <https://doi.org/10.1509/jmkg.2005.69.4.133>
- Bauer, H. H., Falk, T., & Hammerschmidt, M. (2006). eTransQual: A transaction process-based approach for capturing service quality in online shopping. *Journal of business research*, 59(7), 866–875. <https://doi.org/10.1016/j.jbusres.2006.01.021>
- Bermeo Giraldo, M. C., Benjumea-Arias, M. L., Valencia-Arias, A., & Montoya-Restrepo, I. A. (2021). Factors determining the use and acceptance of mobile banking in Colombia. *Journal of Telecommunications the Digital Economy*, 9(4), 44–47. <https://doi.org/10.18080/jtde.v9n4.391>
- Chaix, L., & Torre, D. (2015). Le double rôle du paiement mobile dans les pays en développement. *Revue économique*, 703–727. <https://doi.org/10.3917/reco.664.0703>
- Chaudhuri, A., & Holbrook, M. B. (2002). Product-class effects on brand commitment and brand outcomes: The role of brand trust and brand affect. *Journal of Brand Management*, 10(1), 33–58. <https://doi.org/10.1057/palgrave.bm.2540100>
- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, 295(2), 295–336. [https://doi.org/10.1007/978-3-031-06374-9\\_2](https://doi.org/10.1007/978-3-031-06374-9_2)
- Chouk, I. (2005). *Déterminants de la confiance du consommateur vis-à-vis d'un marchand internet non familier: une approche par le role des tiers* (Doctoral dissertation, Paris 9). Paris 9. Retrieved from <https://www.theses.fr/2005PA090047>
- Chandra, S., Srivastava, S. C., & Theng, Y. L. (2010). Evaluating the role of trust in consumer adoption of mobile payment systems: An empirical analysis. *Communications of the Association for Information Systems*, 27, 1529–3181. <https://doi.org/10.17705/1CAIS.02729>
- Dounia, D., & Fatine, B. (2020). Proposition d'un modèle explicatif de l'adoption du service «Sans contact». *Information Systems Management Innovation*, 4(2), 4–16. <https://doi.org/10.34874/IMIST.PRSM/ISMI/28599>
- Eastin, M. S. (2002). Diffusion of e-commerce: an analysis of the adoption of four e-commerce activities. *Telematics informatics*, 19(3), 251–267. <https://doi.org/10.17705/1CAIS.02729>
- Fernandes, V. (2012). En quoi l'approche PLS est-elle une méthode a (re)-découvrir pour les chercheurs en management? *M@n@gement*, 15(1), 102–123. <https://hal.archives-ouvertes.fr/hal-00827984>
- Fornell, C. L., & David F (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 18(1), 39–50. <https://doi.org/10.1177/002224378101800104>



- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Inexperience and experience with online stores: The importance of TAM and trust. *IEEE Transactions on engineering management*, 50(3), 307–321. <https://doi.org/10.1109/TEM.2003.817277>
- Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. *Journal of management information systems*, 18(1), 185–214. <https://doi.org/10.1080/07421222.2001.11045669>
- Guibert, N. (1999). La confiance en marketing: fondements et applications. *Recherche et Applications en Marketing*, 14(1), 1–19.
- Guibert, N., Paris, H., Rech, J., & Claudin, C. (2009). Identification of thrust force models for vibratory drilling. *International Journal of Machine Tools Manufacture*, 49(9), 730–738. <https://doi.org/10.1177/076737019901400101>
- Gurviez, P., & Korchia, M. (2002). Proposition d'une échelle de mesure multidimensionnelle de la confiance dans la marque. *Recherche et Applications en Marketing*, 17(3), 41–61. <https://doi.org/10.1177/076737010201700304>
- Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European business review*. <https://doi.org/10.1108/EBR-10-2013-0128>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal*, 6(1), 1–55. <https://doi.org/10.1080/10705519909540118>
- Huang, Y., Wang, X., & Wang, X. (2020). Mobile payment in China: Practice and its effects. *Asian Economic Papers*, 19(3), 1–18. [https://doi.org/10.1162/asep\\_a\\_00779](https://doi.org/10.1162/asep_a_00779)
- Hwang, Y., & Kim, D. J. (2007). Customer self-service systems: The effects of perceived Web quality with service contents on enjoyment, anxiety, and e-trust. 43(3), 746–760. <https://doi.org/10.1016/j.dss.2006.12.008>
- Jarvenpaa, S. L., Tractinsky, N., & Vitale, M. (1999). Consumer trust in an Internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, 5(2), JCMC526. <https://doi.org/10.1111/j.1083-6101.1999.tb00337.x>
- Lee, T. (2005). The impact of perceptions of interactivity on customer trust and transaction intentions in mobile commerce. *Journal of Electronic Commerce Research*, 6(3), 165. [http://ojs.jecr.org/jecr/sites/default/files/06\\_3\\_po1.pdf](http://ojs.jecr.org/jecr/sites/default/files/06_3_po1.pdf)
- Liébana-Cabanillas, F., Marinkovic, V., de Luna, I. R., & Kalinic, Z. (2018). Predicting the determinants of mobile payment acceptance: A hybrid SEM-neural network approach. *Technological Forecasting Social Change*, 129, 117–130. <https://doi.org/10.1016/j.techfore.2017.12.015>
- Malaquias, R. F., & Hwang, Y. (2016). An empirical study on trust in mobile banking: A developing country perspective. *Computers in human behavior*, 54, 453–461. <https://doi.org/10.1177/0266666915616164>

- McKnight, D. H., Choudhury, V., & Kacmar, C. (1995). Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of management journal*, 38(1), 24–59. <https://doi.org/10.5465/256727>
- McKnight, D. H. C., & Norman L. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The journal of strategic information systems*, 11(3–4), 297–323. [https://doi.org/10.1016/S0963-8687\(02\)00020-3](https://doi.org/10.1016/S0963-8687(02)00020-3)
- Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International journal of electronic commerce*, 7(3), 101–134. <https://doi.org/10.1080/10864415.2003.11044275>
- Rana, N. P., Barnard, D. J., Baabdullah, A. M., Rees, D., & Roderick, S. (2019). Exploring barriers of m-commerce adoption in SMEs in the UK: Developing a framework using ISM. *International Journal of Information Management*, 44, 141–153. <https://doi.org/10.1016/j.ijinfomgt.2018.10.009>
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review*, 23(3), 393–404. <https://doi.org/10.5465/amr.1998.926617>
- Sawadogo, A. D., Sawadogo, Z., Ataky, S., Askia, K. M., Roland, K., & Boussim, I. (2022). Preliminary Investigation of Mobile Banking Attacks in West Africa: Feedback from Orange Money Customers in Burkina Faso. Paper presented at the International Conference on e-Infrastructure and e-Services for Developing Countries. [https://doi.org/10.1007/978-3-031-06374-9\\_2](https://doi.org/10.1007/978-3-031-06374-9_2)
- Srivastava, S. C., Chandra, S., & Theng, Y. L. (2010). Evaluating the role of trust in consumer adoption of mobile payment systems: An empirical analysis. *Communications of the Association for Information systems*, 27, 561–588. <https://hal.archives-ouvertes.fr/hal-00537097/>
- Tournois, N., & Cheikho, A. (2015). L'impact des facteurs d'adoption des innovations sur la relation banque-client dans le contexte mobile. *Congrès IAE France*.
- Touzani, M., & Driss, F. B. (2007). Sécurité perçue et fréquentation des points de vente: proposition d'une échelle de mesure et étude d'impact. 10ème Colloque Etienne Thil, La Rochelle, France. Retrieved from [https://www.researchgate.net/publication/260170996\\_Securite\\_percue\\_et\\_frequentation\\_des\\_points\\_de\\_vente\\_proposition\\_d'une\\_echelle\\_de\\_mesure\\_et\\_etude\\_d'impact](https://www.researchgate.net/publication/260170996_Securite_percue_et_frequentation_des_points_de_vente_proposition_d'une_echelle_de_mesure_et_etude_d'impact)
- Tritah, S., & Daoud, M. (2021). The conceptual and theoretical foundations of the PLS structural equation method. *International Journal of Accounting, Finance, Auditing, Management and Economics*, 2(1), 378–395. <https://doi.org/10.5281/zenodo.4474527>
- Veijalainen, J. (2007). *Developing Mobile Ontologies; who, why, where, and how?* 2007 International Conference on Mobile Data Management. <https://doi.org/10.1109/MDM.2007.85>
- Wang, W. T., Ou, W. M., & Chen, W. Y. (2019). The impact of inertia and user satisfaction on the continuance intentions to use mobile communication applications: A mobile service quality perspective. *International Journal of Information Management*, 44, 178–193. <https://doi.org/10.1016/j.ijinfomgt.2018.10.011>

- Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in human behavior*, 21(1), 105–125. <https://doi.org/10.1016/j.chb.2003.11.008>
- Wetzels, M., Odekerken-Schröder, G., & Van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS quarterly*, 177–195. <https://doi.org/10.2307/20650284>
- Xin, H., Techatassanasoontorn, A. A., & Tan, F. B. (2013). Exploring the influence of trust on mobile payment adoption. <https://aisel.aisnet.org/pacis2013/143>
- Yousafzai, S., Pallister, J., & Foxall, G. (2009). Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal*, 29(5), 591–605. <https://doi.org/10.1080/02642060902719958>
- Zhani, N., Mouri, N., & Ahmed, T. (2022). The role of mobile value and trust as drivers of purchase intentions in m-servicescape. *Journal of Retailing Consumer Services*, 68, 103060. <https://doi.org/10.1016/j.jretconser.2022.103060>
- Zhou, T. (2011). Examining the critical success factors of mobile website adoption. *Online Information Review*. <https://doi.org/10.1108/14684521111161972>

# Towards Optimization of Patients' Turnaround Time using Bluetooth Low Energy Based Solutions

---

Ganes Raj Muthu Arumugam

Faculty of Management, Multimedia University, Malaysia

Saravanan Muthaiyah

Faculty of Management, Multimedia University, Malaysia

Thein Oak Kyaw Zaw

Faculty of Management, Multimedia University, Malaysia

---

**Abstract:** Smart Healthcare can use the Internet of Things (IoT) to broaden the reach of digital healthcare by collecting patient data remotely using sensors. This can reduce Patient Turnaround Time (PTAT) and enable high-quality care to be provided. PTAT is the length of time from when a patient arrives at the hospital until they are allowed to return home. Malaysia's Ministry of Health claimed in 2016 that healthcare at government hospitals continues to encounter issues in providing high-quality care to patients, particularly in terms of the PTAT of patients who receive treatment versus those who are sent home without treatment. In this paper, we propose a Bluetooth Low Energy-based solution that optimizes PTAT using low calibrated transmission power, allowing hospitals to enable Real-time Patient Localization and Patient Movement Monitoring. The RSSI value is used to calculate the distance between a wearable device and the Access Points (AP) situated throughout the facility. When a patient passes an AP, data such as the wearable device name and RSSI value are taken and saved in a database, to determine the patient's location. A proof of concept was conducted using three AP points and 8 wearable devices to gauge distance measurement.

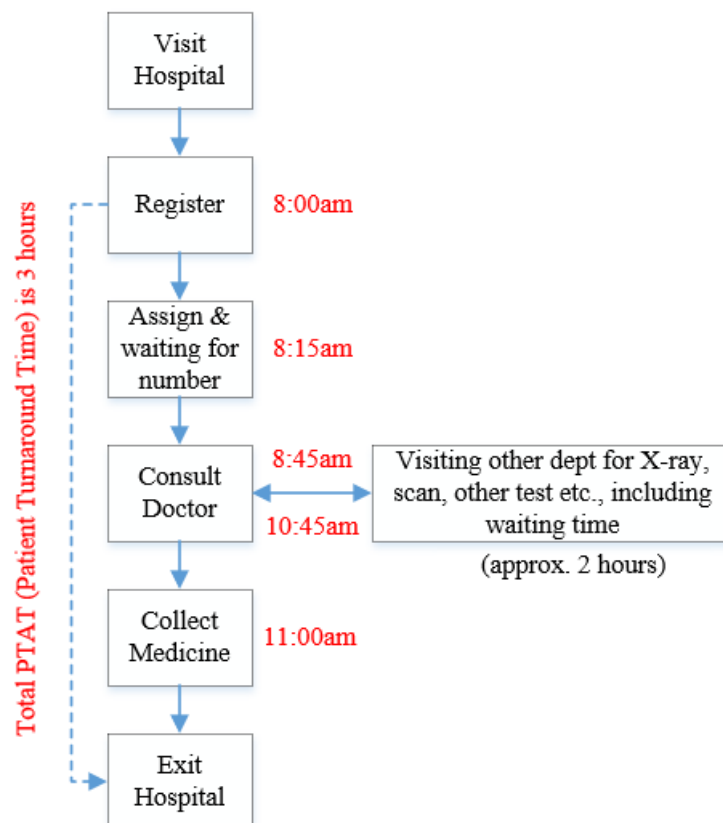
**Keywords:** BLE, Healthcare, RSSI, Optimization, Patients' Turnaround Time (PTAT).

## Introduction

Overcrowding in hospitals, patients not receiving timely treatment, and people missing doctors' appointments are all common problems in the healthcare industry (Vize, 2017). Not only that, but patients must wait longer to be processed and seen by a doctor, which adds to their wait time. Patients may wander about the hospital property at this period, making it difficult for employees to locate them. Additionally, issues could arise if a doctor contacts a patient from a different department after finishing with another patient. As a result, a patient

may wander aimlessly from one department to the next or be summoned by another doctor, and their whereabouts are ultimately unknown. This status quo does not just affect an individual but others as well. It makes the waiting duration for all patients (Patient Turnaround Time, PTAT) to be longer than usual and productivity to drop significantly.

Figure 1 shows an example of how the PTAT is calculated. Hospital optimization is therefore necessary to enhance better patient care by improving control of resource use and enhancing hospital productivity ([Huang, Hwang & Lin, 2021](#)).

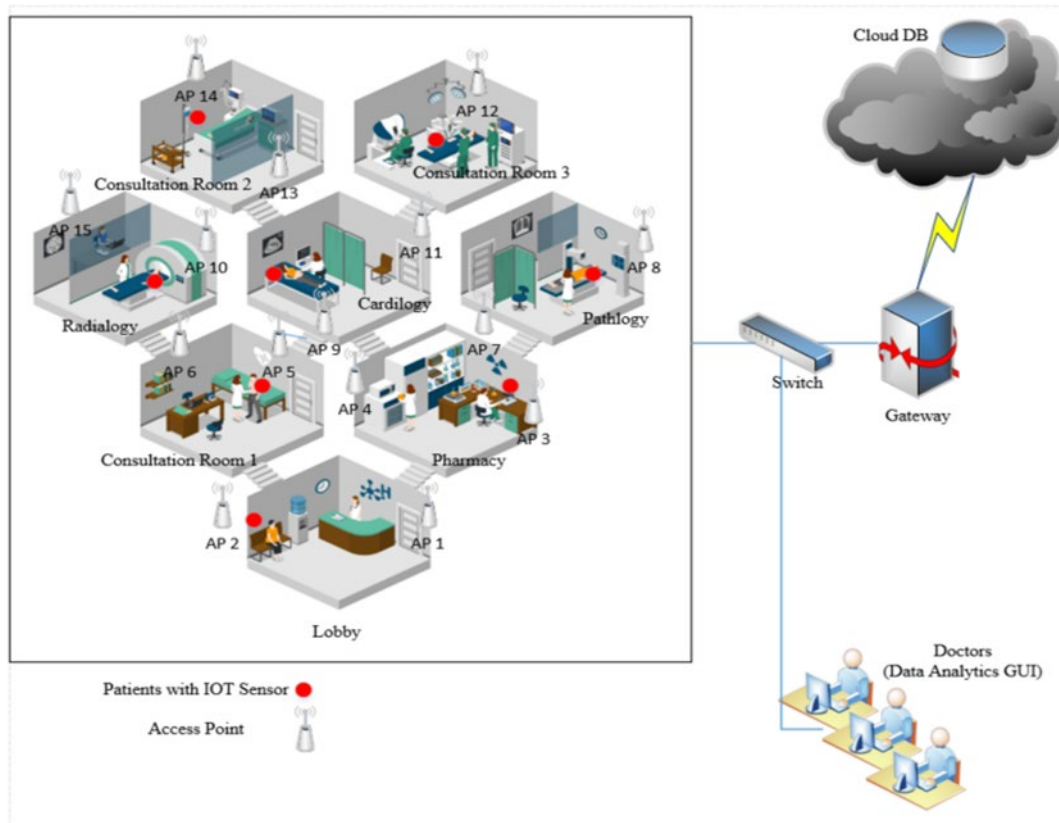


**Figure 1. How PTAT is calculated**

The risk of a patient missing an appointment exists even while they are in medical facilities because hospital employees cannot see or recognize the patient's position most of the time before the actual treatment. These problems culminate into dissatisfaction among patients, doctors and the public, as stated by Malaysia's Ministry of Health ([Ministry of Health, 2016](#); [National Institute for Health and Clinical Excellence, 2007](#)). Thus, optimizing quality of care and better managing the resources at medical facilities are essential. Even so, not many studies or solutions have been able to combine localization and monitoring into a single complete solution for PTAT, as it is not an easy task to accomplish.

As the world progresses into an era of Smart Healthcare, it is crucial that a solution exists if developments are to commence in a fast manner ([Zhu et al., 2019](#)). In general, an efficient and comprehensive Real Time Patient Location Tracking solution will mainly be based on two

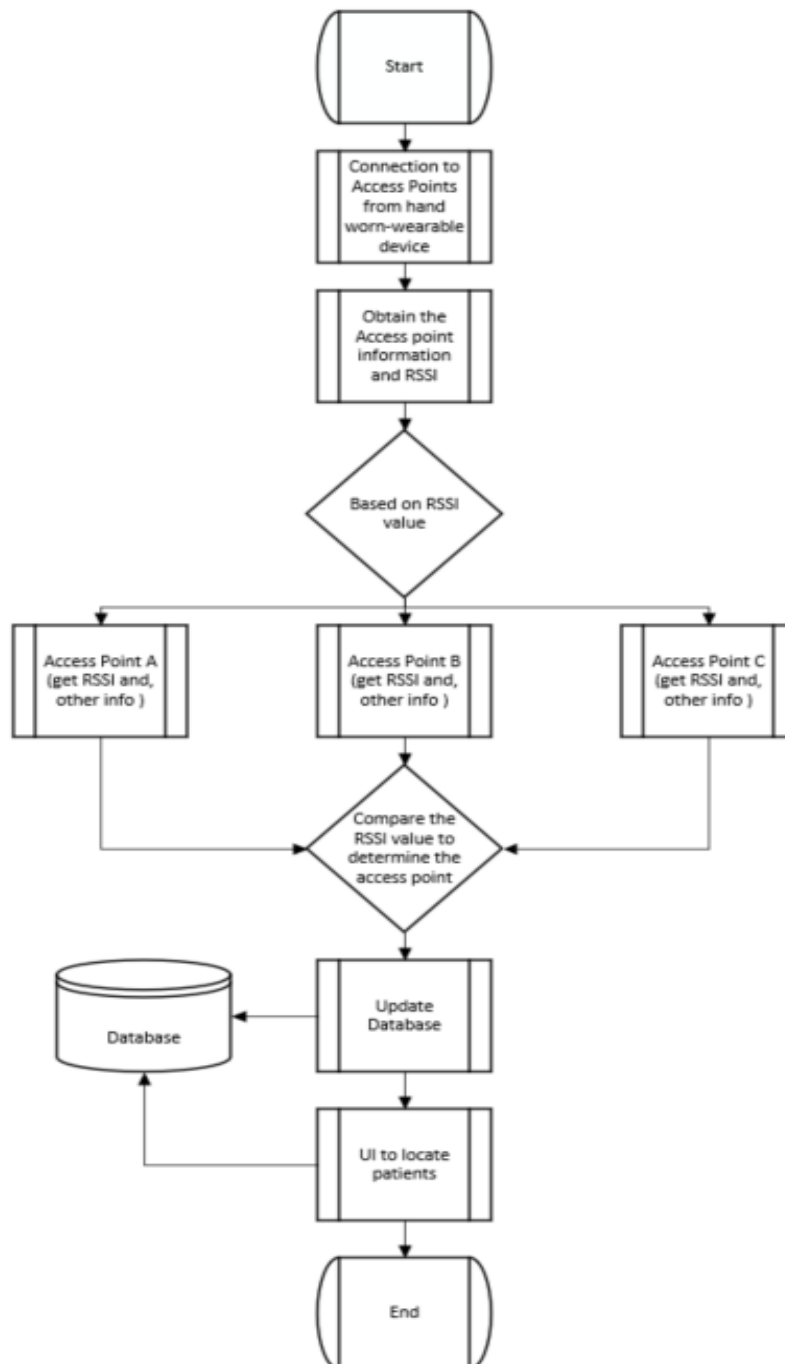
technologies: Bluetooth Low Energy (BLE) and Internet of Things (IoT) (Lin & Lin, 2018). BLE allows monitoring on its own (Mackey *et al.*, 2020), while IoT is used for data collection and analysis.



**Figure 2. Real-Time Patient Location Tracking Solution architecture**

In our solution, upon arrival at the hospital by a patient, a BLE-tagged bracelet will be issued in which each tag will include important patient information, such as ID, name, RSSI value and other details. When a patient travels around the hospital, readers called Access Points (APs) on the walls and ceilings of the hospital and its surrounding area obtain information about the location of the tags and send it to a cloud database for storage and analysis. Refer to Figure 2. for the architecture diagram.

To estimate the locations of patients, low calibrated transmission power (Tx) wearable devices are used and RSSI (Received Signal Strength Indicator) values are obtained, as shown in Figure 3. Patients receive RSSI signals via their hand-worn device, and a system server uses the APs and locations mapping table to map the estimated nearest beacons transmitted from the patient's side to the locations of the pertinent subareas. For the proof of concept, we tested with 3 APs and 8 wearable devices using the algorithm described in Figure 3.



**Figure 3. Flow chart of positioning and data capture algorithm**

## Related Work

The Received Signal Strength Indicator (RSSI) is the foundation of several localisation methods in Wireless Sensor Networks. Absolute location is not always possible, hence localization using RSSI is common compared with other technologies, such as Wi-Fi, infrared or ultrasonic-based solutions. We can determine the RSSI trends quite well based on the variation of radio signals. We will be able to tell if we are going closer to or farther away from an Access Point based on if the signal is getting stronger or weaker. Even better, if we are aware



of the precise mapping between the RSSI and the position of the particular receiving device, we may be able to determine the distance with some degree of accuracy.

Numerous localization efforts are being carried out; governance, economy, administration, infrastructure, technology, and people are all part of the location and movement tracking techniques idea. This implies that they may have varying communication requirements. Wireless technologies, such as Wi-Fi, LiFi, BLE, ZigBee, RFID, LoRa, and LTE (Long Term Evolution) have emerged as answers to the communication requirements of localization techniques ([García et al., 2018](#)) which link to the Smart Healthcare industry. Future smart healthcare systems, also known as the Internet of Medical Things (IoMT), will integrate a slew of wireless devices and apps that employ wireless communication technologies to share healthcare data.

Smart healthcare necessitates adequate bandwidth, dependable and secure communication linkages, energy-efficient operations, and support for Quality of Service (QoS). The incorporation of Internet of Things (IoT) technology into healthcare systems has the potential to greatly improve intelligence, flexibility, and interoperability. Currently, IoT communication protocols and technologies are appropriate for smart healthcare applications ([Gardašević et al., 2020](#)). Furthermore, as the Internet of Things (IoT) evolves, the rate at which physical items are connected to the Internet is rising dramatically ([Al-Fugaha et al., 2015](#)). Low-power wireless technologies have received special attention as a major enabler for energy-efficient IoT-based healthcare systems particularly suitable for a Real Time Patient Location Tracking Solution.

Many wireless devices have been studied in order to minimize the expense and complexity of indoor position systems. A description of the common technologies ([Glow labs, 2019](#)) can be found in Table 1.

**Table 1. Comparison of the Common Technologies for Optimization of Patient Turnaround Time Solution**

Wireless Technology	Cost	Availability	Implementation Complexity	Interference	Accuracy
Wi-Fi	Moderate	High	Low	High	Moderate
Li-Fi	High	Low	High	High	Moderate
BLE	Low	High	Low	Moderate	High
Zigbee	High	Moderate	Low	Moderate	Low
RFID	Low	High	Low	Moderate	Low
LoRa	Moderate	Low	Moderate	Moderate	Low

RSSI is a measure that indicates how effectively the device can pick up a signal from a network or access point. It is a number that might help you figure out if you have adequate signal to establish a reliable wireless connection ([Bensky, 2019](#)). Note that an RSSI number is not the same as transmit power from a router or AP because it is derived from the client device's Wi-Fi card. Each received packet may have its received signal intensity (energy) assessed. The

received signal strength indication is calculated by quantizing the observed signal energy. MAC, NWK, and APL layers have access to the RSSI and the time the packet was received (timestamp) for analysis (Farahani, 2008). RSSI is a relative index (Herres, 2021), whereas dBm is an absolute statistic that represents power levels in milliwatts. RSSI may be measured on a scale of 0 to 255, and each chipset manufacturer can select its own “RSSI Max” number, according to the IEEE 802.11 standard (a large volume of specifications for building Wi-Fi equipment). For example, Cisco employs a 0-100 scale, but Atheros uses a 0-60 scale. The manufacturer has complete control. However, the greater the RSSI score, the better the signal.

A better technology could be BLE, as lower in cost, higher in availability, and lower in implementation complexity, with moderate interference and high accuracy.

## RSSI Values for Distance Estimation Definition

The first step in the experiment is to determine the average reference RSSI value,  $RSSI_r$ , at a distance of 1 m for Bluetooth applications (Maccari & Cagno, 2021). Apart from that, the maximum RSSI value at a distance of 5 m for the specified transmitted power must be observed. The results of the first stage of the experiment are shown in Table 2 based on the experimental BLE device, which used the nRF52832 chipset (Figure 4). The experiment was carried out with the nRF52832, a flexible Bluetooth 5.2 system-on-a-chip (SoC) with a maximum RSSI sensitivity of -96 RSSI value (Nordic Semiconductor, 2021).



Figure 4. nRF52832 chipset

Table 2. Results for RSSI Measurement for Three Different Distances using Two Devices under Line-Of-Sight Condition

Device Number, $n$	Condition	Distance, $m$ in meters	Average RSSI, $RSSI_{avg}$
1	No obstacle – Line of sight	0	-34.01
2			-36.43
1		1	-50.01
2			-52.13
1		3	-67.12
2			-68.15
1		5	-88.45
2			-89.14

Table 2 shows that the average RSSI readings for both devices is -35 RSSI value at a distance of 0 m. A similar scenario was also discovered with the other two distances, but there is a tiny variance in value for the 1 m distance. However, a difference of merely -1 RSSI value is insufficiently large to suggest that the results acquired are unreliable. At a distance of 5 metres, both devices produced average maximum RSSI values of from -88 to -94 RSSI value, respectively, which will be utilized. A number greater than this indicates a user's distance is more than 5 m. The average of the RSSI values is obtained using the formula to determine the RSSI reference point:

$$\text{For } m = 1, \quad \text{RSSI}_r = \frac{(\text{RSSI}_{avg1} + \text{RSSI}_{avg2})}{2}$$

## RSSI drawback

In reality, there are several factors that might influence the RSSI ([Figueiredo e Silva et al., 2018](#)), rendering it inaccurate for distance calculation. The two key elements that affect RSSI are discussed in this section, as well as how the technique overcomes some of these limitations.

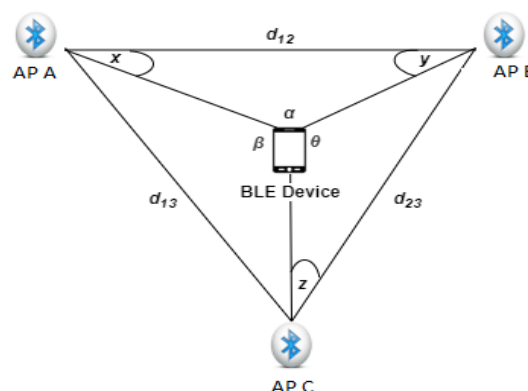
When it comes to internal components, it is mostly the hardware and software that can have a big impact on the RSSI. The transmission power of a Bluetooth chipset can have an impact on RSSI. Not only that, but antenna architecture, orientations, and data transfer capacity can all have a significant impact on the signal strength ([Zhao et al., 2020](#)).

When it comes to external elements, they are separated into two categories: physical obstacles and radio waves. Effects of radio waves include Wi-Fi, which may be set to operate on the same 2.4GHz channel as Bluetooth, allowing both signals to affect each other ([Sibiński, 2021](#)). Because the travelled distance is not great, using a calibrated low Tx method will make it less susceptible to interference from other radio waves. Additionally, angle of arrival (AOA) can significantly affect RSSI and cause variances, especially when the distance is vast. These physical barriers can cause the signal to weaken and vary, causing the calculation to be larger than the actual distance between two people ([Labrique, 2020](#)). This new strategy, on the other hand, causes the RSSI to be large in value, nearing the chipset's maximum sensitivity at the ideal distance of 5 m. Physical obstructions, such as people passing by or nearby walls, will merely raise the RSSI, making the chipset unable to identify it, resulting in less inaccuracy. Nonetheless, because the signal ([Parker, 2017](#)) travels a shorter distance and can only be received within a restricted range, the inaccuracy will be limited and smaller than in many other BLE-based solutions

## Solution Approach – Proof of Concept

Point of Interest (PoI) information applications fall under the topic of proximity solutions (for example, departments in hospitals that provide the user with information about their location). This category also includes options for recovering lost or misplaced items, such as Bluetooth tags. Bluetooth tags send BLE broadcast frames on a regular basis in these implementations. The AP examines these frames for Bluetooth tag information, which it then sends to the location server through an access controller (AC). In PoI proximity applications, it is required to determine which PoIs are in close vicinity to the computed location.

Positioning systems comprise location-based services that use Bluetooth to determine a device's physical location, for real-time locating systems for people monitoring and indoor positioning systems for pathfinding solutions that assist people navigate through complex interior settings. Only by knowing the direction from which the received signal is coming, the estimated distance to that beacon, and the location of the beacon can the application establish the position of its host device.



**Figure 5. Triangulation-Based Location Estimation**

The BLE standard is used to create Bluetooth beacon technology. A beacon sends out a unique ID. An application on a BLE device that receives that ID looks up the transmitting beacon in a database and then provides the user with information about its position. The strategy used to estimate the distance between the BLE device and the beacon are shown in Figure 5. Triangulation-based location estimation is a technique for calculating the position of a point that relies on a known distance between two or three reference points and the angles measured using the Bluetooth direction-finding feature between those reference points to that point. These angles can be the Angle of Arrival or the Angle of Departure. The triangulation technique uses angle measurements (Zhao *et al.*, 2020). Using this method, you may determine any point's location in two-dimensional (2-D) space, given three angles between it and three other reference points.

In 2-D space, however, estimating the position of every point requires a minimum of two angles. The distances between the Bluetooth beacons A–B, B–C, and A–C are denoted by  $d_{12}$ ,  $d_{23}$  and  $d_{13}$ , respectively, in Figure 5. The known angle measurements between the BLE device and Bluetooth beacons, A, B, and C, are  $x$ ,  $y$ , and  $z$ , respectively. The triangulation approach determines the BLE device's position from this known data.

## Proposed architecture for Real-time Patient Localization and Patient Movement Monitoring

This section explains the proposed architecture to capture the data from the patient in order to determine the location the patient in hospital areas based on the RSSI value.

### Experimentation setup for data collection

The experimental setup to simulate the deployment of a Real Time Patient Location Tracking Solution used an existing Wi-Fi network and a floor plan (in a private clinic). We set up environment parameters (AP name, model name, channel, bands, etc.), placed APs on the floor plan, adjusted the APs' location and parameters, viewed the planned results, and uploaded the data captured to a database. Figure 6 shows the APs on the floor plan in the clinic setup for experimentation, to get the RSSI values to identify the distance and determine the nearest access point to give patient location status.



Figure 6. Experimental setup for data collection

Readings from five nRF52832 SoCs powered by a 5 V lithium-ion battery were used in this study. A proof of concept as used to determine whether the method performs as anticipated under ideal circumstances and to determine whether a distance estimate might be included. Two nRF52832s were used in the proof of concept to calculate RSSI readings at various distances for line of sight under perfect conditions. By employing APs to capture data packets from these client devices, the use of two BLE modules ensures that any deviations may be detected. The chipsets will send out advertising packets to the APs every 50 ms (this might vary depending on the scenario) and the AP will scan every 5 s. Following that, the data is entered into a database. The following pieces of data are included in the captured data: Medium Access Control Address, Patient Name, Device Name, RSSI value, Date and Time.

A maximum Tx of -4 RSSI value is more than capable of serving as the transmitter for testing the low-calibrated Tx technique for near location tracking. Tx is set at -8 RSSI value in this study, which is the optimal value because the RSSI reaches -96 RSSI value at a distance of 5 metres.

In the proof-of-concept section, a sample size of -100 to -200 RSSI value measurements was employed to ensure that the data was acceptable and trustworthy. It is worth noting that the experiment was carried out in a controlled setting with no additional network connectivity or barriers. Both the sender and receiver were lifted to 0.5 m at the same time to simulate true wearables on the wrist and provide a direct angle. Figure 6 depicts the Proof-of-Concept experimental setup, while Table 3. depicts a sample of data gathered from the scan.

**Table 3. Sample of Captured Data which is stored in Database for Analysis**

Access Point	AP Address	Device Name	Device Address	RSSI Value	Date	Time
AP01	00:1B:44:11:3A:B7	BLETag1	01:1C:44:11:3B:B8	-50	15/06/2022	10:00:34
AP02	01:1C:44:11:3B:B8	BLETag2	02:1C:44:11:3B:B9	-25	15/06/2022	10:23:29
AP03	00-14-22-01-23-45	BLETag3	04:1C:44:11:3B:B10	-10	15/06/2022	10:12:34
AP01	01-23-45-67-89-AB	BLETag4	05:1C:44:11:3B:B11	-15	16/06/2022	10:23:57
AP04	00-14-22-01-23-BC	BLETag5	01:1C:44:11:3B:B12	-7	16/06/2022	10:05:50

Data was taken and structured in a database with the same information as the proof of concept. Devices were raised to a height of 7 m to simulate actual wearing of wearables. The usage of four devices is intended to assess the approach's capacity to handle many users as well as the number of successful scans for various angles of arrival.

### Analysis and results based on the data collection

In the case of Bluetooth, the distance travelled and the broadcasting power value affect the signal strength. Bluetooth uses broadcasting signals: the RSSI intensity of the signal ranges from -26 to -100. Using a different iBeacon standard value, Measured Power, it is possible to



determine the Bluetooth proximity between two coupled or unpaired devices and the beacon. Measured Power (also known as the 1 Metre RSSI) is a read-only constant that has been factory calibrated and shows the anticipated RSSI at a distance of 1 metre from the beacon. RSSI has a tendency to change as a result of outside influences that affect radio waves, such as diffraction, interference or absorption. The RSSI becomes more erratic the farther away the device is from the beacon. Measured Power and RSSI enable calculating the distance between the device and the beacon:

$$\text{Distance} = 10^{((\text{Measured Power} - \text{RSSI}) / (10 * N))}$$

where N is a constant that depends on environmental factors. It ranges from 2 to 4 (low to high strength).

For example, if Measured Power is -69 and obtained RSSI value is -80, with N=2 (low strength), then calculated Distance =  $10^{((-69 - (-80)) / (10 * 2))} = 3$  metres.

Table 4 shows the results of the RSSI value based on the distance experimentation with the number of 1, 4 and 8 devices.

**Table 4. Results of RSSI value based on the distance and number of devices**

<i>Device Number, n</i>	<i>Condition</i>	<i>Distance, m in metres</i>	<i>Average RSSI, RSSI<sub>avg</sub></i>
1	No obstacle – Line of sight	0	-34.01
4			-36.43
8			-37.55
1		1-2	-50.01
4			-52.13
8			-53.14
1		2-3	-67.12
4			-68.15
8			-68.32
1		3-4	-88.45
4			-89.14
8			-89.53

## Significance of the architecture

Many problems in healthcare facilities can be observed, such as hospital overcrowding. As described in the Introduction, patients may wander about, making their whereabouts unknown. Hence, using Real-time Patient Localization and Patient Movement Monitoring helps to locate the patient to minimize the turn-around time. A BLE-tagged wristband with each tag containing vital patient data, including an ID number, name, and other specifics, will be given to each patient upon their arrival at the hospital. When a patient travels around the hospital, Access Points on the walls and ceilings of the hospital and its surrounding area obtain



information about the location of the tags and send it to the cloud database for processing and analysis (Figure 2).

Therefore, using this data and using the Real-Time Patient Location and Patient Movement system, the staff and the doctors can locate the patients and quickly contact them to be reported. By doing this, the patient will get treatment faster than expected and the throughput in every department will be increased, which can contribute to a reduction of patient turnaround time from 3 hours to 2 hours. At the same time, the doctors can treat more patients using the Real-Time Patient Location and Patient Movement system with the BLE IoT solutions.

## Conclusion

An increase in patient turnaround time (PTAT) has a direct impact on health care industries as patients' quality of service is reduced. One of the crucial KPIs in the health care sector is the turnaround time for patients. Faster turnaround times are always the secret to raising patient satisfaction and quality of service. Additionally, it saves the hospitals money and resources. Low PTAT is not just a sign of a hospital's effectiveness, it also serves as a sign of high calibre hospital service. Real Time Patient Location Tracking can be used to detect patients more quickly in a hospital setting and provide quicker care. The current inability of the hospital staff to find a patient's whereabouts increases the PTAT.

In the current situation, without Real Time Patient Location Tracking, a patient spends almost 3 hours in the hospital from the registration process until he/she leaves the premises (Figure 1). During this time, hospital staff and doctors do not know the actual location of the patient and, as a result, it is difficult to be contactable and manage the consultation time with the doctor, as the patient can leave the hospital for meal breaks, talking to their fellow patients or friends, etc. This may also make the patient miss the consultation time with a doctor.

The Real Time Patient Location Tracking and Movement Solution allows hospital staff to follow the patient's whereabouts and swiftly get in touch with them for a consultation. Based on the data collection and analysis, the patient will receive treatment faster than expected. Real-time patient location tracking and increased departmental throughput will help cut the patient turnaround time from three to two hours. This will avoid the need to wait for the patient to show up for the consultation, because staff could contact them and ask for an immediate report for consultation. Table 5 shows the comparison of the benefits upon implementing the Real Time Patient Location Tracking and Movement Solution.

**Table 5. Comparison of Benefits before and after Implementation of Real Time Patient Location Tracking and Movement Solution**

Description	Before	After
Registration	✓	✓
Patient missed Doctor's consultation due whereabouts in hospital	✓	✗
Trackable after registration	✗	✓
Locate the Patient where about within hospital	✗	✓
Faster Doctor consultation	✗	✓
Improve the Quality of Service (QoS)	✗	✓
Optimize the throughput of the departments	✗	✓
Saving Time	✗	✓
Cost saving	✗	✓
Patients are happy	✗	✓

## Future Work

In order to conduct efficient Real-Time Patient Location Tracking to minimize the Patient Turnaround Time (PTAT), we used low calibrated Tx in our proposed solution. RSSI will be used as a bonus feature for distance estimate in this method, and will be determined by the number of successful signal scans. Experimentation showed that our proposed solution is positive and accurate. It has been proven to have good accuracy for Real-Time Patient Location Tracking in order to optimize the Patient Turnaround Time (PTAT). As a result, it can be concluded that adopting a low-calibrated Tx technique for Real-Time Patient Location Tracking to improve Patient Turnaround Time (PTAT) is a useful method that governments and implementors may use.

Based on the findings of the study, low calibrated Tx for Real Time Patient Location Tracking to optimize the Patient Turnaround Time (PTAT) was highly successful and accurate. Nonetheless, there are still some limits and need for development. Mass testing, for example, has not yet been done, but it may be a future direction that researchers take before deciding to use in the real world. Not only that, but there are constraints in place, such as a limited number of devices and distance testing. If further experiments with more distances of 5 m can be undertaken, the results will be more robust. As a result, it is critical that more testing be done to determine the accuracy's consistency. When looking at the results of the experiment, it is evident that, as the number of devices increases, the number of successful scans decreases since the receiver has a limited time scan interval. However, this variable can be altered to improve precision or to accommodate more users. It should balance the number of users and the scanning interval to reach an appropriate level of RSSI accuracy. Otherwise, a large number of successful scans for a small number of users would give the impression of high accuracy when it is not.

Based on the experiment conducted real-time patient location tracking can make a significant contribution to public hospitals in Malaysia in terms of reducing patient waiting time. As a result, it appears necessary to determine hospital requirements, apply novel technologies such as BLE and the Internet of Things, and integrate them to gain maximum benefits to improve patient turn-around time in Malaysian public hospitals.

In the future work, BLE chipsets with even lower power consumption can be integrated with the Real-Time Patient Location Tracking system to save energy and improve tracking sensitivity.

## References

- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies protocols and applications. *IEEE Communications Surveys & Tutorials*, 17(4), 2347–2376. <https://doi.org/10.1109/COMST.2015.2444095>
- Bensky, A. (2019). *Short-range Wireless Communication*, 3rd Edition. Elsevier. <https://doi.org/10.1016/C2017-0-02356-X>
- Farahani, S. (2008). *ZigBee Wireless Networks and Transceivers*. Elsevier. <https://doi.org/10.1016/B978-0-7506-8393-7.X0001-5>
- Figueiredo e Silva, P., Richter, P., Talvitie, J., Laitinen, E., & Lohan, E. S. (2018). Challenges and Solutions in Received Signal Strength-Based Seamless Positioning. In Conesa, J., Pérez-Navarro, A., Torres-Sospedra, J., & Montoliu, R. (eds), *Geographical and Fingerprinting Data to Create Systems for Indoor Positioning and Indoor/Outdoor Navigation*. Academic Press. <https://doi.org/10.1016/B978-0-12-813189-3.00013-7>
- García, L., Jiménez, J. M., Taha, M., & Lloret, J. (2018). Wireless Technologies for IoT in Smart Cities. *Network Protocols and Algorithms*, 10(1). <https://doi.org/10.5296/npa.v10i1.12798>
- Gardašević, G., Katzis, K., Bajić, D., & Berbakov, L. (2020). Emerging Wireless Sensor Networks and Internet of Things Technologies—Foundations of Smart Healthcare. *Sensors* 2020, 20(13), 3619. <https://doi.org/10.3390/s20133619>
- Glow labs. (2019). Table Comparing Wireless Protocols For IoT Devices. Available at <https://glowlabs.co/wireless-protocols/>
- Herres, D. (2021). Understanding decibels and decibel measurements. Test & Measurement Tips. <https://www.testandmeasurementtips.com/understanding-decibels-and-decibel-measurements-faq/#respond>
- Huang, Y.-C., Hwang, J.-C., & Lin, Y.C. (2021). The Optimization between Physician Satisfaction and Hospital Profit in Cross-Hospital Scheduling—A Case Study of Some Hospitals in Taiwan. *Healthcare (Basel)*, 9(8), 1004. <https://doi.org/10.3390/healthcare9081004>
- Labrique, D. (2020). Effects of obstructions on the accuracy of Bluetooth contact tracing. OSF Preprints. Available from <https://osf.io/ezb43>

- Lin, Y.-W., & Lin, C.-Y. (2018). An Interactive Real-Time Locating System Based on Bluetooth Low-Energy Beacon Network. *Sensors*, 18(5), 1637. <https://doi.org/10.3390/s18051637>
- Maccari, L., & Cagno, V. (2021). Do we need a contact tracing app? *Computer Communications*, 166, 9–18. <https://doi.org/10.1016/j.comcom.2020.11.007>
- Mackey, A., Spachos, P., Song, L., & Plataniotis, K. N. (2020). Improving BLE Beacon Proximity Estimation Accuracy Through Bayesian Filtering. *IEEE Internet of Things Journal*, 7(4), 3160–3169. <https://doi.org/10.1109/JIOT.2020.2965583>
- Ministry of Health. (2016). Annual Report Kementerian Kesihatan Malaysia. [https://www.moh.gov.my/moh/resources/Penerbitan/Penerbitan%20Utama/ANNUAL%20REPORT/Annual\\_Report\\_MoH\\_2016\\_compressed.pdf](https://www.moh.gov.my/moh/resources/Penerbitan/Penerbitan%20Utama/ANNUAL%20REPORT/Annual_Report_MoH_2016_compressed.pdf)
- National Institute for Health and Clinical Excellence. (2007). Acutely ill patients in hospital- Recognition of and response to acute illness in adults in hospital. NICE clinical guideline 50, London, UK.
- Nordic Semiconductor. (2021). nRF52832, Versatile Bluetooth 5.3 SoC supporting Bluetooth Low Energy, Bluetooth mesh and NFC. Nordicsemi.com [Internet]. Available from <https://www.nordicsemi.com/-/media/Software-and-other-downloads/Product-Briefs/nRF52832-product-brief.pdf?hash=2F9D995F754BA2F2EA944A2C4351E682AB7CB0B9&la=en>
- Parker, M. (2017). *Digital Signal Processing 101*, 2nd Edition. Newnes. Available at <https://www.sciencedirect.com/book/9780128114537/digital-signal-processing-101#book-info>
- Sibiński, D. (2021). WiFi and Bluetooth interference — diagnosing and fixing. CodeJourney.net [Internet]. Available from: <https://www.codejourney.net/2017/04/wifi-and-bluetooth-interference-diagnosing-and-fixing/>
- Vize, R. (2017). How can health services keep pace with the rapid growth of cities? *The Guardian*, 24 February 2017. <https://www.theguardian.com/sustainable-business/2017/feb/24/how-can-health-services-keep-pace-with-the-rapid-growth-of-cities>
- Zhao, Q., Wen, H., Lin, Z., Xuan, D., & Shroff, N. (2020). On the accuracy of measured proximity of Bluetooth-based contact tracing apps. In Park, N., Sun, K., Foresti, S., Butler, K., Saxena, N. (eds), *Security and Privacy in Communication Networks*. SecureComm 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 335. Springer, Cham. [https://doi.org/10.1007/978-3-030-63086-7\\_4](https://doi.org/10.1007/978-3-030-63086-7_4)
- Zhu, H., Wu, C. K., Koo, C. H., Tsang, Y. T., Liu, Y., Chi, H. R., & Tsang, K.-F. (2019). Smart Healthcare in the Era of Internet-of-Things. *IEEE Consumer Electronics Magazine*, 8(5), 26–30. <https://doi.org/10.1109/MCE.2019.2923929>

# A Proposal for Dynamic and Secure Authentication in IoT Architectures Based on SDN

---

Younes Abbassi

Hassan II University, Casablanca, Morocco

Hicham Toumi

Chouaïb Doukkali University, El Jadida, Morocco

El Habib Ben Lahmar

Hassan II University, Casablanca, Morocco

---

**Abstract:** The connectivity of private resources on public infrastructure, user mobility, and the advent of new technologies have added new client and server-side security requirements. Security is the major element of the Internet of Things (IoT) that will certainly reinforce an even greater acceptance of IoT by citizens and companies. Security is critical in this context given the underlying stakes. This paper aims to advance the thinking on authentication of connected objects by proposing an authentication mechanism that meets the needs of IoT systems in terms of security and performance. It is based on SDN (Software-Defined Networking), which refers to a set of advanced technologies that allow for centralized control of network resources. OTP (One-Time Password) is a type of authentication that could be useful in connected object environments and smart cities. This research work extends the principle of OTP and proposes a lightweight authentication method using a new approach to OTP generation that relies on two parameters (Two-Factor Authentication, 2FA) to ensure the security of underlying systems. Subsequently, we leverage the combination of SDN and the 2FA algorithm to propose an adaptive authentication and authorization solution in the IoT network.

**Keywords:** Internet of Things (IoT), Software-Defined Networking (SDN), One-Time Password (OTP), Two-Factor Authentication (2FA).

## Introduction

Internet of Things (IoT) and Cloud Computing are actually broad areas of interest and research. They will change the way we live and work by making different aspects of life smart. According to IoT Analytics estimates by Koohang *et al.* (2022), at the end of 2018 there were around 50.1 billion users connected to IoT devices.

The Internet of Things opens up new possibilities, such as the capacity to remotely monitor and manage devices, as well as to analyze and act on data from multiple real-time traffic data streams. Consequently, with the advent of cloud computing ([Junior et al., 2021](#)), IoT products are changing habits and cities by enhancing infrastructures, improving municipal services to make them more effective and cost-effective, improving transportation services by reducing traffic congestion, boosting citizen safety, and delivering smart health services ([Mitake et al., 2021](#)). IoT technologies, on the other hand, provide a slew of security and privacy concerns. Due to the hardware limitations of IoT devices, implementing and deploying complete and effective security and privacy solutions for the IoT environment remains a major challenge.

The IoT's immense power comes from the fact that its objects can communicate, analyze, process, and manage data without the need for human interaction. However, security issues are holding back the evolution and rapid deployment of this high technology. Identity theft, information theft, and data modification are a real danger for a parent system. Several cyberattacks have been blamed on flaws in the authentication procedures of connected door locks, computers, and phones. In 2016, Anna Senpai developed Mirai ([Biggs, 2016](#)), a malicious malware that allows attackers to take control of susceptible connected equipment such as surveillance cameras and routers, launching large-scale distributed denial-of-service (DDoS) assaults. Mirai turns infected objects into bots; in other words, it turns them into autonomous and intelligent computer agents controlled remotely.

In 2017, another malicious program, BrickerBot, appeared. It brute-force attacks objects using conventional password identification systems ([Lagane, 2017](#)) in order to eliminate them and thus delete their data. It is evident that the prosperity of the IoT can only be achieved when good security is provided for the objects and the communication networks used. It is crucial to implement a security policy that prevents any malicious or unauthorized object from accessing the IoT systems, reading their data, or modifying them. For an object to have the ability to operate a service or associate with a network, it must first prove its identity and have the necessary access rights. Connected objects are generally very limited in computing and storage capacity. They are also constrained by energy consumption. Therefore, we cannot use classical security mechanisms, such as authentication with digital certificates, or the use of asymmetric cryptographic asymmetric cryptographic algorithms, such as Rivest Shamir Adleman (RSA) or Diffie-Hellman ([Kocher, 1996](#)), because they are very costly or not even supported by the objects. As a result, a new lightweight and robust mechanism must be created to provide object authentication and data protection services, while adapting to object and communication technology capabilities.



This article describes a security system to ensure the authentication services of connected objects, the integrity of the inter-exchanged data, and the confidentiality of the information. This approach must take into account the constraints of the objects and the communication technologies used.

We used the SDN (Software-Defined Networking) technology in conjunction with the 2FA (Two-Factor Authentication) method based on the OTP (One-Time Password) algorithm in order to accomplish this goal. The remainder of the paper is laid out as follows. We first provide some background information on IoT, Cloud Computing, SDN, Access Control, and Authentication, as well as their principles. Then, we describe our proposed solution, its objective, and its functioning. We then provide a discussion of our findings, and, finally, we conclude this paper with some perspectives and further insights.

The objective of our IoT authentication solution is to enable intrusion detection (to prevent identity theft in a virtual environment by using mobile agents to collect malicious data and generate new signatures from this malicious data). We highlight IoT access control and authentication devices that can dynamically recognize and connect multiple real and virtual sensors in a unified secure system, and provide dynamic deployment of updates between clusters in an IoT cloud, using master and slave SDN.

What makes our work unique is that we use SDN architecture for dynamic deployment of a strong authentication mechanism and generation of inter-cluster updates in an IoT network, a framework never before dealt with by researchers, today offering access to the IoT network by registering and verifying the identity of objects, as well as updating the framework automatically.

## Theoretical Foundations and Related Research

### Internet of Things (IoT)

The CERP-IoT “Cluster of European Research Projects on the Internet of Things” represents the Internet of Things as “a dynamic backbone of a global network. This global network has self-configuration capabilities based on interoperable communication standards and protocols. Physical and virtual items in this network have identities, physical attributes, virtual personalities, and intelligent interfaces, and they’re all perfectly interwoven” ([Botta et al., 2014](#)).

Internet of Things is a continuously evolving system of interconnected devices based on a set of technologies, namely RFID, Barcode, Zigbee, WSN, Wi-Fi and Cloud Computing. It faces several challenges, of which security is a major challenge. The scope of application of IoT is



almost unlimited, which will allow it to make the environment intelligent and favourable to any human activity ([Abdellatif et al., 2022](#)).

## Cloud Computing

The National Institute of Standards and Technology (NIST) claims that ([Sturm, Pollard & Craig, 2017](#)), Cloud computing is a concept that allows users to access a shared set of computer resources (such as servers, storage, and apps) on-demand over a telecommunications network. Cloud computing is a model that allows users to use a shared set of computing resources on demand (e.g., servers, storage, apps) that may be immediately put to use over a telecommunications network. There are four different kinds of clouds:

- 1) Public Cloud: dedicated to the general public, it is a set of free or paid services accessible via the Internet. It is offered by a company that manages an infrastructure that belongs to it.
- 2) Private Cloud: a set of resources available to a single customer that can be managed by the user company or by an external provider.
- 3) Community Cloud: cloud resources shared by several companies or organizations which can be managed by member organizations or by an external provider.
- 4) Hybrid Cloud: allows the company to be able to supply services in multiple clouds either public, private or community.

Some services offered by Cloud Computing are SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and NaaS (Network as a Service) ([Hussain & Chun, 2022](#)). IaaS provides computing and storage services on a rental basis; in addition to the data storage in IaaS, the data will be universally accessible on the Internet. PaaS offers a complete environment for the development and deployment of applications. SaaS allows remote access to software via the Internet. Users can have heterogeneous networks with NaaS since it gives virtual network(s) to them.

## SDN (Software-Defined Networking)

SDN is a technology that is now mature, usable and “marketed” by operators. It allows centralizing the control logic in a controller. It also enables the separation of the control and data planes ([Munther et al., 2021](#)). SDN is characterized by the following elements ([El Kamel, Eltaief & Youssef, 2022](#)):

- Separation of control plane and data plane: Control functionality is removed from the network nodes, which become simple (packet) forwarding elements.

- Forwarding (packet) decisions are flow-based (rather than destination-based): A flow is a collection of packets that travel from one point to another. All packets in the same flow are subject to identical service and processing policies at the transfer devices.
- The control logic (intelligence) is passed to a third party, the SDN controller or Network Operating System (NOS). The NOS is a software platform based on server technology that provides the tools and abstractions required to simplify the construction of forwarding devices using an abstract view of the network and logical centralization. Its purpose is therefore similar to that of a traditional operating system.
- The network is programmable: The network can be programmed using software applications that connect with the devices on the underlying data plane and run on the NOS. This is a core feature of SDN, as well as its primary value-added feature.

### Functions of the SDN

SDN separates the data plane from the control plane, as previously indicated. In other words, the intelligence of the network is transferred to a controller, all computations are performed there, and many applications and features can be added as needed.

In Tok & Demirci (2021), the researchers discussed the basic modules of an SDN controller. They concluded that the modules of link discovery, topology management, storage, policy, flow table management and control data are the core modules of the SDN controller. Topology management is one of the essential and critical functions of the architecture. It is provided by two modules, the topology manager and the routing and link discovery manager, that also provide the routing service.

### Authentication and Access Control

Access control is a security technique that can be used to determine which users or programs are allowed to see or use resources in an IT environment (Zhang & Hu, 2021). Physical and logical access control are the two main types of access control. Physical access control restricts access to campuses, buildings, rooms and computer equipment.

Connections to computer networks, system files, and data are all restricted by logical access control.

Access control systems handle approved identity, authentication, access approval, and entity responsibility using login credentials, such as passwords, PINs, biometrics, and electronic or physical keys. An access control model includes (Shan, Zhou & Hong, 2021):

- An access control policy (or rule) that specifies what access to data is allowed;

- An administration policy that specifies how the access controls policy can be updated. An access control mechanism is a software or hardware solution for enforcing an access control policy.

IoT now confronts numerous issues in authenticating the devices and sensors that connect to the network. Because the sensors' hardware IDs can be faked ([Alizadeh, Tadayon & Jolfaei, 2021](#)). As a result, there are few options for authenticating device sensors or home automation devices. Although standard security protocols, such as X10, ZWave, and ZigBee, have been embraced by the industry and can provide encryption methods, it is still a work in progress to develop acceptable mechanisms for authenticating devices.

Many security techniques based on private key cryptographic primitives have been developed due to quick computation and energy efficiency, as mentioned in Nait-Hamoud, Kenaza & Challal ([2021](#)). It is inefficient to keep keys for heterogeneous devices in the IoT because of the scalability issue and the memory requirement. IoT does not now solve all authentication requirements, such as mutual authentication, replay attack resistance, DOS (Denial of Service), MITM (Man in the Middle), and lightweight solutions.

### OTP (One-Time Password)

A one-time password (OTP) is a random string of numbers or letters that is used to authenticate a user for a single transaction or login session ([Lee, Kang & Cho, 2017](#)). A password created by the user is less secure than an OTP, especially if it is weak and/or used across numerous accounts. OTPs can be used in place of or in addition to authentication login information to offer another degree of protection ([Babkin & Epishkina, 2018](#)).

#### Example:

OTP security tokens are microprocessor-based smart cards or pocket-size key fobs that generate a numeric or alphanumeric code to authenticate access to a system or transaction. This secret code varies every 30 or 60 seconds, depending on how the token is programmed.

Mobile device apps, such as Google Authenticator, rely on the token device and PIN to generate the one-time password for two-step verification. Hardware, software, or on-demand security tokens can all be used to implement OTP security tokens. Unlike regular passwords, which remain static or expire every 30 to 60 days, the one-time password is only used for one transaction or login session.

### 2FA (Two-Factor Authentication)

Two-factor authentication (2FA) is a security method that needs two different forms of identity to gain access to anything ([Kemshall, 2011](#)). Two-factor authentication can be used to strengthen the security of an online account, a smartphone, or even a door. 2FA needs two

types of input from the user: a password or personal identification number (PIN), a fingerprint, or a code texted to the user's smartphone before anything being secured can be accessed.

Two-factor authentication is a security feature that prevents unwanted users from getting access to an account using only a stolen password. Users may be at greater risk of compromised passwords than they realize, particularly if they use the same password on more than one website. Downloading software and clicking on links in emails can also expose an individual to password theft ([Sadri & Asaar, 2021](#)).

## Relevant Works and Limitations

**Table 1. State of the art.**

Research Work	Used Technology					Summary contributions
	IoT	Cloud	SDN	OTP	2FA	
<a href="#">Hammi et al., 2020</a>	✓	*	*	✓	*	Aim to advance the literature on IoT authentication by proposing three authentication schemes that satisfy the needs of IoT systems in terms of security and performance.
<a href="#">Baseri, Hafid &amp; Cherkaoui, 2018</a>	✓	✓	*	*	*	A method based on the Attribute-Based Encryption (ABE) technique, for designing secure and efficient data access control for mobile cloud
<a href="#">Hammi, Bellot &amp; Serhrouchni, 2018</a>	✓	*	*	✓	*	An approach that uses the asynchronous mode, which is based on the challenge/response method defined by RFC 1994
<a href="#">Botta et al., 2014</a>	✓	✓	*	*	*	Physical and virtual items in this network have identities, physical attributes, virtual personalities, and intelligent interfaces, and they are all perfectly interwoven
<a href="#">Abdellatif et al., 2022</a>	✓	*	*	*	*	Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced data
<a href="#">Hussain &amp; Chun, 2022</a>	*	✓	*	*	*	Services offered by Cloud Computing are SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and NaaS (Network as a Service)
<a href="#">Mutlag et al., 2019</a>	✓	✓	*	*	*	Cloud4IoT is a platform that enables plug-and-play integration of additional sensor objects, as well as dynamic scalability, by automating the deployment, orchestration, and dynamic configuration of IoT support software components and data processing and analysis applications.

Research Work	Used Technology					Summary contributions
	IoT	Cloud	SDN	OTP	2FA	
<a href="#">Stergiou et al., 2018</a>	✓	✓	*	*	*	Cloud Things, IaaS, PaaS, and SaaS to help developers, deploy, and manage Internet of Things applications more quickly
<a href="#">Munther et al., 2021</a>	*	*	✓	*	*	Scalable and secure SDN-based Ethernet architecture by suppressing broadcast traffic
<a href="#">El Kamel, Eltaief &amp; Youssef, 2022</a>	*	*	✓	*	*	Attack mitigation in SDN using Deep Neural Network-based rate limiting
<a href="#">Lee, Kang &amp; Cho, 2017</a>	✓	*	*	✓	*	Design and implementation for Data Protection of Energy IoT utilizing OTP in a Wireless Mesh Network
<a href="#">Babkin &amp; Epishkina, 2018</a>	*	*	*	✓	*	One-Time Passwords: Resistance to Masquerade Attack
<a href="#">Kemshall, 2011</a>	*	*	*	*	✓	Two-factor authentication makes sense in mobile
<a href="#">Sadri &amp; Asaar, 2021</a>	✓	*	*	*	✓	Two-factor authentication protocol for IoT-based applications

In the literature, only a few works use SDN, 2FA, and OTP in the authentication for IoT. Table 1 presents various studies, including a summary of their contributions. Some work is done on securing authentication of IoTs in the cloud with authentication principles like OTP or 2FA, which does not lead to secure and satisfactory results. In this section, we present three works. The first work ([Hammi et al., 2020](#)) aims to advance the literature on IoT authentication by proposing three authentication schemes that satisfy the needs of IoT systems in terms of security and performance. One-Time Password (OTP) is a type of authentication that could be beneficial in Internet of Things and smart city applications. To ensure the security of such a protocol, this research effort extends the OTP principle and provides a novel way to produce OTP based on Elliptic Curve Cryptography and Isogeny.

The second work ([Baseri, Hafid & Cherkaoui, 2018](#)) is a method based on the Attribute-Based Encryption (ABE) technique, for designing secure and efficient data access control for mobile cloud. These methods allow data owners (enterprises or individuals) to ensure data security and provide mobile users with fine-grained access to data using defined policies and constraints.

The third work ([Hammi, Bellot & Serhrouchni, 2018](#)) is an approach that uses the asynchronous mode, which is based on the challenge/response method defined by RFC 1994 ([Simpson, 1996](#)). We chose this mode because it does not require any prior agreement between the communicating objects, in contrast to the synchronous mode, which requires an agreement between objects on some parameters, such as “time”, (for example, the Time-

based One-Time Password (TOTP) algorithm ([M'Raihi et al., 2011](#)) or a “counter” (for example, the HMAC-based One-Time Password (HOTP) ([M'Raihi et al., 2005](#))).

There is no SDN-based research work for securing IoT authentication to date, as Table 1 shows. For this reason, our idea is to set up a framework for securing IoT authentication dynamically based on SDN and the two authentication principles OTP and 2FA.

## Proposed Solution

The proposed solution concentrates on controlling the access to the devices or objects that are connecting in an IoT network based on SDN. In this section, we first highlight the objectives of the proposed framework, its overall architecture, its four main layers, and its overall operation. Finally, we explain the IoT authentication scenario as well as the role of each component and how it will react in case of an attack or otherwise.

## Objectives of the Framework

The objectives of our framework are grouped into three main points as follows:

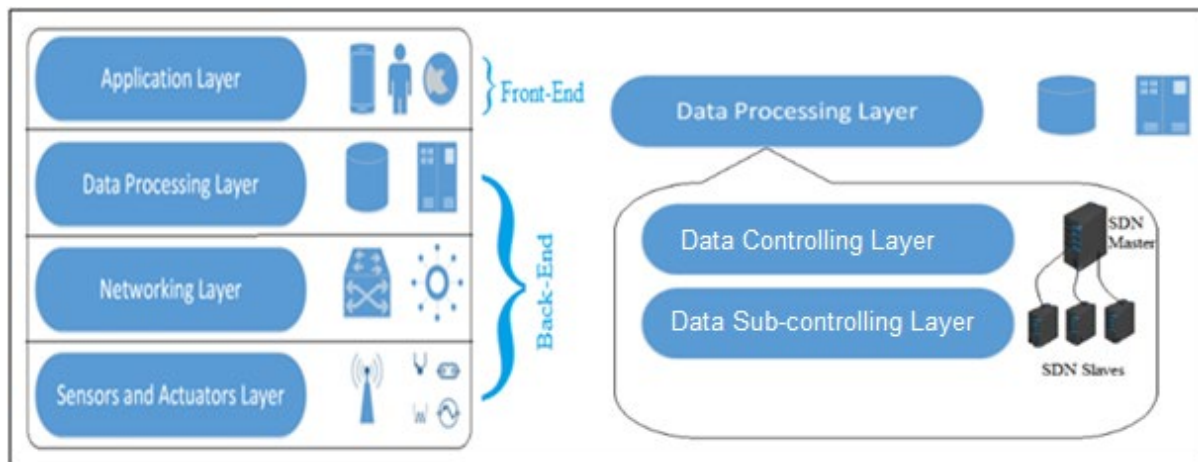
- Intrusion detection and identity usurpation in a virtual environment using IDS (Intrusion Detection System) Checker and IDS Analyser to collect malicious data, and generation of new signatures from malicious data.
- Internet of Things (IoT) access control and authentication devices, which can recognize and connect many real and virtual sensors dynamically into a unified secure system.
- Dynamic deployment of updates between clusters in an IoT cloud, using SDN master and slave.

## Proposed Model of IoT Architecture Based on SDN

As shown in Figure 1, we define an IoT architecture based on SDN with front-end and back-end. The front-end is connected to both an external network as well as the internal network. It is represented in Figure 1 by the application layer.

IoT users are able to communicate with the Cloud via the front-end. The back-end consists of computer hardware and software that are designed for the delivery of services. It allows treatment of the user's query and executes it allowing access to sensors and actuators. It is represented in Figure 1 by the Data Processing Layer, Networking Layer and Physical Layer (sensors and actuators layer).

**Application Layer:** It is the application layer that defines all applications in which IoT has been deployed. It is the interface between the end IoT devices and the network. Examples of IoT Applications are smart homes, smart health, and smart cities.



**Figure 1. IoT architecture based on SDN with a front-end and back-end**

The Application Layer has the authority to provide services to the applications. The services may be different for each application based on the information collected by the sensors. It is implemented at the device level by a specific application. The browser, for example, applies the application layer to a machine. It is the browser that executes application-layer protocols like HTTP, HTTPS, SMTP, and FTP. The application layer has numerous issues, the most important of which is security.

**Data Processing Layer:** In a three-layer system, data is transmitted directly to the networking layer. The likelihood of experiencing damage arises as a result of delivering data directly. In a four-layer architecture, data from a perception layer is transferred to this layer. The Data Processing Layer has two responsibilities: it verifies that data is forwarded by legitimate users and it protects the data from being tampered with.

Authentication is the most commonly used method to verify the users and the data. It is applied by using pre-shared keys and passwords for the concerned user. The second responsibility of the layer is to send information to the network layer. The medium through which data is transferred from the Data Processing Layer to the network layer can be both wireless and wire-based.

**Data Controlling Layer:** The SDN Controller serves as a bridge between the application and back-end layers. The northbound interface is the connection between the controller and applications, while the East/West interface is the connection between the controller and the data sub-controlling layer. This layer processes the instructions and requirements sent by the application layer (via northbound interface) and passes them to the networking



components (via southbound interface). It also communicates back necessary information extracted from the networking devices to the application to function optimally.

Data sub-controlling Layer: also called the “control plane”, is mainly composed of one or more SDN controllers. Its role is to control and manage the infrastructure equipment through an interface called ‘southbound API’.

Network Layer: A transmission layer is another name for this layer. It functions as a bridge, carrying and transmitting data collected from physical things via sensors. The transmission medium can be wireless or wired. It also allows network devices and networks to communicate with one another. As a result, it is particularly vulnerable to attacks. It has important security issues regarding the integrity and authentication of data that is being transmitted to the network.

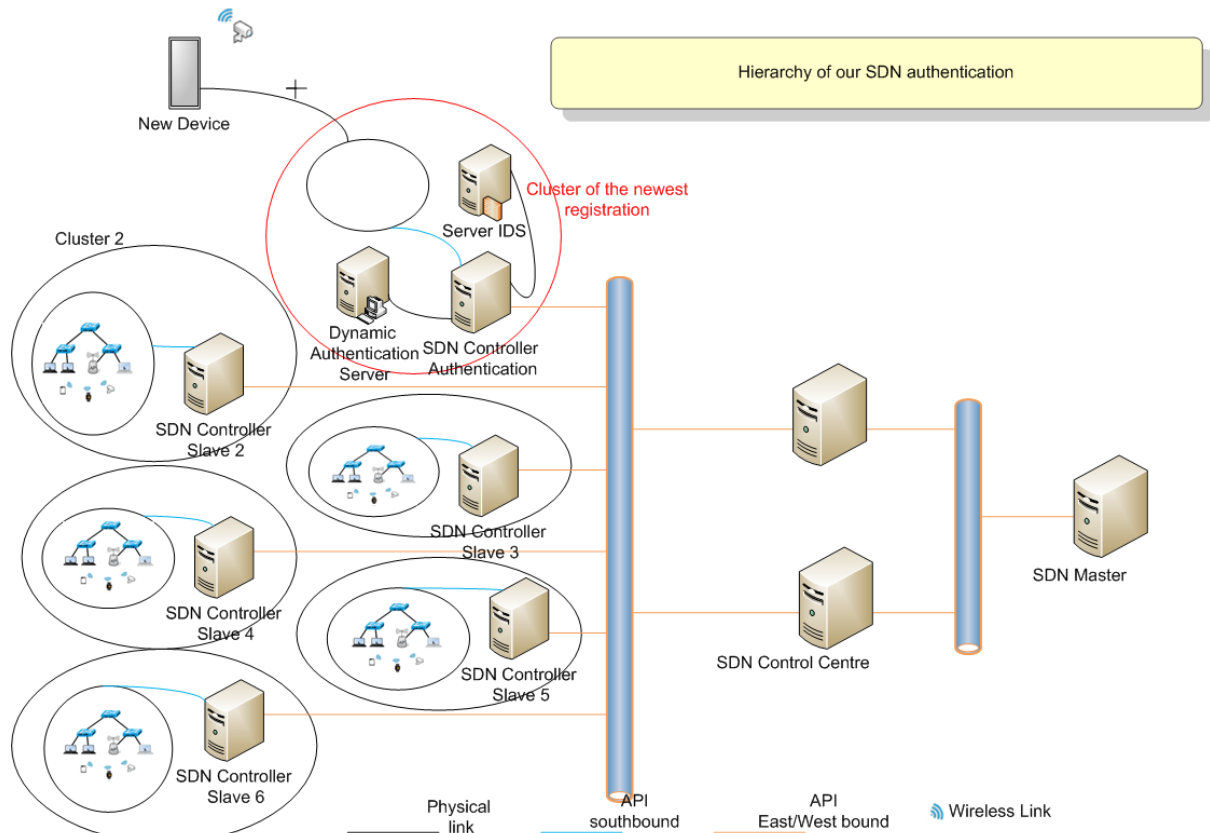
Perception layer/Sensor layer: The sensor layer is in charge of recognizing objects and collecting data from them. RFID, sensors and 2-D barcodes are just a few of the sorts of sensors that can be used to gather data from items. The sensors are selected as per the requirement of applications. The data that is collected by these sensors can be about location, changes in the air, environment etc. They are, however, mostly of interest to attackers who seek to use them to replace the sensor with their own.

## Building a Solution Framework

After the presentation of the IoT architecture-based SDN, we now proceed to the establishment or distribution of the components of our framework according to our strategy for authentication security. Then, we shed light on the general architecture of our framework, shown in Figure 2.

In traditional networks, authentication security is mainly provided by firewalls to protect against attacks. With the advent of connected objects, these techniques are not enough to protect against attacks that are increasingly sophisticated and cover even larger perimeters with mobility. This is why we propose a new approach based on an intelligent and dynamic concept, using the functionalities of an SDN controller, the services of an IDS and an authentication server based on the 2FA mechanism, which we will call a Cluster of registration. This concept is a decentralized middleware to implement management and security policies for network devices via an SDN controller, IDS and a Dynamic Authentication Server (DAS). All network devices are located in a domain called a cluster. A cluster of the newest registrations is a main cluster where each new object must pass through to register in the IoT network in a direct or indirect way; i.e., if a new object tries to integrate

with an already active cluster, it will be automatically redirected to the registration cluster, which makes our approach dynamic.



**Figure 2. General architecture of framework**

Before registering or deregistering a node in a cluster, one must consider these registration rules:

- We need to enable the object on the registering SDN so that the registering SDN communicates its authentication table to all Slave SDNs up to the master SDN.
- A node cannot be registered in a cluster if it is already a member of another cluster. In this situation, the node must first be unregistered from its current cluster.
- Node registration is done directly and dynamically through the local management interface of the appliance we want to join to the cluster. The appliance we are registering must be able to communicate with the registering SDN.
- Deregistration of a node must occur on the primary master.
- A node cannot be deregistered if it is not registered on the entire SDN chain.

**SDN Controller Authentication:** consists of a physical machine running OpenFlow switches, an OpenDayLight controller, control elements of the distributed network. In order to ensure high programmability of control plane and a global view of the newest things in the network, it is decoupled from the data routing devices and centralized. This means that decision making is concentrated in a single (or redundant) location, the controller. Data

routing is based on flow rules defined by controller instructions. The controller's decisions can be made based on a much wider range of criteria as well as on pre-programmed rules.

**Dynamic Authentication Server (DAS):** is an SDN Controller authentication client that implements the 2FA (Two Factor Authentication) algorithm based on OTP (One time Password). The DAS has been adapted to indicate whether the object is accepted or refused for authentication.

**Server IDS:** used to detect attacks against the registration cluster at an early stage and on the IoT network generally. It is the unit that reacts first in our approach whose purpose is to monitor and analyze all network activities, to detect unusual traffic and to notify the SDN Controller Authentication in such a case. This allows the latter to react to network access attempts by intruders and thus prevent an attack.

**Other clusters:** is a cluster of authenticated objects in the IoT network containing objects, nodes, network devices and mainly the OpenFlow Switch, communicating with the SDN.

**SDN Controller Slaves:** used to set the flow tables of the data plane switch (based on the OpenFlow protocol); such a feature set enables centralized and intelligent control and inspection of data packets that may be transmitted or received by any SDN switch connected to the network.

**SDN Control Centre:** complement of the SDN architecture, which aims at communicating the OpenFlow tables within the network and also the load balancing between SDNs, as well as a backup in case one of the slaves fails.

**SDN Master:** the major element of the architecture that has all the controls and authentication data, synchronizes with the Slave SDNs, and distributes the load in the SDN Controller centre.

## Analyzing the Functioning of the Framework

We discuss how our framework works based on Figure 3.

Every time a new object wants to access an IoT network, it confronts our authentication concept based on the SDN and the authentication server adopting 2FA, as well as the IDS server.

The object sends a request for affiliation to the network; this request is redirected directly and dynamically to the registration cluster; the SDN Controller Authentication receives it and processes it, while ensuring the validity of the request. SDN Controller Authentication consults the data in its temporary log file to see if this object refers to a previous affiliation request: in the legitimate case, nothing is reported, so the event must be passed to the IDS

server (based on Radius) so that it undergoes a thorough analysis to decide if the event is an attack or a straightforward authentication request. If it is an attack, the SDN Controller Authentication rejects the request; otherwise, the IDS server sends an authentication request to the DAS. The DAS comes to its process (that we will see later in detail) of authentication based on 2FA: if the two parameters are validated, a new affiliation is generated with the SDN. The SDN Controller Authentication communicates its authentication table to the SDN Control Centre, then to the SDN Master, so that the latter propagates this affiliation on all the SlaveSDNs. This is called an authentication network update. The SDN Controller Authentication updates its log file for a new affiliation attempt temporarily (logging principle).

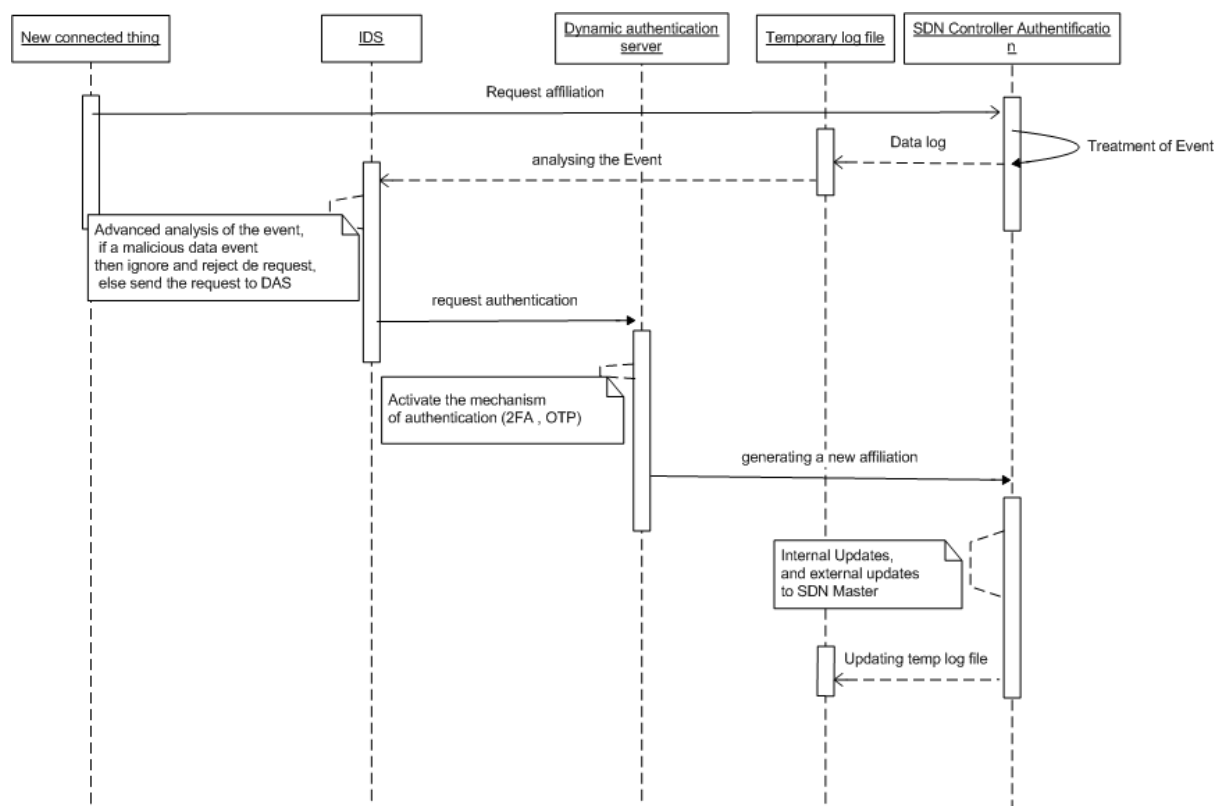


Figure 3. Framework's general sequence diagram

### IDS Process

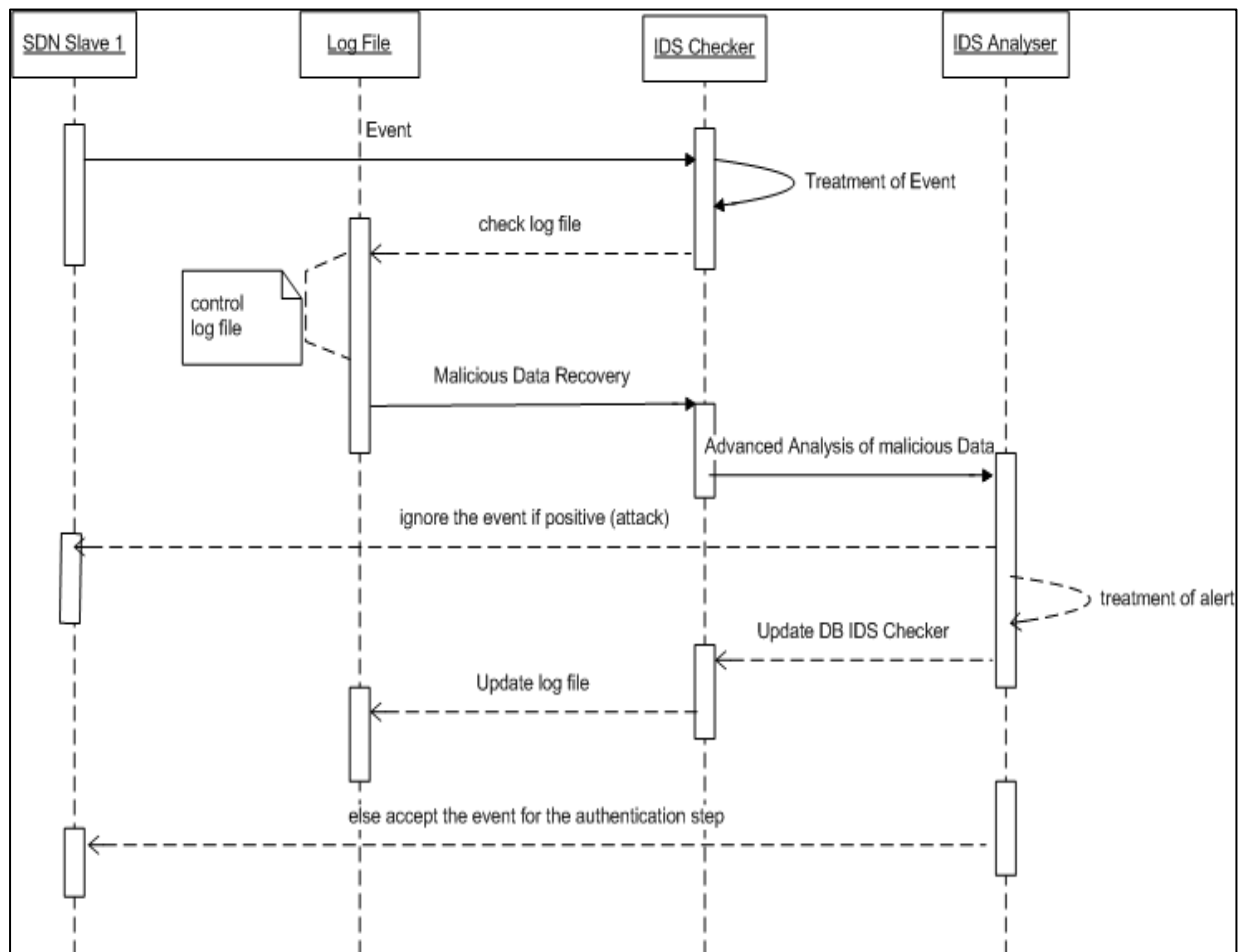
In this section, we detail the exchange part of the SDN Controller Authentication and the IDS server. From the previous global sequence diagram, we can see that, when a new object arrives, the SDN receives its affiliation request. This request is obviously to be analyzed. So, the SDN Controller Authentication gives it to the IDS server to be analyzed and to pass the IDS process.

In our approach, specifically in the detection and analysis of events from new objects, our IDS server is subdivided into two virtual machines (VM). To assure a new degree of trust in the VMs, we use Virtual Machine Monitoring (VMM) in our framework. The IDS-Checker

components are then deployed at the node (physical server) level to monitor virtual machines.

**IDS Checker:** it is in the form of a program analyzing a predefined attack database; this VM is self-powered according to its successor IDS analyzer.

**IDS Analyzer:** a VM implementing an intrusion detection and analysis system, such as RADIUS.

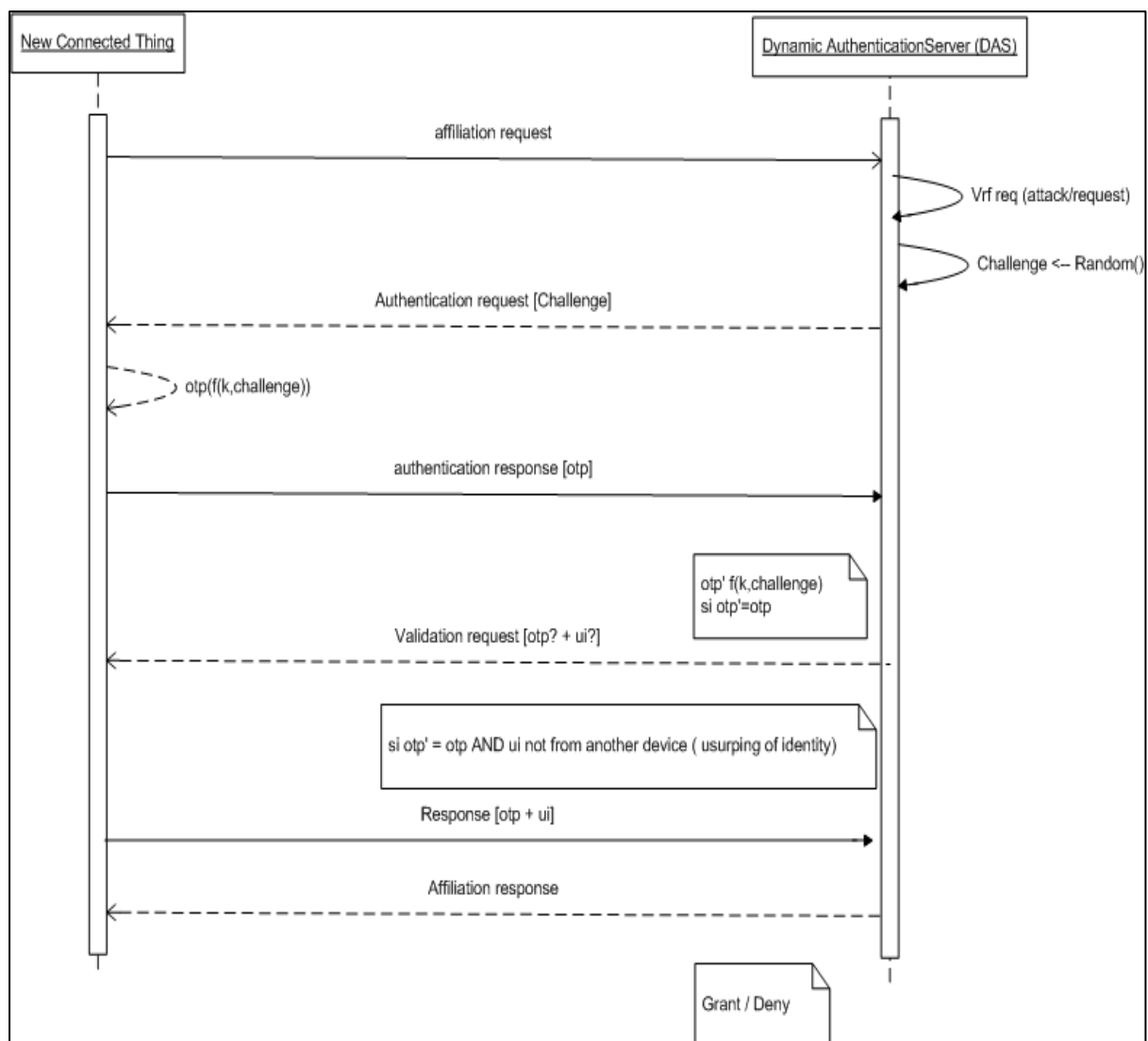


**Figure 4. Sequence diagram between SDN Slave and IDS**

As shown in Figure 5, the analysis process of the IDS server starts with SDN that sends the event to the IDS Checker, which processes this event and at the same time checks the IDS log file containing the access log of the objects. The log file returns a summary of the attempts of the objects that have launched attacks. Based on the summary and the processing of the IDS Checker, the IDS Analyzer receives the whole thing to decide if it is an attack or not. If it is an attack already predefined in the database, the IDS Analyzer ignores the event, sets an alert, and updates the IDS Checker and the log file. In the opposite case, that is, the event is a real affiliation request, the IDS Checker informs the SDN with an authentication acceptance.

## Dynamic Authentication Server

When designing our approach, we first studied an initial version that ensures the authentication of a device during the association phase. The authentication mechanism used is based on the principle of 2FA, which takes two parameters into account to ensure authentication. The first parameter is the One Time Password (OTP), defined in RFC 2289 and RFC 4226, as well as the challenge/response principle described by RFC1994. Indeed, an OTP is a password that is valid only during a single authentication operation, which is why it represents a very resistant authentication mechanism against replay attacks and cryptanalysis attacks. One-time passwords can be used in synchronous or asynchronous mode.



**Figure 5. Sequence diagram between new thing and DAS**

The synchronous mode is based on a shared secret (e.g., symmetric key) between two objects to prove the identity of one or both communicating entities and a pre-shared parameter, such as time or a counter, that changes in a synchronized way after each authentication

operation. As for the asynchronous mode, it is based on a shared secret and a random number called a challenge sent by the authenticator. We used the asynchronous mode because, unlike the synchronous mode, it does not require any prior approval between the communicating entities (e.g., a counter). And because of the instability of most wireless networks, if a message is lost then this will cause a synchronization problem as the counter values become different. Moreover, many wireless technologies do not support absolute time.

To remedy the problem of identity usurpation not taken into account in asynchronous mode, our authentication protocol adds the exchange of two more messages, which are “authentication request” and “authentication response”. Therefore, in order for a device to associate securely, it first sends an association request to the DAS. The latter responds with an authentication request containing a challenge. Then, via a cryptographic function described by RFC 4226, which we have adapted for the asynchronous mode, the device computes an OTP using a shared secret key and the received challenge. Then, it derives and stores a session key,  $k_u$ , that will be used to secure the session data exchanged in unicast mode. After that, it sends the OTP via an authentication response. Finally, upon receiving the message, the DAS calculates another OTP based on the same parameters and functions used by the device, and then compares the two OTPs. If they are identical, this proves the identity of the device. Thus, the authentication of the device is successful and its association is confirmed by a response association. After the authentication of the device, a symmetrical session key, identical to the one stored in the device is generated at the DAS level in order to ensure the integrity of messages in unicast mode.

Sharing the master key, used for object authentication and session key generation, is a challenge for security protocol designers. For a secure protocol, this key must be unique and personalized for each device. This personalization must not negatively influence the network performance and the proper functioning of the DAS. Therefore, we have created a key management mechanism called “Customization” of keys. The latter represents a secure, flexible and optimal method of distributing pre-shared keys that protects objects against internal spoofing attacks. Indeed, the principle of this mechanism is based on the fact of installing an initial key,  $k_i$ , at the DAS level and deriving from it a personalized key,  $k_d$ , for each device. The key  $k_d$  is calculated from  $k_i$  and the unique identifier (UI) of the device using a hash function (HMACSHA256). The latter represents a one-way function that prevents the input parameters (e.g., secret key) from being obtained from the result depending on the data provided; it generates a wide range of results. This customization offers many advantages:



- The DAS does not need to store the  $k_d$  key of each device belonging to its network, but rather to deduce it automatically thanks to its  $k_i$  key and the UI of the device requesting the association.
- When a new device with a  $k_d$  is added, the DAS does not need to be updated. This allows a great transparency and flexibility when adding new devices.
- Unlike some approaches that propose authentication based on a broadcast key, the fact that each device has its own key, which is linked to its identity, protects the system against internal identity theft.

Finally, once the association ends, a secure channel is created between the communicating entities. This channel ensures the integrity of the data by signing all messages with the messages using the key  $k_u$ . The signature represents the first  $n$  octets of the HMACSHA256 of the frame to be sent. Due to the limitation of the frame payload size in IoT networks, it is preferable that  $n$  does not exceed 16 bytes. This way, if a message is modified or tampered with, the system can automatically detect the problem.

## Discussion

The IoT is an Internet-based computing technology, in which the necessary resources are provided on a rental basis to clients. Therefore, the existence of vulnerabilities in the IoT allows intruders to affect the confidentiality, availability and integrity of IoT network resources as well as services. Authentication intrusions, identity theft, and other malicious activity at the network level are major security issues in the IoT. To ensure a high level of access control in the IoT network, we propose a new framework based on the cooperation of SDN and 2FA and OTP mechanisms. This framework allowed us to achieve three objectives: intrusion detection (known and derived from known attacks) at the front-end and back-end of the IoT environment autonomously; dynamic deployment of updates between clusters in an IoT network, using SDN communication APIs; a dual parameter secure authentication, the first based on the OTP algorithm and the second based on a challenge calculation. We used the OpenFlow protocol to exchange updates between clusters to obtain new knowledge and detect new devices. Exceptional scalability is another strong point of this framework. When, for example, our object migrates from a Cluster1 to Cluster2, it is still possible to make exchanges in the network because our SDN Master can migrate any SDN slave table to another SDN slave. The strength also lies in our framework, which gives IDSs scalability and flexibility. Therefore, we have met almost all the challenges mentioned in our framework. Therefore, this framework has several advantages; for this reason, it can be considered as an effective solution for object authentication in an IoT network. Thus, it can be used to protect people and assets from the risks of intrusion and aggression.

## Conclusions and Future Work

The IoT is enjoying undeniable success, which could be compromised by concerns about the risks associated with potential misuse of this model to conduct illegal activities. There is a major need to bring security, transparency and reliability into the IoT model for customer satisfaction. Therefore, one of the security issues is how to reduce the impact of any type of intrusion in this environment and mainly in the authentication process. Thus, in this paper, we propose a dynamic framework, which is based on the collaboration of IoT, SDN, IDS, 2FA, and OTP. As mentioned earlier, SDN controllers are used in our framework to examine devices, to transfer object data, and to update exchanges between different clusters in the IoT network; thus, SDN controllers could have the ability to examine objects and provide communication between hierarchical layers or clusters. Therefore, the Dynamic Authentication Server (DAS) is present to ensure secure authentication while relying on the 2FA mechanism, a two-parameter authentication where the first parameter is derived from the computation of an OTP and the second parameter is based on the computation of a challenge launched by the DAS. However, there are also the IDSs, which allow an analysis and detection of attacks at each affiliation of an object – that is, the analysis of an event and also the detection of an identity theft. Therefore, further development of mobile agent toolkits will facilitate their application in IDS systems. Finally, a dynamic deployment of a strong authentication mechanism and generation of updates between clusters in an IoT network, using SDN architecture, will also be of significant value. Further research can be undertaken to improve the presented work. Future directions are:

- Continuing to further develop the concepts and notions of this architecture and then proceed with an implementation to validate it.
- Taking into account minimizing the affiliation time between DAS and the object.
- The use of cooperation mechanisms between other authentication algorithms in order to reinforce the access control.
- Automatic improvement of the attack database at the IDS level.

## References

- Abdellatif, A. A., Mhaisen, N., Mohamed, A., Erbad, A., Guizani, M., Dawy, Z., & Nasreddine, W. (2022). Communication-efficient hierarchical federated learning for IoT heterogeneous systems with imbalanced data. *Future Generation Computer Systems*, 128, 406–419. <https://doi.org/10.1016/j.future.2021.10.016>
- Alizadeh, M., Tadayon, M. H., & Jolfaei, A. (2021). Secure ticket-based authentication method for IoT applications. *Digital Communications and Networks*. [online]. <https://doi.org/10.1016/j.dcan.2021.11.003>

- Babkin, S., & Epishkina, A. (2018). One-Time Passwords: Resistance to Masquerade Attack. *Procedia Computer Science*, 145, 199–203. <https://doi.org/10.1016/j.procs.2018.11.040>
- Baseri, Y., Hafid, A., & Cherkaoui, S. (2018). Privacy preserving fine-grained location-based access control for mobile cloud. *Computers & Security*, 73, 249–265. <https://doi.org/10.1016/j.cose.2017.10.014>
- Biggs, J. (2016). Hackers release source code for a powerful DDoS app called Mirai. *Tech Crunch*, October 11, 2016. Retrieved from <https://techcrunch.com/2016/10/10/hackers-release-source-code-for-a-powerful-ddos-app-called-mirai/#:~:text=Hackers%20release%20source%20code%20for%20a%20powerful%20DDoS%20app%20called%20Mirai,-John%20Biggs%40johnbiggs&text=After%20doing%20heavy%20damage%20to,the%20source%20code%20on%20Github.>
- Botta, A., DeDonato, W., Persico, V., & Pescapé, A. (2014). On the integration of cloud computing and internet of things. Future internet of things and cloud (FiCloud), International Conference on, IEEE. <https://doi.org/10.1109/FiCloud.2014.14>
- El Kamel, A., Eltaief, H., & Youssef, H. (2022). On-the-fly (D)DoS attack mitigation in SDN using Deep Neural Network-based rate limiting. *Computer Communications*, 182, 153–169. <https://doi.org/10.1016/j.comcom.2021.11.003>
- Hammi, M. T., Bellot, P., & Serhrouchni, A. (2018). BCTrust: A decentralized authentication blockchain-based mechanism. *IEEE Wireless Communications and Networking Conference (WCNC)*. <https://doi.org/10.1109/WCNC.2018.8376948>
- Hammi, B., Fayad, A., Khatoun, R., Zeadally, S., & Begriche, Y. (2020). A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT). *IEEE Systems Journal*, 14(3), 3440–3450. <https://doi.org/10.1109/JSYST.2020.2970167>
- Hussain, A., & Chun, J. (2022). Cloud service scrutinization and selection framework (C3SF): A novel unified approach to cloud service selection with consensus. *Information Sciences*, 586, 155–175. <https://doi.org/10.1016/j.ins.2021.11.024>
- Junior, N. F., Silva, A. A. A., Guelfi, A. E., & Kofuji, S. T. (2021). Privacy-preserving cloud-connected IoT data using context-aware and end-to-end secure messages. *Procedia Computer Science*, 191, 25–32. <https://doi.org/10.1016/j.procs.2021.07.007>
- Kemshall, A. (2011). Why mobile two-factor authentication makes sense. *Network Security*, 2011, 9–12. [https://doi.org/10.1016/S1353-4858\(11\)70038-1](https://doi.org/10.1016/S1353-4858(11)70038-1)
- Kocher, P. C. (1996). Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz, N. (ed.) *Advances in Cryptology — CRYPTO '96*. CRYPTO 1996. Lecture Notes in Computer Science, 1109, 104–113. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/3-540-68697-5\\_9](https://doi.org/10.1007/3-540-68697-5_9)
- Koohang, A., Sargent, C. S., Nord, J. H., & Paliszkievicz, J. (2022). Internet of Things (IoT): From awareness to continued use. *International Journal of Information Management*, 62, 102442. <https://doi.org/10.1016/j.ijinfomgt.2021.102442>
- Lagane, C. (2017). BrickerBot, un destructeur d'objets connectés qui agit... pour la bonne cause. *Silicon (France)*, April 21, 2017. Retrieved from <https://www.silicon.fr/brickerbot-destructeur-objets-connectes-bonne-cause-172891.html>

- Lee, S., Kang, B., & Cho, K. (2017). Design and Implementation for Data Protection of Energy IoT utilizing OTP in the Wireless Mesh Network. *Energy Procedia*, 141, 540–544. <https://doi.org/10.1016/j.egypro.2017.11.116>
- Mitake, Y., Tsutsui, Y., Alfarihi, S., Sholihah, M., & Shimomura, Y. (2021). A life cycle cost analysis method accelerating IoT implementation in SMEs. *Procedia CIRP*, 104, 1424–1429. <https://doi.org/10.1016/j.procir.2021.11.240>
- M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). HOTP: An HMAC-Based One-Time Password Algorithm. *IETF, RFC 4226*. <https://www.ietf.org/rfc/rfc4226.txt>
- M'Raihi, D., Machani, S., Pei, M., & Rydell, J. (2011). TOTP: Time-Based One-Time Password Algorithm. *IETF, RFC 6238*. <https://doi.org/10.17487/rfc6238>
- Munther, M. N., Hashim, F., Abdul Latiff, N. A., Alezabi, K. A., & Liew, J. T. (2021). Scalable and secure SDN based ethernet architecture by suppressing broadcast traffic. *Egyptian Informatics Journal*, 23(1), 113–126. <https://doi.org/10.1016/j.eij.2021.08.001>
- Mutlag, A. A., Abd Ghani, M. K., Arunkumar, N., Mohammed, M. A., & Mohd, O. (2019). Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, 90, 62–78. <https://doi.org/10.1016/j.future.2018.07.049>
- Nait-Hamoud, O., Kenaza, T., & Challal, Y. (2021). Certificateless Public Key Systems Aggregation: An enabling technique for 5G multi-domain security management and delegation. *Computer Networks*, 199, 108443. <https://doi.org/10.1016/j.comnet.2021.108443>
- Sadri, M. J., & Asaar, M. R. (2021). An anonymous two-factor authentication protocol for IoT-based applications. *Computer Networks*, 199, 108460. <https://doi.org/10.1016/j.comnet.2021.108460>
- Shan, L., Zhou, H., & Hong, D. (2021). Application of access control model for confidential data. *Procedia Computer Science*, 192, 3865–3874. <https://doi.org/10.1016/j.procs.2021.09.161>
- Simpson, W. A. (1996). PPP challenge handshake authentication protocol (CHAP). RFC 1994. <https://www.rfc-editor.org/rfc/rfc1994.html>
- Stergiou, C., Psannis, K. E., Kim, B.-G., & Gupta, B. (2018). Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems*, 78, 964–975. <https://doi.org/10.1016/j.future.2016.11.031>
- Sturm, R., Pollard, C., & Craig, J. (2017). *Application Performance Management (APM) in the Digital Enterprise*, Appendix C - The NIST Definition of Cloud Computing, 267–269. Morgan Kaufmann, Boston.
- Tok, M. S., & Demirci, M. (2021). Security analysis of SDN controller-based DHCP services and attack mitigation with DHCPguard. *Computers & Security*, 109, 102394. <https://doi.org/10.1016/j.cose.2021.102394>

Zhang, R., & Hu, Z. (2021). Access control method of network security authentication information based on fuzzy reasoning algorithm. *Measurement*, 185, 110103. <https://doi.org/10.1016/j.measurement.2021.110103>

# A History of Reshaping Australian Telecommunications

## A Review of John Doyle's *Crossed Lines: Disruption, Politics and Reshaping Australian Telecommunications*

---

Judith Brett  
La Trobe University

---

**Abstract:** A review of John Doyle's, *Crossed Lines: Disruption, Politics and Reshaping Australian Telecommunications*, published by Australian Scholarly Publishing, 2022.

**Keywords:** Telecommunications, Policy, History, Australia, Book Review

## Disruption and Politics in the Reshaping of Australian Telecommunications

When the Postmaster-General's Department (PMG) was formed after Federation out of the six colonial postal and telegraph departments, it was a colossus, dwarfing every other Australian enterprise, public or private. From the beginning it had dual objectives. It had to provide essential communication services to all Australians at an affordable price; and it had to operate like a business. In a huge country like Australia, much of it sparsely populated, these objectives could not but conflict and the result was an opaque and complex system of cross subsidy in which the city subsidised the bush, business households, and telecommunications postal services. The system had largely bi-partisan support, and were anyone to raise questions the Country Party would quickly spring to the defence of a system that benefitted people living outside the metropolitan centres.

During the 1960s, the PMG came under great strain, from technological change and from increased demand, including from business, for new services such as data transmission. Its appetite for capital was vast, but its capacity to make a return on the investment was

constrained by inflexible funding arrangements and the political difficulty of increasing charges for its services. The Coalition, by then in its second decade of government, had little interest in fundamental reform of the PMG, so it was left to the Whitlam Labor government. Whitlam's interest in modernising government administration coincided with a push from the Amalgamated Postal Workers' Union (APWU) to get PMG workers out from under the control of the Public Service Board and into a statutory corporation. So began the end of the long-standing co-dependence of telecommunications and postal services.

John Doyle's new book ([Doyle, 2022](#)), *Crossed Lines: Disruption Politics and Reshaping Australian Telecommunications*, tells the story of the politics of this reform process up to and including the 1991 reforms of the Hawke government which brought full-service competition into the sector. It is based on thorough archival research, the extent of which is truly impressive as this was a time of dramatic change in Australian telecommunications. Doyle also interviewed key political players, including Kim Beazley, Gareth Evans, Tony Staley, Malcolm Fraser, Paul Keating and Ian Sinclair. The book comes with a swag of endorsements including from George Megalogenis, who describes it as 'the definitive history of telecommunications reform in Australia'; and Richard Alston, who praises it for its rigour and balance. The focus is on the politics, not on the engineering or the technical challenges, but it will interest readers of this journal, many of whom will have lived through the policy shifts it describes.

Lionel Bowen was Labor's Postmaster-General, whom Whitlam charged with reforming the behemoth, and he instituted an inquiry under James Vernon. This set the pattern as the various stakeholders made their submissions: the unions and various staff associations, rural interests, including various rural shires and the Country Party, the PMG itself, and many members of the public. Notably uninvolved, notes Doyle, were the Liberal Party and the general business sector. Vernon recommended the creation of two entities and in 1975 Telecom and Australia Post were formed as separate statutory authorities.

If the aim of Labor's reforms was to create a new, stable organisational structure for the delivery of Australia's telecommunications services, it didn't work. Telecom lasted barely two decades. The Fraser government, which came to office after the dismissal at the end of 1975, had given little thought to telecommunications policy, but as the pressures on the system continued it had no choice but to take it on. New business-oriented equipment and data services were creating a level of demand Telecom was not set up to meet and the Coalition was caught between the demands of the Liberal's core business constituency and that of the Country Party's rural base. The one big thing the Fraser government did, when Tony Staley was minister, was to establish Aussat, a state-owned company to develop and operate a national satellite system. It did not, however, act on the recommendations of the Davidson



Enquiry, which it had instigated, and so lost the opportunity to begin the telecommunications reform process.

The reform process did not really get underway again until around 1987 when the Hawke government, alarmed at Australia's deteriorating terms of trade, embarked on a host of microeconomic reforms to increase the international competitiveness of the Australian economy. Gareth Evans, the minister at this time, stresses that Labor's approach was pragmatic and nonideological. As minister he argued that consideration be given to winding back some of Telecom's traditional monopoly areas and creating space for the private sector to meet the increasing range and diversity of users' needs. In the background of the debate in the late 1980s and early 1990s was the spectre of privatisation. This was not Evans' intent for telecommunications. Rather, it was to corporatise Telecom and embed principles of competition into the sector. Nevertheless, he received a good deal of pushback, from the unions and from Telecom itself in particular, as well as from sections of caucus committed to the public provision of essential services. Evans was Minister for Transport and Communications for just fifteen months, after which he became Foreign Minister and it is for this latter role that he is largely remembered. Doyle shows us how important his focus and energy were in creating momentum for reform.

Reform, though, was cautious and incremental, dependent on caucus support and union acquiescence. One impediment to faster progress was uncertainty as to the cost of Telecom's universal service obligation. When he became minister, Ralph Willis, who was an economist, commissioned a study which showed that this was much lower than the sums Telecom habitually claimed. This, says Doyle, was a true breakthrough because it provided evidence that introducing competition into the sector to stimulate innovation was compatible with providing affordable community services, and so removed the core political risk in dismantling Telecom's monopoly.

Doyle says that, from the late 1980s, the shift to full competition was probably inevitable, but that the timing and the model were uncertain. The model introduced by Kim Beazley in 1990 was built on strengthening Telecom to compete with a privatised Aussat. Optus bid successfully for Aussat, and in 1993 a third mobile provider, Vodafone, entered the market. The Opposition generally supported the government's legislation, so long as it was moving in the direction of greater openness, flexibility and competition. Doyle ends his story there, but the stage was now set for the privatisation of telecommunications provision under the Coalition, though it had to spend big on rural Australia to allay fears about the weakening of the universal service obligation.

The book concludes with a brief look forward to the politics of the National Broadband Network (NBN), which awaits the sort of detailed investigation Doyle has given to earlier periods. He concludes that 'Continuous disruption, whether technological or political, is the only real certainty in telecommunications reform' (p. 210). I would put this slightly differently. Politics is not the main driver here. The continuous disruption is driven by relentless technological innovation to which politics has little choice but to respond as some stakeholders try to protect their interests and others to take advantage of new opportunities.

Telecommunications policy is a complicated and technical area. Doyle's is the first book to look in depth at the policy changes set in train when Whitlam put reform of the PMG on the national policy agenda. Doyle writes well, without jargon, in straightforward, clear prose and the book has a comprehensive index. His book will be of great interest to those whose working lives were affected by these changes, as well as to others interested in the always challenging process of policy reform.

## References

Doyle, J. (2022). *Crossed Lines: Disruption, Politics and Reshaping Australian Telecommunications*. Australian Scholarly Publishing, Melbourne. \$49.95.

## David Piltz is Awarded the 2022 Charles Todd Medal

---

Peter Gerrand

TelSoc Life Member

David Piltz

TelSoc Member

---

**Abstract:** On 21 October 2022, David Piltz was awarded TelSoc's Charles Todd Medal for 2022, at TelSoc's annual Charles Todd Oration in Sydney. This article provides Dr Peter Gerrand's speech in presenting the medal on behalf of the TelSoc Board, and David Piltz's speech in reply.

**Keywords:** Charles Todd Medal, Australian telecommunications history, TelSoc.

### Presentation of the Charles Todd Medal

On 21 October 2022, as part of TelSoc's 2022 Charles Todd Oration event in Sydney, David Piltz was awarded this year's Charles Todd Medal for his outstanding contribution to celebrating Australia's telecommunications history, through protecting and celebrating its valuable historical assets. This article includes the short speech made by Dr Peter Gerrand, in awarding the medal on behalf of the TelSoc Board; it is followed by David Piltz's response.

### Award Speech by Dr Peter Gerrand

The Charles Todd Medal has been awarded regularly since 1992 to individuals who have made the most outstanding contribution to Australian telecommunications in recent years.

Because 2022 is the sesquicentenary of the completion of the Overland Telegraph Line, the TelSoc Board decided it would be appropriate this year to award the Medal to the individual who has made the most outstanding contribution to celebrating the industry's history. There has been no major work by an historian on Australian telecommunications as a whole since Ann Moyal's masterpiece, *Clear across Australia*, published in 1984 ([Moyal, 1984](#)). So, we turned to those who have played a vital role in protecting and celebrating our industry's valuable historical assets.

Before 1990, there were several telecommunications museums in Australia, housed in telephone exchange buildings of Telecom Australia and OTC, with the support of local

management, and staffed part-time by unpaid volunteers. With the creation of Telstra, these museum assets, together with many other heritage items not yet forming part of the museums, became the property of Telstra. As Telstra became progressively privatised in the 1990s and 2000s, and at times became headed by CEOs with little personal interest in the industry's history, many became concerned at the fate of the valuable historical archives and heritage equipment. We would hear how some of the original museums had been closed down, and much of the archives and valuable historical equipment had simply been bundled up and sent off to warehouses.

But, throughout this period, there would be whispers that a Telstra engineering executive named David Piltz was acting as a guardian angel, co-ordinating the efforts of many volunteers in keeping the Melbourne, Sydney and Brisbane telecommunications museums in operation, and protecting as much as he could of the remaining national heritage assets, whether already warehoused or still kept in Telstra buildings across the nation.

In 2018, we learned to our great pleasure that Telstra had created a not-for-profit charitable subsidiary, Heritage Telecommunications Ltd, with David as its foundation Chairman, and had transferred all of its heritage assets plus considerable funding to this subsidiary. Not only would there be money to upgrade the remaining museums, the Melbourne museum would become the National Communications Museum and be professionally staffed. Even better, the vast bulk of the heritage assets would be catalogued and stored in a high-quality, temperature- and humidity-controlled warehouse, purpose built for the organisation in Dandenong.

David Piltz retired from Telstra in June this year after 49 years' service as a telecommunications engineer, and as a member of Telstra's executive team since 1990. His responsibilities have included the planning, design, construction and maintenance of its national network, through several generations of technology change.

In 2006, he was appointed chairman of a voluntary and informal group within Telstra, which took over the management of Telstra's historical collection from Telstra's Corporate Affairs group. By 2018, with the support of CEOs David Thodey and particularly Andy Penn, David was instrumental in the creation of Heritage Telecommunications Ltd as a not-for-profit subsidiary of Telstra, with the charter of managing Telstra's heritage collection as a stand-alone organization with charitable status. As its foundation Chairman, David continued in the job until his retirement from Telstra four months ago.

I think you have heard enough to realize that David Piltz thoroughly deserves the award of TelSoc's Charles Todd Medal in 2022, for his outstanding contributions to Australian telecommunications in celebrating our industry's history and protecting as much as possible of its heritage assets.

## Response by David Piltz



David Piltz in October 2022

Thank you, Peter.

The Charles Todd medal is a very prestigious award. I am extremely pleased to be the 2022 recipient with the focus on acknowledging the dual aspects of my career in telecommunications. I sincerely thank the TelSoc Board for their consideration that I might be a worthy recipient. When announced, I was both overwhelmed and humbled, as it puts me in illustrious company. I recently looked up the recipients' list from previous years — quite a Who's Who.

## Aspects of my nearly 50 years in Australian telecommunications

I started in 1973 with the PMG in Adelaide as a Cadet Engineer and graduated with a BE (Hons) degree from Adelaide University. My career with Telecom Australia, starting in 1975, had me working in District Works (Adelaide North), then with Transmission Construction Country SA (in the Murray Bridge and Mt Gambier District), and then with Darwin and NT (Regional Planning) in the Outer Darwin Semi-Rural Area.

I then transferred to National Office in Melbourne, where I worked in Transmission Planning on Interexchange Fibre Networks, ISDN, Inter-Capital Planning, National Fibre Network, and Data Networks Bandwidth expansion.

In the National Office, I then worked with the Access Planning and Technology division on the following: Broadband for Consumers and Business, ADSL1, ADSL2+, VDSL, and HFC DOCSIS1. My next job was with Technology Selection and Development, variously for Voice, Data, Video, Mobile services, Connectivity, Broadband, Fibre, copper cables, HFC, Satellite services, PCM, ATM, IP, Internet and Cyber Security.

The rate of change of technologies has had the most significant impact on my engineering career in telecommunications. But it has also been influenced by changes in government policy, company restructures, company policies and, of course, people and personalities in leadership positions.

## Driving the preservation of the heritage of Australian telecommunications

My involvement in protecting the industry's heritage began with a suggestion by some work colleagues in 2006, to which I readily responded. It required a commitment of time and thought on how to take the then Telstra heritage collection, which was about to be dispersed and to be no more, to a sustainable, solid, business-based solution that preserved the collection and its valuable knowledge. We took the view that 'Telstra's Heritage = Australia's Heritage'.

For twelve years we worked within Telstra, beyond our day jobs, as the unofficial 'Heritage Telstra Board'. We eventually persuaded Telstra's senior management to create a wholly owned subsidiary, Heritage Telecommunications Ltd (HTL), as a registered charity. I served as Board Chairman of HTL for four years until my retirement from Telstra in June 2022, after 49 years and 95 days with the PMG, Telecom Australia and Telstra.

Taking this road could not have been possible without some very close collaboration with some equally passionate people. Two individuals in particular should be acknowledged and thanked: Paul Kinchington as Policy and Strategy advisor, and Stefan Nowak as the 'man on the ground' Collections Officer and keeper of the heritage collection knowledge.

Our network included experts both within Telstra (from Legal, Finance, Corporate Affairs and Operations) and outside Telstra in volunteer organisations that had kept our national telecommunication history and heritage alive in Queensland, NSW and Victoria primarily; but also with links into South Australia, Western Australia and internationally via the OTC Veterans Association.

I have previously presented to TelSoc members, in 2021, the details of this sixteen-year journey. So now I will only touch on three significant moments that led to the creation of Heritage Telecommunications Ltd:

1. In 2006, a crucial meeting with Corporate Affairs, the then 'owner and manager' of Telstra's heritage collection. This was a meeting that changed their direction: instead of dispersing the collection, it was decided to hold it together. The start of the new direction began.
2. In 2014, the collection was evaluated by an independent external firm, who reported that Telstra had a collection of "National Significance" and recommended two actions: (a) to preserve and look after the collection; and (b) to bring it to life.
3. In 2018, the completion of the CEO Approval Paper, creating the Heritage Telecommunications Limited (HTL) as a subsidiary with charitable status, and the

Deed of Gift. This was the culmination of a year-long term intensive effort to convince senior Telstra Executives (the CFO, COO, Legal, Corporate Affairs, and CEO) of the virtues of having a sustainable approach to managing and displaying the Heritage collection. They rose brilliantly to the challenge.

## Outcomes

Since its inception in 2018, Heritage Telecommunications Ltd (HTL) has funded:

- A new, modern National Storage Facility (NSF) in Dandenong South, Victoria that houses the collection in museum standard conditions of temperature and humidity control.
- The creation of the National Communications Museum (NCM) that is under construction at 375 Burwood Rd, Hawthorn, Victoria.
- The volunteer-run Museum at Bankstown, NSW.
- The volunteer-run Museum at Albion, Queensland.

Overall, the HTL entity is adequately funded and resourced, enabling the heritage collection to be consolidated and brought to life in a sustainable way.

Finally, I wish to thank the TelSoc Board for awarding me the Charles Todd Medal for 2022.

## Reference

Moyal, A. M. (1984). *Clear across Australia: A history of telecommunications*. Nelson, Melbourne.



# Marconi Wireless Telegraphy Trialled in Australia

---

Simon Moorhead

Ericsson Australia and New Zealand

---

**Abstract:** A historic paper from 2010, republished here, describes a demonstration of wireless transmission between Victoria and Tasmania by the Marconi Wireless Telegraph Company in 1906. The subsequent debate and delays in adopting the new wireless communication system highlight the influence of imperial politics on Australian telecommunications, post Federation. The impasse with Marconi over his initial refusal to license his patent was eventually resolved by the creation of Amalgamated Wireless Holdings (AWA) in 1911.

**Keywords:** History, Telecommunications, Marconi, Politics

## Introduction

Guglielmo Marconi and several contemporaries are generally recognised as the inventors of wireless telegraphy early in the twentieth century. Marconi was awarded several key patents for his discoveries and shared the Nobel prize for physics in 1909 with Karl Ferdinand Braun for their “contributions to the development of wireless telegraphy” ([Smith-Rose, 2022](#)).

The historic paper below ([Given, 2010](#)) describes a demonstration of wireless transmission between Point Lonsdale, near Queenscliff in Victoria, and Devonport in Tasmania, by the Marconi Wireless Telegraph Company in 1906. Australia had recently federated, and the young parliament was meeting in Melbourne to debate important industrial legislation. The parliament deferred the debate and took a special train to see the demonstration, because Marconi’s invention had become internationally recognised by that time.

Marconi was represented locally by Captain Louis Walker. Walker, who would be paid 5% commission on any business contracted (but had very little success), arranged the installation of radio equipment including mast antennas at Point Lonsdale and Devonport. The local municipalities also took the opportunity to impress the politicians with various meetings, speeches and toasts.

The demonstration was successful because, by 1906, Marconi had perfected his equipment such that he could easily achieve transmissions over water for distances up to 500 km. Unfortunately for Walker, the parliament could not decide what to do with the new technology

and, after six months of lobbying, hit a policy roadblock. Walker was forced to mothball the equipment and return to the United Kingdom.

In the minutes of the proceedings of the Colonial Conference 1907 ([Colonial Conference, 1907](#), p. 607), it is obvious the British Government was encouraging the “Colonies” to choose wireless telegraphy systems that interworked with each other and not to adopt the Marconi system. Marconi wished to maintain his monopoly and refused to interwork with other systems. The British Government believed this monopoly would be eroded as time went on and history shows they were correct.

In 1910, Australia built two high powered wireless land stations in Sydney and Fremantle, covering the east and west maritime approaches to the mainland. They were not Marconi systems and Marconi naturally commenced legal action against the Commonwealth. The action was resolved by the merger of Australasian Wireless, the Marconi Company, and Telefunken to form Amalgamated Wireless (Australasia) Ltd (AWA) in 1911 ([Moyal, 1984](#), p. 112).

In July 1906, Walker provided a souvenir brochure ([Marconi, 1906](#)) of the Marconi demonstration between Point Lonsdale and Devonport – but, curiously, it concentrated on examples of maritime incidents where the Marconi system assisted in the rescue, rather than describing the equipment used in Australia.

## References

- Colonial Conference. (1907). Minutes of Proceedings of the Colonial Conference, 1907. Section A-05, Appendix to the Journals of the House of Representatives of in New Zealand, 1907. Available at <https://atojs.natlib.govt.nz/cgi-bin/atojs?a=d&d=AJHR1907-L1.698&cl=&srpos=0&e=-----10--1-----0-->
- Given, J. (2010). Wireless Politics: Marconi and the Parliament at Point Lonsdale, 12 July 1906. *Telecommunications Journal of Australia*, 60(4), 60.1–60.7.
- Marconi. (1906). Marconi’s Wireless Telegraph Coy., Ltd. Souvenir of Queenscliff and Devonport Demonstration. July 1906. Available at <https://viewer.slv.vic.gov.au/?entity=IE2651290&mode=browse>
- Moyal, A. M. (1984). *Clear across Australia: A History of Telecommunications*. Melbourne: Thomas Nelson.
- Smith-Rose, R. L. (2022). Guglielmo Marconi. *Encyclopedia Britannica*. Available at <https://www.britannica.com/biography/Guglielmo-Marconi>

## The Historic Paper

### ○ WIRELESS POLITICS

#### MARCONI AND THE PARLIAMENT AT POINT LONSDALE, 12 JULY 1906

Jock Given

*Swinburne University of Technology, Institute for Social Research*

On 12 July 1906, representatives of Marconi's Wireless Telegraph Company staged a demonstration of the new medium of wireless telegraphy across Bass Strait, between Point Lonsdale in Victoria and Devonport in Tasmania. A special train was organised from Melbourne for the Governor-General, the Prime Minister, most of the cabinet and members of the young Australian Parliament, who deferred debate that day on important industrial legislation. The event and its aftermath provided a striking illustration of the relationship between politics and communications. Political enthusiasm for the idea of new communications technology ran well ahead of the capacity to make lasting decisions about how it should be deployed.

A little over a hundred years ago, the Australian Parliament took a train from Melbourne to Queenscliff. They were there to see some magic.

It was 1906, a decade after a 22-year-old Italian had been granted a patent for 'wireless telegraphy'. (Baker 1970, 28) Experimenting at his family's home in Bologna, Guglielmo Marconi had worked out how to transmit Morse Code signals across short distances without wires. People had been doing this with wires for half a century. Much of the world was traversed by overhead, underground and submarine telegraph cables. But doing it without wires was magic.

When Marconi claimed to have transmitted a signal across the Atlantic in December 1901, many refused to believe him. They thought nature may have played tricks with his equipment, or bravado with the interpretation of his results. Although 'Mr Marconi has gradually accustomed us to the wonders of wireless telegraphy', wrote *The Times*, the achievement was still 'in some degree a shock to all preconceived notions'.<sup>1</sup> But the man who a few years later shared the Nobel Prize in Physics with the German wireless innovator Karl Ferdinand Braun was not deceived.<sup>2</sup> He had done it first, then tried to work out how. Human understanding of the transmission of electromagnetic energy over long distances had some catching up to do.

By 1906, when the Commonwealth Parliament took a train down the Bellarine Peninsula, the Italian was a global celebrity. Though his London-based company had still not turned a profit, it had a global network of subsidiaries and affiliates and some prestigious customers – the Royal Navy, Lloyd's and Cunard. Marconi was not going to be in Queenscliff himself, but if his system of wireless magic was coming to town, everyone wanted to be there. In his place came a representative, Captain Louis Walker, and two technical assistants. Signing himself 'Agent in Australasia for Marconi's Wireless Telegraph Company Limited', Walker spent a year and a half in Australia and New Zealand trying to sell three things: the idea of wireless, the Marconi wireless system, and shares in Marconi's Wireless Telegraph Company. He was to be paid a 5% commission on any business contracted.<sup>3</sup> The immediate priorities were the international passenger steamers and point-to-point communication between the Australian mainland, New Zealand and Tasmania.<sup>4</sup> Walker had very little success.

The timing seemed good. Walker arrived in Australia soon after the first *Wireless Telegraphy Act* was passed by the Commonwealth Parliament in 1905. The Canadian Parliament also passed a *Wireless Telegraphy Act* that year, as had New Zealand in 1903 and Britain in 1904. (Baker

1970, 110; Wilson 1994, 92) Under pressure from the Colonial Office, the governments of the empire responded in unison to the new technology. They asserted public control of the airwaves, but left open the possibility of licensed use of them by private operators.

The Australian Parliament's legislation was the second major use of its constitutional power over 'postal, telegraphic, telephonic and other like services'. (see LaNauze 2001) The first, the *Post and Telegraph Act 1901*, consolidated the separate state post, telegraph and telephone administrations into a single national monopoly responsible to the Postmaster-General.<sup>5</sup> Some had argued a monopoly would ensure the new organisation did not resist new technologies that threatened existing investments. This might have occurred if the telephone had not been controlled by the same colonial agencies that ran the telegraphs. (Moyal 1984, 88–90) The *Wireless Telegraphy Act* appended Marconi's medium to this Commonwealth colossus. A state monopoly of the ether was argued to be 'purely a formal measure',<sup>6</sup> although there was some confusion about whether or not the Commonwealth was also taking over privately-held wireless patents. Attorney-General Isaacs explained this was not the case. The intention was 'not to appropriate the invention, but to control it'.<sup>7</sup>

A demonstration of wireless communication across Bass Strait seemed a politically savvy pitch to the politicians of the young Australian federation. The distance, around 200 miles, was comfortably within the capacity of Marconi's technology by then. Just fifteen months after the Australian demonstration, in October 1907, the company would open a commercial wireless telegraph service across the Atlantic, using stations in Clifden, Ireland and Glace Bay, Canada. (Baker 1970, 123–128) But it was far from the first telegraphic communication across Bass Strait. Tasmania was first connected to the mainland by submarine cable in 1859, although the cable failed and a permanent link was not re-established until a decade later. (Adams 1992, 3–4; Atkinson 2001) Nor was it the first wireless demonstration in the area. A Post Office engineer established a station near the Black Lighthouse at Fort Queenscliff in 1901, exchanging messages with a ship escorting the Royal Yacht as it arrived in Port Phillip Bay, bringing the Duke and Duchess of Cornwall and York to open the first Australian Parliament. (site visit 5 Jan 2006)

Permission for a demonstration across Bass Strait between Point Lonsdale in Victoria and Devonport in Tasmania was granted, and Walker's two technical assistants established communication over the route in May 1906.<sup>8</sup> (Walker and one of his engineers on the trip, H.M. Dowsett, later published many editions of a wireless manual.<sup>9</sup>) 12 July was supposed to be a sitting day for the House of Representatives, which met in Melbourne at the time. But three-quarters of the members and all but two of the Cabinet told Prime Minister Alfred Deakin they were accepting Captain Walker's invitation to attend the demonstration. So much for the new Australian parliamentary democracy. Politicians prefer a new communications infrastructure project any day.

The House adjourned for most of the day, though not without dissent. The federal member for Corangamite, the electorate adjoining Corio where the demonstration was held, complained the invitation was 'merely to attend a picnic'. There had already been 'a great many picnics' in the five-year life of the national Parliament, he said. And this one was 'a picnic to support a monopoly'—the Marconi system, which the company was trying to make the sole world wireless standard. 'Worse than that,' he said, 'it is a foreign monopoly.'<sup>10</sup>



What the member for Corangamite thought particularly offensive was that, to make way for the Marconi picnic, the Parliament had to adjourn debate on the Australian Industries Preservation Bill. This 'Anti-Combine Bill' was based on the United States Sherman anti-trust legislation passed in 1890, which outlawed restrictive trade practices. It was a decisive shift away from the English Common Law, which supported freedom of contract, even where the consequences of particular contracts were trade restrictive. Though eventually passed by the Australian Parliament, the legislation was interpreted so narrowly by the High Court in a case a few years later that Australia was left without effective trade practices law until the 1970s. (Walker 1967, 24–36)

So debate on the Australian Industries Preservation Bill was set aside and a specially-organised train took the politicians from Melbourne to Queenscliff station.<sup>11</sup> The Governor-General, the Prime Minister, the Governor of Victoria and the sender of Australia's first telegraph message between Melbourne and Williamstown 52 years before were the stars of a large and luminous cast. They were greeted by 200 schoolchildren who sang the national anthem, a small price to pay for the half-day holiday they were granted.<sup>12</sup> Cobb and Co coaches took the party past the flags, strung between the Post Office and the Grand Hotel, to The Springs, just before Point Lonsdale.<sup>13</sup> There, *The Age* thought there was 'little for the eye to see—nothing of ostentatious display', just two masts 162 feet high. Wires strung across the 70 yards between them provided the aerial, which was connected by cable to equipment housed in three buildings.<sup>14</sup>

The 200–300 guests were treated to a luncheon and speeches. Prime Minister Deakin joked that, since the Anti-Combine Bill had not yet passed, he had entered a conspiracy with the Victorian Attorney-General to replace the toast to the Parliament with one to the success of Marconi's Wireless Telegraph Company. If Tennyson had not been able to foresee the scientific development the crowd had assembled to witness, the Australian poet Brunton Stephens 'had gone very near to it', when he spoke of Australia as 'she whose ear thrills to the finer atmosphere'. Wireless telegraphy 'seemed likely to transform future economic, political and warlike proceedings all over the globe'.<sup>15</sup>

Contemplating future uses of the technology, the Victorian Attorney-General favoured what he called pocket Marconi installations. These devices, he imagined, could be used to transmit photographs to the wives of politicians, letting them know where their husbands were. Prime Minister Deakin thought federal members would have nothing to fear from such mobile applications, though he was less confident about the members of the Victorian Parliament. Governor-General Northcote worried that wireless may make it harder for him to travel beyond the control of the Prime Minister.<sup>16</sup>

As the cigars arrived, the exchange of official messages between the Point Lonsdale and Devonport stations began. Deakin sent a message to the People of Tasmania: 'Australia tirelessly pursuing her great distances by rail and wire, to-day enlists the waves of the ether in perfecting the union between her people in Tasmania and upon the mainland.' Senator Keating also emphasised the federal theme: 'We narrow the straits as we call across them.' Postmaster-General Chapman – the Stephen Conroy of the day – sent a message on behalf of the mainland press to the press of Tasmania: 'No limits can be set to the beneficent influence of journalism now that the atmosphere has, at the bidding of genius, become its servant.' (Marconi's 1906) Chapman had visited wireless stations overseas, including in Italy. He thought people who asked 'Will this pay?' needed 'to look at the matter from something more than the commercial aspect'.<sup>17</sup>

The Tasmanian Governor did not miss his moment, reciprocating the mainland's greetings on behalf of the 'small and beautiful sister, by whom Victoria was founded'. He hoped the wireless experiment 'may accelerate the date at which this state's contribution towards cable subsidies can be diminished'. (Marconi's 1906) The Blame Game would be over soon. Across Bass Strait in Devonport, things were less rosy. There was a crowd of 2000, but it did not include ministers in the Tasmanian Government. They were stuck in the Parliament in Hobart facing a no confidence motion.<sup>18</sup> It took forty minutes to get a reply from the Governor of Tasmania there, because of a bit of a backhaul problem. The wireless messages in Devonport had to be written down and sent by bicycle and ferry to the nearby Post Office, where they were relayed by cable to Hobart.<sup>19</sup>

The Tasmanian proposer of the toast to the Federal and State Parliaments didn't miss his moment either, using it to complain about the impact of federation. Defences had not improved; there had been no consolidation of State debts; and the nation had implemented a tariff that pleased nobody. This Tasmanian was particularly fed up with minority federal governments: he 'did not want wobblers at the present juncture'. The Master Warden of the Mersey Marine Board proposed 'Prosperity to Devonport'.<sup>20</sup>

A sheaf of correspondence was sent to Captain Walker by men looking for jobs with Marconi's new medium. Many already had experience in telegraphy at the Post Office or the submarine cable companies in Australia and overseas. Some had worked in the very new art of wireless telegraphy, as ship's wireless operators or with the Royal Navy. An electricity lecturer from the Launceston Technical School wanted to be Marconi's agent. He had 'from the first taken a keen interest in the development of wireless Telegraphy as far as it has been possible on this side of the globe', but stressed he had no interest in the German Telefunken system, Marconi's main global rival, whose equipment he had borrowed for a demonstration. Another, from St James, on the railway line between Benalla and Yarrawonga, wanted to call in and 'see how the latest wonder works'. St James was just a small country town, but it was, he said, the home of Jas Carruthers, the Inventor of 'Carruthers Electrical Clock'. This was 'a great thing nearly as great as Marconi's invention, but they won't put it on the market I don't know why'. A strict teetotaler from the Victorian Railways Audit Office, with nearly four years experience as a warden in the Yarra Bend Asylum, said he was 'quick at picking up anything in electricity or machinery'.<sup>21</sup>

Captain Walker helped to sell the idea of wireless, but failed to sell either the Marconi system or shares in Marconi's companies. The Government agreed to place £10,000 on the estimates for a chain of coastal wireless stations, although it had no clear plan for how to spend it. (Curnow 1963, 54) Poulsen's arc wireless system was attracting a lot of publicity as a rival to Marconi's spark system—'These people are all full of this man's invention and talk of nothing else', an exasperated Walker told his boss in London—and the Australian Government insisted there must be an open tender for any wireless stations it decided to establish.<sup>22</sup> The idea of conceding the whole field of wireless to Marconi forever, or even for the duration of his patents, was troubling to governments and commercial rivals alike. As to the chances of selling Marconi shares in Australia, Walker said 'although there are a large number of rich men, they would prefer to invest their money in things they understand, and they would regard this as rather too speculative'.<sup>23</sup>

Six months after his demonstration, it was clear that Australian communications policy had hit a roadblock. No decisions would be made about wireless in Australasia before the Colonial



Conference in London the following year. It might be useful for Walker to be there himself when the Australasian leaders he had lobbied arrived. He booked a passage home and, with his technical team, arranged for the storage of the demonstration equipment. Four years later, Marconi's new Australasian representative had to break in through the window to collect it.<sup>24</sup>

Walker told the Secretary to the Postmaster-General's Department he feared Australia's delays would 'not be considered by the Public here or the outside world as in keeping with the splendid progressive traditions of the Australian Colonies'.<sup>25</sup> He was frank about the failure of his trip, but he felt the year-and-a-half was not completely wasted. New Zealand Prime Minister Sir Joseph Ward, he said, gave him a verbal promise of a five years' contract with his government. Australian Prime Minister Deakin had told him 'most emphatically that we had distinctly the prior claim for consideration from the Government, and that I might depend upon it that this would be borne in mind by the Government when they came to determining the matter'. At the very least, he said 'if I have failed to obtain a contract by my presence and work here, I have certainly made it very difficult for anybody else to, and have succeeded in keeping others away'.<sup>26</sup>

Australia eventually got a national wireless network – an NWN – but not for another five years, once a Labor Government, led by a Queenslander – Andrew Fisher – was in office. The NWN was established by the government, not the private sector. The first wireless station was in Melbourne. It did not use Marconi's technology. (Amos 1936) The Italian magician responded in Australia as he did around the world,<sup>27</sup> by commencing legal action against the Commonwealth alleging infringement of his patents. Marconi's got a court order allowing it to enter the government stations to inspect the technology, but before the case could be decided, the government changed.<sup>28</sup> Joseph Cook's incoming Liberal administration made a large payment to Marconi's and the matter was settled. Then the government changed again. The Queenslander was back in charge, though not for long. Brought down from within his own party, Fisher resigned and headed off to an overseas post. (Day 2008, 347-52)

I could tell a long story about Australian telecommunications, but it may sound like a short story told many times.

## NOTE

*This is an expanded version of a talk given at the 75th anniversary dinner of the Telecommunications Journal of Australia in Melbourne on 2 August 2010. It draws on material held in The Marconi Archive at the Bodleian Library, University of Oxford and in the Mitchell Library in Sydney.*

*A cairn beside the sports field near Point Lonsdale now marks the spot where the Parliament went for the wireless demonstration. One of the original Morse Code transmissions across Bass Strait was re-enacted at a centenary celebration in 2006 attended by the Governor of Victoria, local politicians, residents and schoolchildren.*

## ENDNOTES

<sup>1</sup> Leader, *The Times*, 21 Dec 1901, p. 11.

<sup>2</sup> Nobel Prize. 2010. 'The Nobel Prize in Physics 1909'. Accessed 12 August 2010. Available from: [http://nobelprize.org/nobel\\_prizes/physics/laureates/1909/](http://nobelprize.org/nobel_prizes/physics/laureates/1909/)



- Marconi Marine Board Minutes, 10 April 1908: The Marconi Archive, Bodleian Library, University of Oxford.
- 'Memorandum for Captain Walker re Australian business', Sept 1905: HIS 109, The Marconi Archive.
- Commonwealth of Australia Constitution Act 1900*, s. 69.
- House of Representatives, *Debates*, 24 Aug 1905, p. 1386.
- House of Representatives, *Debates*, 13 Sept 1905, p. 2243.
- Dowsett to Walker, 'Report on the establishment of communication between Pt. Lonsdale, Victoria and East Devonport, Tasmania, 10 May 1906', 14 May 1906: HIS 109, The Marconi Archive.
- See for example Dowsett, Harry Melville; Walker, Louis Edward Quintrell. *Handbook of Technical Instruction for Wireless Telegraphists*: 1942/44. 7<sup>th</sup> edn. London: Iliffe; 1945. 8<sup>th</sup> edn. London: Iliffe; 1950. 9<sup>th</sup> edn. London: Iliffe for Wireless World.
- House of Representatives, *Debates*, 11 July 1906, pp. 1262-3.
- 'Wireless Telegraphy', *Geelong Advertiser*, 13 July 1906: 4.
- 'Wireless Telegraphy', *The Argus*, 13 July 1906: 4.
- 'Queenscliff Visited by Two Governors', *Queenscliff Sentinel*, 13 July 1906: 2.
- 'Wireless Telegraphy', *The Age*, 13 July 1906: 5.
- 'Wireless Telegraphy', *The Argus*, 13 July 1906: 4; 'Wireless Telegraphy', *The Age*, 13 July 1906: 5.
- 'Wireless Telegraphy', *The Argus*, 13 July 1906: 4; 'Wireless Telegraphy', *The Age*, 13 July 1906: 5.
- 'Wireless Telegraphy', *The Age*, 13 July 1906: 5.
- 'Wireless Telegraphy. Successfully Installed', *Launceston Examiner*, 13 July 1906: 6; 'Wireless Telegraphy. Between Victoria and Tasmania', *Hobart Mercury*, 13 July 1906: 5.
- 'Wireless Telegraphy', *The Age*, 13 July 1906: 5.
- 'Wireless Telegraphy. Successfully Installed'. *Launceston Examiner*. 13 July 1906: 6.
- Applications for employment with Marconi's Wireless Telegraph Company in Australia and New Zealand: HIS 109, The Marconi Archive.
- Walker to Cuthbert Hall, 6 Mar 1907: HIS 109, The Marconi Archive. Poulsen was granted two Australian patents for improvements in receivers in October and December 1905 (nos 4432 and 4814), and a patent for improvements in transmission in May 1906 (no 6034): Spruson to Australasian Wireless Ltd/Telefunken, 23 Aug 1911, 1 Dec 1911, 23 Jan 1912; Walsh to Australasian Wireless Ltd, 12 April 1911: Mitchell Library MSS 6275 Box 19 f. 10.
- Walker to Cuthbert Hall, 20 Feb 1907: HIS 109, The Marconi Archive.
- Fisk to MWT Co, 9 Jan 1912: Mitchell Library MSS 6275 Box 18 f. 5.
- Walker to Robert T. Scott, Secretary PMG's Department, 14 March 1907: HIS 109, The Marconi Archive.
- Walker to Cuthbert Hall, 6 Mar 1907: HIS 109; Marconi Marine Board Minutes, 25 June 1907: The Marconi Archive.
- Marconi and [MWT Co] v. British Radio-Telegraph and Telephone Company (Limited)* (1911) 27 TLR 274 (3 March 1911); Patent, Design and Trademark Cases. vol. XXVIII no. 10, p. 181 (26 April 1911); *The Times*, 22 Feb 1911, p. 24 [the 'Parker Judgment'].
- Marconi's Wireless Telegraph Company v The Commonwealth [No. 2]* (1913) 16 CLR 178. A stay of the order was later granted, pending appeal to the Privy Council: *MWTC v The Commonwealth [No. 3]* (1913) 16 CLR 384.

## REFERENCES

- Adams, K.C. 1992. *Telecommunications Technology in Tasmania: the First 100 Years*. Sandy Bay: K.C. Adams.
- Amos, D.J. 1936. *The Story of the Commonwealth Wireless Service*. Adelaide: E.J. McAlister & Co.
- Atkinson, I.R. 2001. 'Linking the Nation – the Victoria-Tasmania Submarine Telephone Cable 1936'. In *Eleventh National Conference on Engineering Heritage: Federation – Engineering a Nation; Proceedings*, edited by Baker, K. Barton, ACT: Institution of Engineers, Australia.
- Baker, W.J. 1970. *A History of the Marconi Company*. London: Methuen & Co.
- Curnow, Ross. 1963. 'The Origins of Australian Broadcasting, 1900–23'. In *Initiative and Organisation*, edited by Spann, R.N.; Mayer, Henry. Melbourne: F.W. Cheshire.
- Day, David. 2008. *Andrew Fisher: Prime Minister of Australia*. Sydney: Fourth Estate/HarperCollins.
- La Nauze, J.A. 2001. "'Other Like Services: Physics and the Australian Constitution'". In *No Ordinary Act: Essays on Federation and the Constitution by J.A. La Nauze*, edited by Irving, Helen; Macintyre, Stuart. Melbourne: Melbourne University Press.
- Marconi's Wireless Telegraph Company. 1906. *Souvenir of Queenscliff and Devonport Demonstration July 1906*. Melbourne: Marconi's Wireless Telegraph Company.
- Moyal, Ann. 1984. *Clear Across Australia: A History of Telecommunications*. Melbourne: Thomas Nelson.
- Walker, Geoffrey de Q. 1967. *Australian Monopoly Law: Issues of Law, Fact and Policy*. Melbourne: F.W. Cheshire.
- Wilson, A.C. 1994. *Wire and Wireless: A History of Telecommunications in New Zealand, 1860–1987*. Palmerston North: Dunmore Press.

Cite this article as: Given, Jock. 2010. 'Wireless politics: Marconi and the Parliament at Point Lonsdale, 12 July 1906'. *Telecommunications Journal of Australia*. 60 (4): pp. 60.1 to 60.7. DOI: 10.2104/tja10060.