Journal of Telecommunications and the Digital Economy

Volume 13, Number 3
September 2025

Published by
Telecommunications Association Inc.

ISSN 2203-1693

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

Journal of Telecommunications and the Digital Economy

Volume 13, Number 3
September 2025

Table of Contents

Editorial Team

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

Cybersecurity and Innovation in the Evolving Digital Economy

Michael de Percy
University of Canberra

Abstract: This editorial introduces the September 2025 issue of the *Journal of Telecommunications and the Digital Economy*, spotlighting the intersection of cybersecurity, emerging technologies, and historical lessons in the digital economy. As digital transformation accelerates, threats to IoT, cloud, and 5G ecosystems proliferate, demanding innovative, resource-efficient solutions for SMEs and emerging markets. Contributions in this issue – from machine learning-driven threat detection to zero-trust architectures and reflections on telecom automation – highlight human and organisational factors in resilience. They bridge legacy telecommunications with future-oriented strategies, underscoring the journal's commitment to fostering adaptive digital ecosystems amid persistent vulnerabilities.

Keywords: Editorial, Editor-in-Chief, Digital Economy, Cybersecurity, IoT Security.

Introduction

This editorial welcomes readers to the September 2025 issue of the *Journal of Telecommunications and the Digital Economy*, with a focus on cybersecurity's pivotal role in sustaining the digital economy. The post-COVID 'new normal' has entrenched online interactions as essential infrastructure, yet it has also amplified vulnerabilities in interconnected systems. From IoT-enabled healthcare to cloud-dependent SMEs, the digital economy thrives on innovation but grapples with escalating threats like ransomware, bandwidth exploitation, and supply-chain attacks. Decades-old technologies now underpin global commerce, but social and organisational norms lag, exposing gaps in preparedness.

The articles in this issue illuminate these tensions, offering practical insights into securing emerging technologies while drawing on historical precedents. They emphasise the human element – talent, awareness, and adaptive business models – as key to bridging challenges in resource-constrained environments. By integrating machine learning, zero-trust principles, and 5G reconfiguration, contributors reveal pathways for resilient digital growth, particularly in developing contexts.

http://doi.org/10.18080/jtde.v13n2.1356

Cybersecurity Imperatives in IoT and Cloud Ecosystems

A dominant theme is the fortification of IoT and cloud infrastructures against sophisticated threats. Anjikumar & Chakravarthy (2025) propose a lightweight encryption framework for remote healthcare, blending elliptic curve cryptography with grasshopper optimisation to slash latency and energy use. Simulation results affirm its efficacy in 5G-smart health setups, addressing privacy pitfalls in real-time data sharing.

This work underscores the digital economy's fragility: IoT's proliferation generates vast data streams, but without tailored, efficient defences, it risks amplifying breaches. As SMEs – 90% of global businesses – adopt these technologies, the emphasis on low-overhead tools like zero-trust architectures becomes imperative.

Reconfiguring Business Models and Organisational Resilience

Shifting to strategic adaptation, Banda & Feukeu (2025) employ qualitative case studies across Sub-Saharan Africa to unpack 5G's disruptive potential. Interviews reveal internal (e.g., infrastructure costs), external (e.g., regulatory hurdles), and hybrid factors reshaping value chains, urging operators to pivot toward fixed-wireless access and spectrum-sharing for GDP gains projected at US$10 billion by 2030. This analysis extends beyond developed markets, spotlighting emerging economies' leapfrogging opportunities amid debt and poverty constraints.

Echoing organisational dynamics, Moya *et al.* (2025) deploy PLS-SEM on 112 Colombian SME surveys, identifying human talent and resources as top predictors of resilience. With 33% of respondents hit by attacks like phishing, the study stresses cyber awareness and supplier vetting, filling gaps in emerging-market research and advocating integrated frameworks like NIST for proactive defence.

Dinh *et al.* (2025) validate a bespoke LZTA, outperforming baselines in throughput and response times under high loads. By fusing multi-factor authentication with role-based controls, it democratises zero-trust for budget-strapped SMEs, countering the 70% disruption rate from breaches and aligning with global calls for ‘never trust, always verify’ paradigms.

Navaratna & Saxena (2025) expose self-regulation gaps in AI chatbots, advocating for a standard compliance score on app stores and enhanced citizen digital awareness to bridge divides. The above issues are becoming increasingly commonplace and deserve our continued attention.

http://doi.org/10.18080/jtde.v13n3.1356

Historical Reflections and Enduring Lessons

This issue also honours telecommunications' legacy, reminding us that today's digital challenges echo yesterday's innovations. Moorhead (2025) considers seminal 1981–1982 papers on Telecom Australia's DAS/C rollout, juxtaposed with Ian Campbell's (2025) commentary revealing deployment delays and union frictions that yielded suboptimal efficiency versus U.S. benchmarks. These pieces, amid AI's rise, caution against repeating historical pitfalls in workforce transitions.

Complementing this, Leith Campbell's (2025) obituary for Dr. Clemens W. Pratt celebrates a 38-year PMG/Telstra career in teletraffic engineering, from theses on congestion to ITC advisory roles. Pratt's mentorship and statistical advocacy underscored the human intellect driving telecom evolution – timely as ML automates threat detection.

Conclusion

The digital economy's 'new normal' demands vigilance: cybersecurity is not merely technical but profoundly human and historical. This issue's contributions – from IoT safeguards to 5G pivots and archival wisdom – enrich our grasp of these dynamics, fostering collaboration across disciplines. As threats evolve, the *Journal of Telecommunications and the Digital Economy* remains a vital forum, bridging telecom's storied past with innovative futures to empower resilient, inclusive growth. We invite readers to engage with these insights and submit their own.

References

Anjikumar, T. & Chakravarthy, A. S. N. (2025). An Energy-Efficient Based Secure IOT Data Transfer with Hashed Data Access Policy Using ACROT-DHSKECC and LSCRC32. *Journal of Telecommunications and the Digital Economy*, *13*(3), 145–175. http://doi.org/10.18080/jtde.v13n3.1301

Banda, L. & Feukeu, E. A. (2025). The Impact of 5G on Business Models for Mobile Operators in Emerging Markets. *Journal of Telecommunications and the Digital Economy*, *13*(3), 71–105. http://doi.org/10.18080/jtde.v13n3.1230

Campbell, I. (2025). Comments on the Two Historical Reprints in Automation of Directory Assistance. *Journal of Telecommunications and the Digital Economy*, *13*(3), 191–195. http://doi.org/10.18080/jtde.v13n3.1340

Campbell, L. (2025). Clemens William ("Clem") Pratt, 2 July 1936–16 January 2025. *Journal of Telecommunications and the Digital Economy*, *13*(3), 196–204. http://doi.org/10.18080/jtde.v13n3.1322

Dinh, T. D., Le, T. D., Nguyen, T. T. H., & Do, H. G. (2025). A Lightweight Zero-Trust Architecture Implementation for Enhancing Cybersecurity in Small and Medium-

Sized Enterprises. *Journal of Telecommunications and the Digital Economy*, *13*(3), 106–144. http://doi.org/10.18080/jtde.v13n3.1284

Moorhead, S. (2025). Automation of Directory Assistance. *Journal of Telecommunications and the Digital Economy*, *13*(3), 176–190. http://doi.org/10.18080/jtde.v13n3.1330

Moya, L. P., Giraldo, M. C. B., Lozano, J. A. A., Arias, A. V., & Rodríguez-Correa, P. A. (2025). Human and organisational factors influencing the preparedness of small and medium-sized enterprises against cyber attacks in developing countries. *Journal of Telecommunications and the Digital Economy*, *13*(3), 30–70. http://doi.org/10.18080/jtde.v13n3.1197

Navaratna, A. R. & Saxena, D. (2025). Digital Governance Through Self-Regulation: A user-developer perspective of AI chatbots. *Journal of Telecommunications and the Digital Economy*, *13*(3), 1–29. http://doi.org/10.18080/jtde.v13n3.1077

Digital Governance Through Self-Regulation

A user-developer perspective of AI chatbots

Anand R Navaratna
School of Management and Entrepreneurship, Indian Institute of Technology, Jodhpur, Rajasthan

Deepak Saxena
School of Management and Entrepreneurship, Indian Institute of Technology, Jodhpur, Rajasthan

Abstract: User-centric development of digital applications must integrate user feedback, developer channels, and regulatory compliance, yet lacks a standardised framework. The rapid rise of AI exacerbates auditing and governance challenges, with self-regulation prevailing but requiring scrutiny of user and developer concerns. This paper analyses the top 10 AI chatbot apps on Google Play Store via a three-prong approach. First, sentiment analysis of 117,353 user reviews using two algorithms reveals sentiments on policy and governance. Second, evaluation of 15 preset developer compliance parameters shows self-declared adherence. Third, comparative results indicate only 69% compliance, despite these apps' high popularity and downloads. Users prioritise experience quality, while developers emphasise service quality. The study exposes self-regulation gaps in AI chatbots, advocating for a standard compliance score on app stores and enhanced citizen digital awareness to bridge divides.

Keywords: AI ChatBot, User-Centric Development, Digital Governance, QoS, QoE.

Introduction

Are AI applications developed the way users want them to be? Are users concerned about the developer's compliance declaration and expressing their concerns in their reviews? These aspects in bits and pieces are covered by various Structured Literature Reviews, Citizen-centric development, public governance and societal impact studies (Bastardo *et al.*, 2024; Henman, 2020; Javaid *et al.*, 2023; Saklani & Kala, 2024; Talanquer, 2023). Is there a gap between developers' agendas and users' sentiments? Are these applications compliant with existing governance frameworks – hard or soft? To ensure a better digital society, we need answers to these questions, promoting holistic assessment of the developer–user–compliance perspectives. This becomes relevant given the emergence of Large Language Models and AI Chatbots. Chatbots have evolved rapidly in numerous fields in recent years, including

http://doi.org/10.18080/jtde.v13n3.1077

marketing, supporting systems, education, health care, cultural heritage, and entertainment (Adamopoulou & Moussiades, 2020). Chatbots are an apt example of intelligent Human-Machine interaction (Bansal & Khan, 2018). Many text-based chatbots target specific functionalities, enabled by tools that let us build bots for many widely used messaging platforms (Dale, 2016).

One of the pre-AI era chatbots could be listed as Microsoft Office's Clippy. One of the most popular AI-based chatbots, which even had voice assistance, was Apple's Siri, an in-built feature associated with the product (Henman, 2020). Amazon Alexa took the revolution forward by making a dedicated personalised voice-assisted experience. An initial application of chatbots within citizen-driven applications was Alex, used by the Australian Tax Office (Henman, 2020). For research areas, the application of chatbots has been in medicine and para-medicine bring out ethical issues and propose an ethical framework for applying conversational AI in patients directly interacting with a chatbot for medical interventions instead of a face-to-face check-up. Towards prevention of suicide (800,000 per year) and their attempts (16,000,000 per year), around 9% of chatbot apps provide erroneous help line numbers, raising governance concerns (Martinengo *et al.*, 2019). Another field of application is customer service on online platforms explore the scenario of customer-chatbot interaction in retailing. They highlight an interesting dynamics of 'perceived governance' of chatbots compared to human involvement during service failures. During these failures, customers are found to be unforgiving of the application or brand. Henman (2020) emphasises the evolution of chatbots through qualitative work with an agenda to improve public service through AI. Fournier-Tombs & McHardy (2023) focus on medical applications and ethics, while Xing *et al.* (2022) explore chatbots in retailing in scenarios where they can fail. All these thoughts are applied to different fields of application, and they have brought out three broad issues surrounding the governance of chatbots. These issues relate to the objectives of the app developers, compliance with the standards set by the hosting platform and/or country, and customer response to these standards. While earlier works touch on these aspects in bits and pieces, there is a gap in a holistic study. This study bridges the gap by studying application compliance and complements it by studying user sentiments. Both aspects are novel concerning existing literature.

The remainder of the paper is as follows. In the next section, we undertake a comprehensive review of practice vis-à-vis policy compliance of AI chatbots. The remainder of the paper is as follows. The next section presents the literature review that underscores its importance and introduces the methods used to analyse customer reviews from a compliance perspective. This is followed by a detailed description of the research methodology adopted in this study. Findings of the study are presented in terms of the assessment of developers' claims and users'

http://doi.org/10.18080/jtde.v13n3.1077

perspectives. The discussion compares these perspectives as well as the findings from existing literature. The paper establishes the limited role of self-regulation in compliance and suggests that user inclination is more skewed towards quality of experience.

Literature Review

In emerging technologies, Artificial Intelligence (AI) could be listed as one of the most disruptive technologies (Chhetri *et al.*, 2023; Zheng *et al.*, 2018). It has emerged from the developing domain to the now evolving domain. In this regard, three major strands of literature are identified – AI adoption, user sentiment analysis, and AI policy, governance and regulation. Table 1 provides a summary of these strands.

Table 1: Literature review approach

Sl No	Crux Area/ Approach	Papers
01	Digital Technology and its adoption analysis, including AI	Hacker *et al.* (2023); Sukhpal *et al.* (2023); Bailao *et al.* (2022); Calo (2017); Navaratna & Saxena (2023); Stix (2021); Chatterjee (2020); Yang *et al.* (2019); Wang *et al.* (2019); Warner & Wäger (2018); Evans & Grefenstette (2018); Jobin *et al.* (2019); Van Berkel, *et al.* (2020).
02	User Sentiment and Google Play Store	Linares-Vásquez *et al.* (2013); Haque & Rubya (2023); De Freitas *et al.* (2024); Tan *et al.* (2022); Sharma *et al.* (2021); Yenkikar *et al.* (2022).
03	AI Policy, Governance and Regulation	Linkov *et al.* (2018); Burak (2020); Navaratna & Sakena (2023); OECD (2017); Katzenbach & Ulbricht (2019); Yeung & Bygrave (2021); Gutierrez & Marchant (2021); May (2007); Djeffala *et al.* (2022); Marwala (2024).

With the success of large language models like ChatGPT, the AI vertical gaining traction apart from the technological development is its policy, governance and regulatory aspects (Hacker *et al.*, 2023; Sukhpal *et al.*, 2023). While some studies focus on specific National AI Strategies (Bailao *et al.*, 2022), many others deal with the cluster, geography, economy or ethnicity (Calo, 2017; Navaratna & Saxena, 2023). There are also studies on the fundamentals of these policies like ethics (Stix, 2021), Global South and North framework (Chatterjee, 2020), data privacy (Yang *et al.*, 2019; Wang *et al.*, 2019) or any other adjacent fields like blockchain (Warner &

http://doi.org/10.18080/jtde.v13n3.1077

Wäger, 2018) or Natural Language Processing (Evans & Grefenstette, 2018). Some studies (Jobin *et al.*, 2019; Van Berkel *et al.*, 2020) perform computational analysis of these national policies.

At the ground level, however, these tools pose two challenges. First, they must be user-friendly and easy to operate (Casiano Flores *et al.*, 2022; Saxena *et al.*, 2022). Second, it has to gain the public's trust (Choi *et al.*, 2016). One of the prominent means over time that has evolved as an effective mechanism to access technological outreach is reviewing user feedback. With the emergence of AI, AI Chatbots have gained much attention. Chatbots have developed rapidly in numerous fields in recent years, including marketing, supporting systems, education, health care, cultural heritage, and entertainment (Adamopoulou & Moussiades, 2020). Chatbots are an apt example of intelligent Human-Machine interaction (Bansal & Khan, 2018). Many text-based chatbots target specific functionalities, enabled by tools that let us build bots for several widely used messaging platforms (Dale, 2016).

In this context, chatbots are the ideal use case. Since they can mimic and engage like humans, they have found applications in education, data retrieval, e-commerce and business (Shawar & Atwell, 2007). The success of chatbots is also attributed to their nature of being 'platform independent'. For instance, they can be integrated with any payment, travel, or messaging applications . Reduction in customer service expenditure and the ability to handle multiple users simultaneously are other reasons for its popularity. Specific chatbot applications have proven to be more 'friend' than 'assistant' (Costa, 2018). At the same time, aspects like lack of emotional connect with the customers, lack of situational awareness, privacy, gender bias and lack of empathy remain its grey area (Adamopoulou & Moussiades, 2020; Costa, 2018; Dale, 2016; Wallace, 2009). Nevertheless, the chatbots are here to stay. Amongst various ways to improve the efficiency and accuracy of these chatbots, taking feedback from users can be a very effective mechanism. One way to distribute these apps and get feedback is through the Google Play Store (GPS). GPS allows users to review through star ratings and user reviews. On a scale of 1-5, 1 being lowest and 5 being highest. The developers are also compensated based on the star rating (Linares-Vásquez *et al.*, 2013). While there are some studies on user reviews on chatbots in the mental health area (Haque & Rubya, 2023; De Freitas *et al.*, 2024), studies on the governance of AI chatbots are missing. Our paper assesses AI chatbot applications based on developers' self-declarations and users' feedback on GPS.

With the emergence of Natural Language Processing, studies have used various algorithms to undertake sentiment analysis. Valence Aware Dictionary and Sentiment Reasoner (VADER) is one of the most popular lexicon-based techniques. VADER is best suited for short sentences and abbreviations. The VADER technique has been widely applied to various managerial and computational contexts (Alam *et al.*, 2021; Daniulaityte *et al.*, 2016; Mathayomchan &

http://doi.org/10.18080/jtde.v13n3.1077

Taecharungroj, 2020). A more computationally heavy and accurate model is Bidirectional Encoder Representations from Transformers (BERT) (Basiri *et al.*, 2021; Sun *et al.*, 2017; Yadav & Vishwakarma, 2019). Restricting aspects of sentiment analysis, we have used an advanced Robustly Optimised BERT-Pretraining Approach (RoBERTa). Compared to BERT, RoBERTa uses about ten times more pre-trained uncompressed data. Few publications establish this finding through various use cases (Tan *et al.*, 2022; Sharma *et al.*, 2021; Yenkikar *et al.*, 2022). This study uses a simple VADER-based sentiment analysis combined with a complex and comparatively more accurate RoBERTa algorithm. The paper is one of the few that uses the two techniques in the same paper for a vast sentiment dataset extracted from the Google Play Store first-hand. The paper presents the application of these algorithms as a use case. It does not deal with the algorithm's inner workings, as the aim of using a second algorithm is to prevent any algorithmic bias.

In AI use, digital privacy, data theft, cybersecurity and social discrepancy remain the main challenges (Linkov *et al.*, 2018). Erkut Burak (2020) analyses the knowledge problem of economics in light of digitisation. The paper brings about knowledge and expectation deficit in accepting digitisation. Regulation of AI remains a grey area around the world. Should AI be regulated at all? (Navaratna & Sakena, 2023; OECD, 2017) is the fundamental question.

The choice between control by government-instituted regulation or self-regulation by stakeholders is often debated (Katzenbach & Ulbricht, 2019; Yeung & Bygrave, 2021). Some authors have argued that lack of a reliable framework for compliance law, the governments are forced to issue soft law with diverse arguments for centralisation or decentralisation of AI regulation between public, private and other institutes (Gutierrez and Marchant, 2021), requiring clear delineation of responsibilities resulting in a more complex regulatory structure (May, 2007; Djeffala *et al.*, 2022). This is a situation that both the governments and the companies wish to avoid. Hence, self-regulation and reporting are often suggested (Marwala, 2024).

Our paper falls in the domain of self-regulation to ensure compliance. The following section outlines the research methodology deployed in this study.

Table 1 highlights the broad strands under which papers relevant to the paper can be listed. The paragraphs above indicate the specific aspects highlighted by previous studies. Previous works (Hacker *et al.*, 2023; Sukhpal *et al.*, 2023; Bailao *et al.*, 2022; Calo, 2017) highlight the aspects surrounding digital technology-AI adaptation and its challenges but fall short of dealing with policy, regulation and governance. In contrast, some works (Linkov *et al.*, 2018; Van Burak, 2020; Navaratna & Sakena, 2023; OECD, 2017) deal with digital policy and governance but are not specific to citizen-centric applications or have not incorporated the

http://doi.org/10.18080/jtde.v13n3.1077

user/citizen in the loop. This aspect is covered by Linares-Vásquez *et al.* (2013) and Haque & Rubya (2023) have applied sentiment analysis to bring in user feedback into application regulation and governance design. Hence, our paper's novelty lies in integrating these three strands of studies into one use case.

Furthermore, the paper aims to highlight the gap between compliance (through self-regulation) and user feedback, a timely and critical research area. Using a dual algorithm to underscore algorithmic efficiency (based on previous studies) and using 117,353 user comments of the top ten AI Chatbot applications makes it a comprehensive paper. Further, the literature review helped us map compliance parameters. A few papers individually spoke of data, privacy, and GDPR. We have made an approach to bring in parameters based on the literature review and GPS preset declarations. The performance results under each parameter are also discussed.

Research Methodology

The research methodology followed in this study is outlined in Figure 1. The thought process for this research design is to independently assess the self-declaration efficiency of developers, and simultaneously perform an analysis of app reviews by the customers to see if these two aspects correlate. These two independent verticals are then compared and discussed in the context of policy and governance of AI with a user-centric perspective.

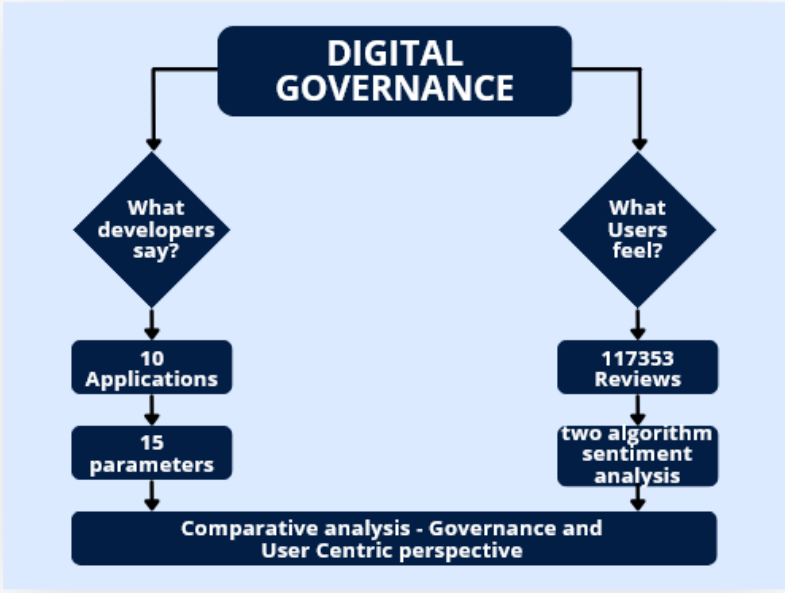


Figure 1: Research Methodology

http://doi.org/10.18080/jtde.v13n3.1077

Table 2: List applications and reviews considered

Sl No	Name of App	Developer	GPS Link	Down -loads	User Review
1	Talkie: Soulful AI	Subup	com.weaver.app.prod	1M+	12897
2	ChatGPT	Open AI	com.openai.ChatGPT	10M+	35109
3	AI Chatbot – Nova	AI Chatbot – Nova	com.scaleup.chatai	10M+	42714
4	ChatOn – AI Chat Bot Assistant	AIBY Inc.	ai.chat.gpt.bot	1M+	4845
5	Ask AI – Chat with Chatbot	Codeway Digital	com.codeway.chatapp	10M+	6620
6	Replika: My AI Friend	Luka, Inc	ai.replika.app	10M+	14256
7	Chat AI – Ask Anything	ElevenThirteen	com.chat.gtp	100K+	3074
8	Chatbot – GPT AI Chat, Ask AI	AppLab Kamil Piekarz	com.intelli.app	100K+	1047
9	Ask Me Anything – AI Chatbot	EVOLLY.APP	evolly.ai.chatbot.chatgpt	500K+	1544
10	Character AI – Chat Ask Create	Character.AI	ai.character.app	5M+	7994

http://doi.org/10.18080/jtde.v13n3.1077

Table 3: Self Declaration parameters

Data Safety (8)	Security (2)	App Permissions(5)
• Data shared • Personal info • Financial info • Messages • App activity • App info and performance • Device or other IDs • Data collected	• Data is encrypted • Data be deleted	• Location • Photo/ Files/ Media • Storage • Camera • Others

To get a user perspective, 'google_play_scraper' was used in a Python environment to scrape the latest review available as of October 2023 for the ten AI chatbot applications noted earlier. The total number of reviews considered for analysis is 117353. These are spread across ten applications, and the application reviews and star ratings vary in popularity. On these 117,353 user comments, sentiment analysis using VADER and RoBERTa is carried out. The data cleaning involved the removal of duplicate entries, missing values and irrelevant records. Next, text normalisation is carried out in which lowercasing, removal of HTML tags, URLs, special characters, and removal of unnecessary punctuation was undertaken. Contractions are expanded and emojis are either preserved (for VADER) or replaced with text equivalents (for RoBERTa). Tokenisation is performed, with VADER working on raw text while RoBERTa requires subword tokenisation. Stopword removal is optional, as deep learning models like RoBERTa can handle them contextually. Lemmatisation helps standardise words by converting them to their base form, ensuring consistency. Additionally, noisy data, such as gibberish text, is removed, and dataset balancing techniques are applied to prevent biases in supervised learning. By following these pre-processing steps, VADER and RoBERTa can effectively analyse sentiments more accurately. This set helps in providing the user experience in terms of feedback.

Keywords from individual applications are also extracted on positive and negative sentiments (Alam *et al.*, 2021; Daniulaityte *et al.*, 2016; Mathayomchan & Taecharungroj, 2020; Basiri *et al.*, 2021; Sun *et al.*, 2017; Yadav & Vishwakarma, 2019). Further, a random check of the reviews was carried out in July 2025 from previous data to ensure the data remained representative and relevant. However, it must be noted that results show most applications have high downloads and positive user sentiments in 2023 and 2025. Thus, the methodology remains representative for listed applications.

http://doi.org/10.18080/jtde.v13n3.1077

The results obtained from the previous steps were used to determine the gap in self-declaration compliance by developers and to see if users' sentiments reflect the compliance gap. In doing so, this study contextualises the state of self-regulation in light of chatbot apps. These findings are presented in the next section.

Findings

In this section, we first assess what developers of the selected apps claim concerning the 15 preset parameters on GPS. The findings on user reviews of these apps follow this.

What developers claim?

Many interesting patterns emerge when dealing with developers' questions about Google Play declarations. The findings are shown in Figure 2a and Figure 2b, revealing some interesting patterns. Firstly, all ten applications have declared whether they ask for user data. Moreover, all apps also declare whether data is shared with third parties. Thus, it may be concluded that the data usage and its declaration are given due consideration regarding digital governance. Developers also declare cybersecurity attributes like data encryption during transmission. The provision to enable the facility to delete the data on request by users stands at eight. This means that two applications do not declare this attribute.

Other attributes like financial information, messages and personal information are not declared actively by most applications. Important application-centric features that have a direct effect on the privacy of individuals, like location and use of camera/microphone, have glaring differences. Only 4/10 applications in AI chatbots have declared the use of cameras. Regarding location aspects, only 4/10 of applications in the chatbot segment have declared it. In general, about five attributes are not declared by five applications. Further, considering the initial three basket parameters of Data Safety, Security and App Permissions, the application performance in each category is listed in Figure 2(b).

Here, Data Shared (10/10) indicates that all the applications have declared a data shared parameter and so on. The total compliance in the category of data safety is about 65%, App Permission is 72% and security is 80%. Thus, the overall assessment of these top ten applications on these 15 parameters is about 69% (104/150). This can be seen as a strength of self-regulation in terms of self-declaration by the developers.

http://doi.org/10.18080/jtde.v13n3.1077

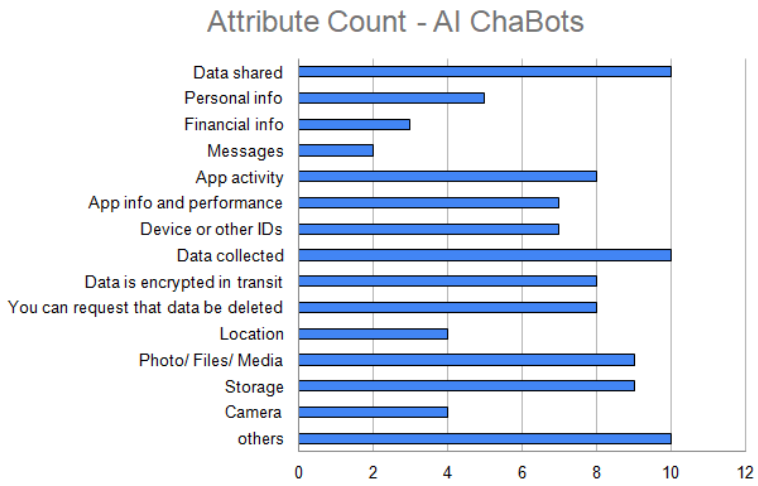


Figure 2(a): Attribute count of AI Chatbot apps

Data Safety	Security	App Permissions
• Data shared (10/10) • Personal Info (5/10) • Financial Info(3/10) • Messages (2/10) • App activity (8/10) • App info and performance (7/10) • Device or other IDs (7/10) • Data collected (10/10) • **TOTAL (52/80) 65%**	• Data is encrypted (8/10) • data can be delected (8/10) • **TOTAL (16/20) 80%**	• Location (4/10) • Photo/ Files/ Media (9/10) • Storage (9/10) • Camera (4/10) • Others (10/10) • **TOTAL (36/50) 72%**

Figure 2(b): Compliance analysis

Keyword analysis on self-declaration by app developers will help us give a ready reference to the keywords that have high term frequency. The top 20 keywords are listed in Table 4. With inclusion of words like store, safety, security, and save, the applications appear to be giving importance to these in their 'About Application' write-up, which users can read before downloading. However, on the 15-parameter declaration, they lack compliance. Even with low compliance ratings, they continue to be popular on GPS. This is a regulation challenge.

http://doi.org/10.18080/jtde.v13n3.1077

Table 4: Top 20 keywords

TOP 20 KEYWORDS
• data • chatgpt • store • developer • safety • practices • device • collect • shared • security • information • deleted • writing • technology • performance • request • downloads • language • interactions • history

What do users feel?

This section presents sentiment analysis of user comments. Table 5 presents a snapshot of how reviews can be interpreted differently by these two individual algorithms. This is also the reason for using two algorithms. The table users Chat GPT user review as an example.

A higher positive score denotes a more positive sentiment, and a negative score indicates a negative sentiment. Using the same, VADER provides a compounded score. RoBERTa, on the other hand, classifies reviews into positive, negative and neutral sentiment. To overcome this ambiguity, we have plotted star rating versus sentiment rating, as shown in Table 6. This table may be considered a prototype to interpret data in Table 7, the outcome of the metric of ten applications analysed in this paper.

Table 7 indicates a comparison of star and sentiment analysis. The star ratings of all ten apps indicate a high five-star rating. Most of the applications have a few four ratings or below. These are indeed good applications in terms of customer perception. Figures 3(a-d) present the result of sentiment analysis of the reviews carried out on these applications. Here, the behaviour of VADER is skewed 65% towards neutral sentiments. RoBERTa, on the other hand, has provided 71% (77,953 reviews) positive sentiments, 16.8% negative and about 12.4% neutral. Three applications had overall positive sentiments in both algorithms. Apart from one application, most applications have positive sentiments of more than 50%, while four applications had positive sentiments of 75% or more. Though ChatGPT from OpenAI has

http://doi.org/10.18080/jtde.v13n3.1077

arguably brought in a revolution, as per users' sentiments, some applications perform much better.

Table 5: Interpretation of sentiments

Application	User Review	VADER	RoBERTa	Remarks
Chat GPT	'gets math wrong occasionally.'	Negative	Negative	Both algorithms have classified the review as negative.
	'Very intelligent. But the new update has been destabilised; it no longer opens. So be careful to click updates. It does not make functionality better. They sent an update to disable free apps so you can go for the premium version. Of course, it is worth the payment. I missed my chatpartner chatgpt.'	Neutral	Negative	VADER fails on a longer comment. It is evident here that the algorithm has classified it as neutral. However, RoBERTa has classified it as negative sentiment.
	'Without threads I am happy.'	Negative	Positive	Here, the classification is in total opposition. The active and passive speech, with 'without', has forced VADER to classify it as negative, while more efficient RoBERTa has classified it as positive.

http://doi.org/10.18080/jtde.v13n3.1077

Table 6: Plot of various metrics

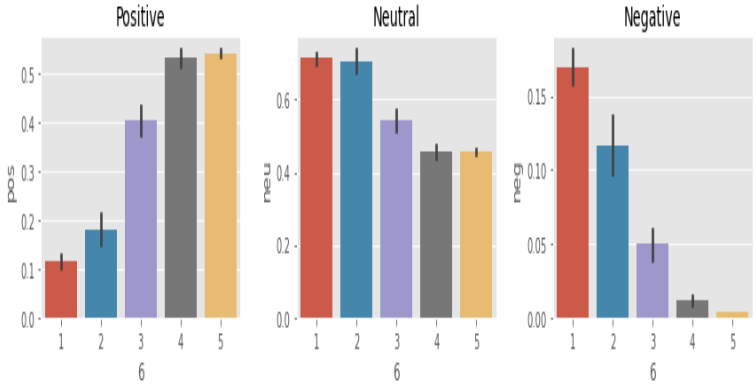
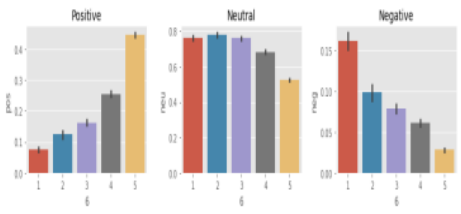
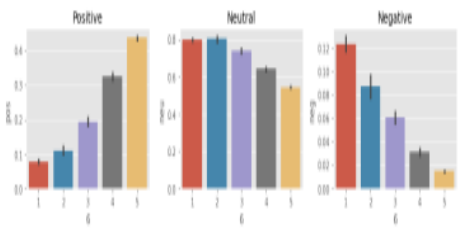
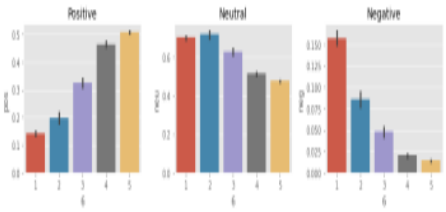
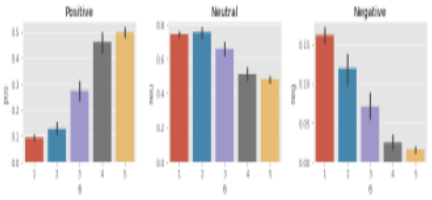
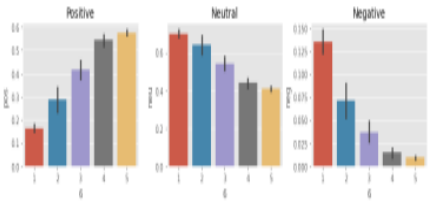
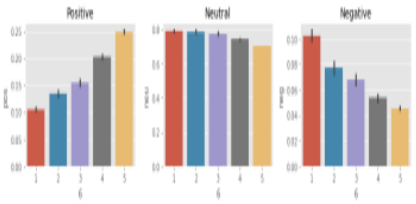
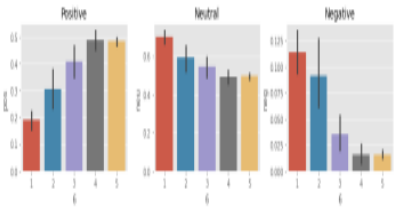
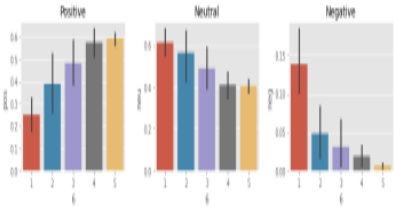
Output	Remarks
	**Star Rating**: This bar graph indicates the reviews count per star rating (1 to 5).
	**Star v/s Sentiments**: The x-axis indicates star rating, and the y-axis indicates polarity score. This graph shows that lower star ratings have negative polarity while higher stars have positive polarity. In the case of neutral polarity, stars exist almost evenly.

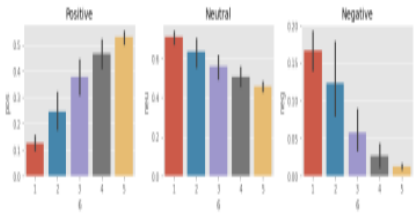
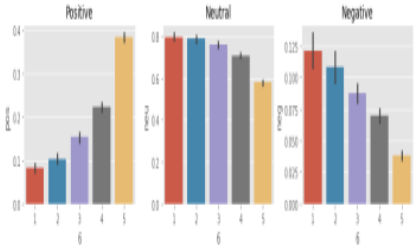
Table 7: Result tabulation of ten applications

AIChatBot	Star Rating Count	Star Rating V/S Sentiments
Talkie Soulful AI		
ChatGPT		

http://doi.org/10.18080/jtde.v13n3.1077

AIChatBot	Star Rating Count	Star Rating V/S Sentiments
AI Chatbot Nova		
Chaton AI Chatbot Assistant		
Chat Ask AI by Codeway		
Replika virtual AI Companion		
Chat AI ask anything		
Chatbot Virtual AI Chat		

http://doi.org/10.18080/jtde.v13n3.1077

AIChatBot	Star Rating Count	Star Rating V/S Sentiments
AI chatbot asks me anything		
CharacterAI AI-powered-chat		

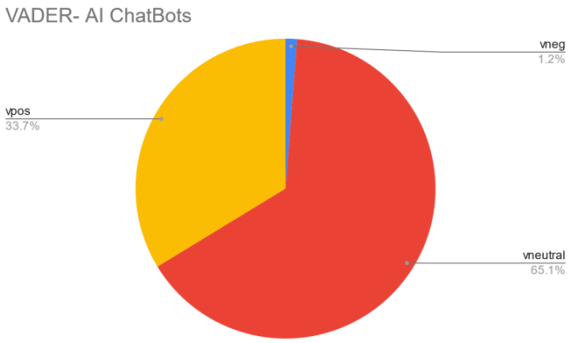


Figure 3(a): VADER sentiment analysis – AI Chatbots

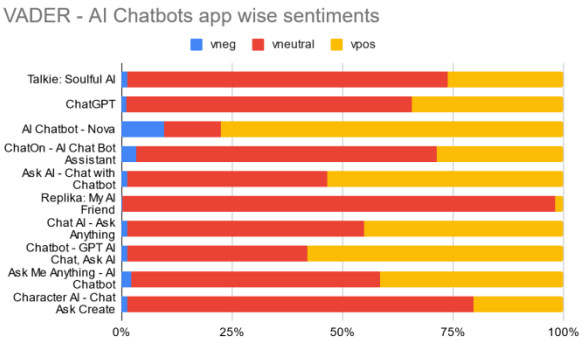


Figure 3(b): VADER app-wise sentiment

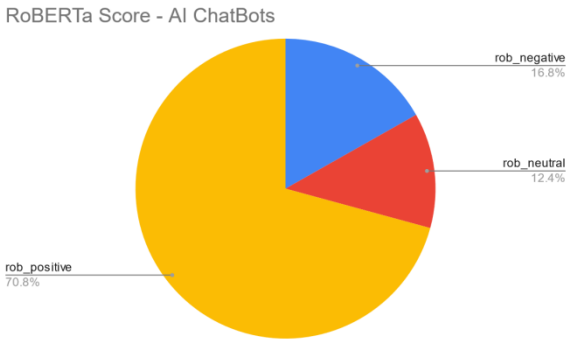


Figure (3c): RoBERTa sentiment analysis – AI Chatbots

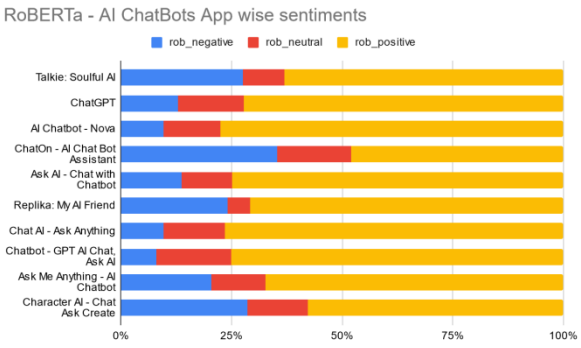


Figure 3(d): RoBERTa app-wise sentiment

http://doi.org/10.18080/jtde.v13n3.1077

Figure 4(a): Most Negative Sentiments

Figure 4(b): Most Positive Sentiments

To understand the nature of positive and negative sentiments, expressions associated with users' most positive and negative feelings were identified. A word cloud of ten applications is pictorially presented in Figure 4(a) and Figure 4(b). Negative sentiments had expressions like poor, bug, error, reason, uninstall, wrong, waste and feature, while positive sentiments were awesome, good, superb, response and useful.

Discussion

In the development aspect surrounding any application, concerns and priorities of various stakeholders are to be addressed, namely those of the developer, the user, and the regulation or compliance. At times, it is observed that developers usually follow development aspects that best suit them, sometimes far from what customers want (Dudley et al., 2015). Sometimes, the application boasts about technology adaptation and alienation from what the users want (Curtis, 2019). Further, some applications have so many services that the customer finds it very cumbersome to use (Castelnovo & Sorrentino, 2017). Saxena *et al.* (2022) have suggested reducing the number of touch points, thus making the user experience more satisfying and simple. The other suggestions include establishing dialogue with the user (Lamberti, 2013) to adopt a user collaborative approach (Martin & Webb, 2009) and hybrid governance (Leiser & Murray, 2016). Thus, this leads us to the question: how do we know what the user wants? How do we know what the developer is developing? Based on the results obtained, the discussion is tailored around these questions.

What developers claim?

Application of 15-parameter scale for the developer perspective and using sentiment analysis for user feedback to understand the gap with AI Chatbots as a use case to study digital governance provides valuable insights. Based on the analysis, a few governance aspects emerge very clearly. Not all apps complied with the 15 parameters set by GPS for declaration. Crucial aspects like data handling (8/10), camera (4/10), location information (4/10),

http://doi.org/10.18080/jtde.v13n3.1077

personal information (5/10) and financial information (3/10) are not complied with by all applications. Yet, the users' review comments did not significantly cater to these aspects and were more vocal about features, speed and quality of service. Thus, the compliance and governance aspect of the developer is indeed under question, but at the same time, the user seems undeterred during onboarding.

A declaration by the developer is expected to state the mandatory disclosures expected from them, either through regulation (self or government-mandated). Due to the absence of standard regulation, soft law continues to be a challenge. Here, to achieve standard comparison, we have chosen applications hosted on Google Play and were expected to comply with their disclosure parameters (Google, 2025). These 15 parameters are listed in Table 2, and their result is tabulated in Figure 2.

Aspects like data encryption, transportation, camera, location, microphone, photo, and media usage remain a grey area of declaration by developers. Data protection rights (Yang *et al.*, 2019; Wang *et al.*, 2019) are a matter of significance from a user and regulatory perspective. Developers must inform users of the intention to share, use, or store their data. Surprisingly, few applications have stated that they collect data from users but do not provide any option to delete it, even though the user desires to do so. Only four applications in AI chatbots have declared the use of cameras.

Regarding location aspects, only 4/10 of applications in the chatbot segment have declared it. The total compliance in the category of data safety is about 65%, App Permission is 72% and security is 80%. Thus, the overall assessment of these top ten applications on these 15 parameters is about 69% (104/150). This can be seen as a strength of self-regulation in terms of self-declaration by the developers. These finer aspects need larger public awareness and require citizens across the globe to be digitally aware. This appears to be a work in progress that requires more extensive public participation. This observation throws up two questions. In the interest of user security and data rights, developers must declare these aspects, which they are not.

Secondly, even though they are not compliant (self-declaration here), the user base is evidence of their popularity. Is self-governance effective at all? Is there a need for a regulator? Further, the application hosting platforms like Google Play Store and Apple Store must also enforce mandatory compliance with these parameters. The above data suggests that, though few developers have declared parameters, they do not appear in the user's interest. For example, the personal data collected from users is not allowed to be deleted by the developer. The digitally unaware user may still use the application; however, as a hosting platform, is it ethically correct to allow such practices in the larger interest of privacy, security and societal

http://doi.org/10.18080/jtde.v13n3.1077

good? Should these app stores impose binary declarations only? What must be the exact definition of each declaration, then? This leads to a larger question of regulation in context, in view of clear definitions and responsibility demarcations.

As per Pugliese *et al.* (2021), the lack of clear definitions leads to 'opaqueness' and 'unforeseeability', making it difficult to establish who should be responsible for the damages caused by ML or AI tools. These grey areas and lack of clear mandates lead to 'soft law'. Due to a lack of a reliable framework for compliance law, governments are forced to issue soft law with diverse arguments for centralisation or decentralisation of AI regulation between public, private and other institutes (Gutierrez & Marchant, 2021). June 2017 OECD Ministerial Meeting in Paris highlighted the following three options for AI Governance: (1) a laissez-faire, industry-driven approach; (2) a precautionary and preemptive strategy on the part of government, and (3) a stewardship and 'active surveillance' approach by government agencies. , while articulating information privacy, argue that corporations are not perceived to manage information privacy effectively; thus, users are more inclined to have strict regulations through law. They suggest that the self-regulatory privacy governance model may not be sustainable over the long term. While presenting analysis of a customer self-regulated environment (Babin, 1995) says feelings of dominance, previously dismissed as unimportant, significantly impact shopping behaviour among those low in self-regulation. In the context of AI governance, while Ferretti (2022) argues for more institutional regulations, Marwala (2024) suggests a more balanced approach.

What do users feel?

9/10 applications considered in the paper have high positive sentiment. This validates their popularity and high volume of downloads. Within AI chatbots, the objective of chatbots varies from writing scripts to LLM to picture-to-word conversion or vice versa. They are popular on the GPS based on their functionality. Irrespective of what the self-declaration says, the number of downloads and reviews is evidence of their acceptability by users. The quantum of reviews and downloads from the Google Play Store in Table 1 is evidence of this. Users have provided their reviews based on the services rendered by the applications. The quality of services, application Human Machine Interface (HMI), user friendliness of applications and response of service providers were observed to be of key importance. Aspects like bad HMI, quantum and reach of applications and service delivery efficacy raised apprehension among the users. The reference to the compliance declaration of the developer or apprehension was generally not observed in keyword analysis.

The acceptability and positivity are very high for AI Chatbots. Thus, irrespective of the state of the nation, the developer, or the firm, the app's service acts as a deciding factor in sentiments.

http://doi.org/10.18080/jtde.v13n3.1077

Table 5 above has pictorially plotted star v/s review. However, in our study, there is evidence that high star-rated reviews complemented low polarity values and vice versa. These are plotted in Table 6. All the applications listed have good star ratings and are complemented by highly positive sentiments and comments. Studies (Noei & Lyons, 2019; Noei, 2018) have previously brought out the ambiguity between star ratings and reviews posted by users. This attribute is negated in our paper due to the high dataset size. These applications are popular on GPS, attracting a large user base. None of the ten applications showed disparity between star versus review sentiments. As we have used ten applications for review, tabulation of the most positive and negative keywords indicated user emotions centred around features and application performance alone.

To limit the length of the paper, Figure 4 indicates the most positive and negative sentiment keywords. Aspects like security and data collection were not prominently featured in keyword analysis. The users are more focused on aspects like HMI, services offered, quality of service, speed and delivery efficiency. Each chatbot considered in the dataset had a varied functionality, so the general sentiments resonated were more or less similar. Thus, sense-making from user feedback on a mobile store to determine why they hate or love the application is challenging (Fu *et al.*, 2013).

Lampropoulos *et al.* (2022, while discussing the customer relationship management (CRM), bring in essential aspects of Quality of Service (QoS) and Quality of Experience (QoE). They argue that integrating these aspects will offer more personalised and customised products and services and significantly improve customers' satisfaction, acquisition, relationships, loyalty, experience and retention. In the context of cloud computing, Xiong & Perros (2009) argue that for the commercial success in the computing paradigm, the ability to deliver Quality of Services (QoS) guaranteed services is crucial, whereby determining the relationship among the maximal number of customers, the minimal service resources and the highest level of services. It now becomes essential to understand the difference between QoS and QoE. Taking examples of network and telephone applications, QoS is measured in terms such as error rate, bit rate, throughput, transmission delay, availability, and jitter, and has been touted as a technological requirement for most services. Shin (2017) brings in a critical aspect surrounding QoS. QoS has a high inward orientation. It's a service provider's or developer's perspective to define technicalities. A need to shift to QoE has emerged to understand the user-centric experience. QoE assesses consumer expectations, feelings, perceptions, cognition, and satisfaction about a product, service, or application (Deng *et al.*, 2010). Thus, QoE can complement User Experience (UX) (Shin, 2017). The significant outcomes of the analysis can be summed up in Figure 5. The sentiments expressed on the Google Play Store revolve mainly around three-prong structures of the application. The application's purpose is to serve (QoS)

http://doi.org/10.18080/jtde.v13n3.1077

and user experience (UX+QoE). Shin (2017), through a model, lists coolness, service, content, hedonicity, affordance, system and utility as QoE factors. In our study, the user sentiments surrounding these factors through direct reference or synonyms are evident in the keyword analysis of post-positive and negative UX.

When users need to use chatbots for routine tasks or other services, they download and use the application. That becomes 'need-based' use. The user experience, on the other hand, is wholly based on the features, service quality, response from the firm and other technical aspects of the application. This becomes 'quality-based' use. What does not prominently figure in self-declaration and sentiment analysis is an expression of any apprehension or fear of policy violation by applications, as observed by users. In reality, digital governance must be the precursor to the download and usage of applications. This becomes 'governance-based' use.

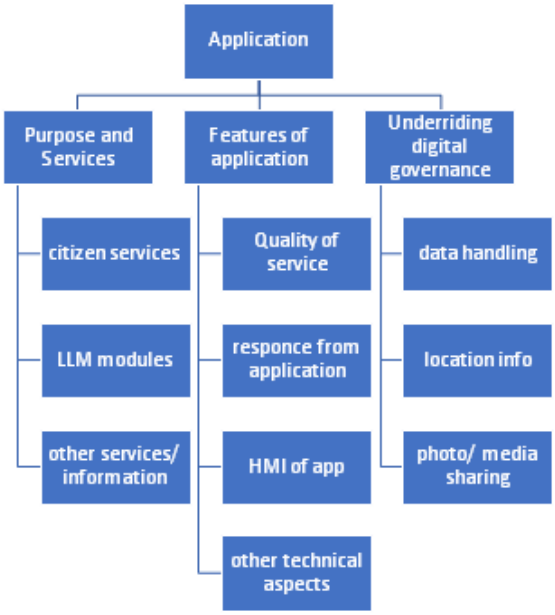


Figure 5: Outcome of result analysis

The user experience versus developer claims in the context of regulation follow one of the contexts as indicated in Figure 6(a) or Figure 6(b). Even if governance means self-declaration, the awareness of users and the responsibility of developers needs further deliberation. There is a need to make citizens and users more digitally aware and knowledgeable. This result further amplifies the need for user-centric development (Bastardo *et al.*, 2024; Henman, 2020; Javaid *et al.*, 2023; Saklani & Kala, 2024; Talanquer, 2023). Some papers have evolved a usability score (Arnhold et al., 2014). This concept is unique but lacks formal backing from application stores or the government, making it fall under the realm of soft law. Policy, regulation and governance from policy to practice needs a ten-step approach (Navaratna &

http://doi.org/10.18080/jtde.v13n3.1077

Saxena, 2025). Thus, is regulation through command and control (primarily through Governments) better than self-regulation?), through a classic work, has established that 'strict' command and control on one hand, and 'pure' self-regulation are mutually exclusive. Further, they state that policymakers can use several 'regulatory variables' to 'fine-tune' regulatory options to suit the specific circumstances of particular environmental issues. In most circumstances, a combination of self-regulation, command, and control will provide the ideal regulatory outcome. While undertaking a psychological analysis of impulsive buying, Verplanken & Sato (2011), regulation against misleading practices that play on the vulnerabilities of impulsive buyers could be sharpened. Providing information to consumers and retailers to strengthen consumers' self-regulatory capacities may mitigate the adverse consequences of impulse buying.

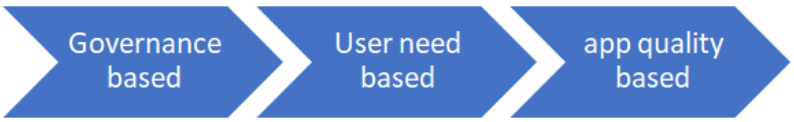


Figure 6(a): Expected Flow of User Evaluation

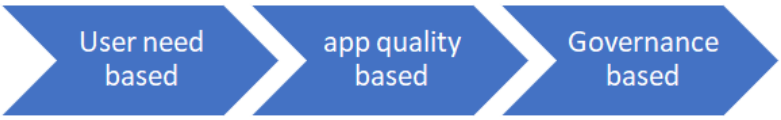


Figure 6(b): Realistic Flow of User Evaluation

Thus, with about 69% compliance as exhibited by our study and many previous works stated above, it is established that self-regulation may lead to selective compliance. On the other hand, in our research, the user exhibited an inclination towards QoE and user experience rather than the compliance aspects. Thus, it is imperative to spread awareness amongst users on aspects of compliance aided by strong statutory laws. With an increasing digital footprint, user awareness on data collection, privacy, compliance, location information, and use of photos and media needs to be enhanced. It is this vertical that impetus is desired from the government on governance and regulation for societal good.) propose a unified model, called the unified model of information security policy compliance (UMISPC), for Information systems security (ISS) to explain security policy compliance. A classic work by Steurer (2013) argues that governmental deregulation has been accompanied by soft governmental regulation and 'societal re-regulation'.

http://doi.org/10.18080/jtde.v13n3.1077

Should the government intervene, enact legislation, and bring regulators into every field? Should the domain of digital governance be self-regulated? Or must it be left to ethical management and understanding of the user-developer? These are a few unanswered questions in this domain (Katzenbach & Ulbricht, 2019; Yeung & Bygrave, 2021). Unable to resolve these hegemonies, governments usually prefer soft laws mainly due to the absence of a reliable framework (Gutierrez & Marchant, 2021). The interrelation between types of regulatory regimes and responsibility (May, 2007; Djeffala *et al.*, 2022) is also crucial in determining a suitable regime for a technology.

Our paper studied the Google Play Store's instituted self-declaration mechanism (Google, 2025). The deviation by applications on these platforms is evident in the parameters. Thus, a standardised, safe and ethical framework in view of achieving a harmonious digital society is needed of the hour. Since self-regulation is not sufficient in the absence of user awareness, a hybrid approach is more suitable (Marwala, 2024) for AI governance. For instance, apart from regulatory and compliance aspects, developers may also utilise user sentiment analysis to include new features demanded by the users. This may result in more user awareness and control of collected information. Aspects like selective permissions for information use and the facility to delete the uploaded personal information.

More such parameters surrounding data privacy must be made available to the users. An in-app facility highlighting the availability of such a facility must be made available. The application hosting platform must ensure strict compliance, keeping in mind users from all strata of society and education in the population. For instance, the compliance information and settings may be available in regional languages based on location information. This will also help increase the compliance mandate above the present 69%. This will create a healthy ecosystem between users and developers in the interest of safety, ethics and fairness, making these applications more citizen-centric. Like the ratings, the app stores may be mandated to provide compliance scores for each application hosted on their platform. For example, Application ABC (Compliance Score: 80/100) can be displayed in a prominent place. The score can be a weighted sum of the compliance score on each parameter that the application store sets. This score needs to be aligned with the legislative framework of the host country and self-regulated (in case of the absence of legislation). This will increase transparency and increase awareness amongst users. Users can exercise caution before using the application based on the compliance score.

Conclusion

Our study analysed ten AI chatbot applications based on 15 self-declaration parameters and a review of 117353 user inputs using two algorithms. We find that more attention is required for

http://doi.org/10.18080/jtde.v13n3.1077

the aspects of data handling, data sharing, and data transmission. Aspects like location, photo, media and the ability to delete user data by the user are shared across platforms. A cumulative strength of 69% is determined towards compliance. However, when it comes to user sentiment, the users assess the applications based more on user experience and not predominantly on governance issues. Thus, with about 69% compliance as exhibited by our study and many previous works stated above, it is established that self-regulation may lead to selective compliance. On the other hand, the users are more inclined towards QoE and user experience than the compliance aspects. Thus, it is imperative to spread awareness amongst users on aspects of compliance aided by strong statutory laws.

With an increasing digital footprint, user awareness on data collection, privacy, compliance, location information, and use of photos and media needs to be enhanced. Further studies can look into adopting frameworks like UMISPC proposed by to achieve information security. Implementing studies surrounding ethics, fairness, compliance, and privacy (Adamopoulou & Moussiades, 2020; Costa, 2018; Dale, 2016; Wallace, 2009) may be adopted to platform applications. Further, the application store can provide a compliance score for each application based on mandatory disclosures. This gives a standardised assessment yardstick for ordinary users to decide before downloading. This compliance score must be made compulsory for sensitive applications surrounding the use case of medical applications, financial transactions or data-intensive processing. The paper uses a primary dataset for application reviews. It is one of the few papers that have used VADER and RoBERTa together for AI chatbots to review policy and governance aspects. One limitation of our study is the review of only ten applications and two algorithms. Further studies can be carried out on the fundamentals of self-declaration of digital applications. It would be ideal to establish proposed declaration guidelines. Other algorithms, transformers, or hybrid models can be explored for analysis. Another limitation of this study is that it draws from self-reported data from developers and users. A more in-depth study would examine the application to see if the declarations correspond to the implementation and use.

References

Abu Shawar, B.A., Atwell, E.S. (2007). Chatbots: Are they really useful? *Journal for Language Technology and Computational Linguistics*, *22*: 29–49.

Adamopoulou, E., & Moussiades, L. 2020. An Overview of Chatbot Technology. *IFIP Advances in Information and Communication Technology*, *584*(1): 373–383. https://doi.org/10.1007/978-3-030-49186-4_31

Alam, K. N., Khan, M. S., Dhruba, A. R., Khan, M. M., Al-Amri, J. F., et al. 2021. Deep Learning-Based Sentiment Analysis of COVID-19 Vaccination Responses from Twitter Data. (A. Korobeinikov, Ed.) *Computational and Mathematical Methods in Medicine*, 2021: 1–15.

Arnhold, M., Quade, M., & Kirch, W. (2014). Mobile Applications for Diabetics: A Systematic Review and Expert-Based Usability Evaluation Considering the Special Requirements of Diabetes Patients Age 50 Years or Older. *Journal of Medical Internet Research*, *16*(4), e104. https://doi.org/10.2196/jmir.2968

Babin, B. (1995). Consumer self-regulation in a retail environment. *Journal of Retailing*, *71*(1), 47–70. https://doi.org/10.1016/0022-4359(95)90012-8

Bailao Goncalves, M., Anastasiadou, M., & Santos, V. 2022. AI and public contests: a model to improve the evaluation and selection of public contest candidates in the Police Force. *Transforming Government: People, Process and Policy*, *16*(4): 627–648.

Bansal, H., & Khan, R. 2018. A Review Paper on Human Computer Interaction. *International Journal of Advanced Research in Computer Science and Software Engineering*, *8*(4): 53.

Basiri, M. E., Nemati, S., Abdar, M., Cambria, E., & Acharya, U. R. 2021. ABCDM: An Attention-based Bidirectional CNN-RNN Deep Model for sentiment analysis. *Future Generation Computer Systems*, 115: 279–294.

Bastardo, R., Pavão, J., & Rocha, N. P. (2024). Methodological Quality of User-Centered Usability Evaluation of Digital Applications to Promote Citizens' Engagement and Participation in Public Governance: A Systematic Literature Review. *Digital*, *4*(3), 740–761. https://doi.org/10.3390/digital4030038

Calo, R. 2017. Artificial Intelligence Policy: A Roadmap. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3015350

Casiano Flores, C., Rodriguez Müller, A. P., Virkar, S., Temple, L., Steen, T., et al. 2022. Towards a co-creation approach in the European Interoperability Framework. *Transforming Government: People, Process and Policy*. https://doi.org/10.1108/tg-03-2022-0033

Castelnovo, W., & Sorrentino, M. (2017). The digital government imperative: a context-aware perspective. Public Management Review, 20(5), 709–725. https://doi.org/10.1080/14719037.2017.1305693

Chatterjee, S. 2020. AI strategy of India: policy framework, adoption challenges and actions for government. *Transforming Government: People, Process and Policy*, ahead-of-print(ahead-of-print). https://doi.org/10.1108/tg-05-2019-0031

Chhetri, T. R., Hohenegger, A., Fensel, A., Kasali, M. A., & Adekunle, A. A. 2023. Towards improving prediction accuracy and user-level explainability using deep learning and knowledge graphs: A study on cassava disease. *Expert Systems with Applications*, 233: 120955.

Chongwarin, J., Manorom, P., Chaichuay, V., Boongoen, T., Li, C., & Chansanam, W. (2024a). Enhancing Book Recommendation Accuracy through User Rating Analysis and Collaborative Filtering Techniques: An Empirical Analysis. *Journal of Telecommunications and the Digital Economy*, *12*(3), 51–72. https://doi.org/10.18080/jtde.v12n3.976

Choi, H., Jae Park, M., Jeung Rho, J., & ZO, H. 2016. Rethinking the assessment of e-government implementation in developing countries from the perspective of the

design–reality gap: Applications in the Indonesian e-procurement system. *Telecommunications Policy*, *40*(7): 644–660.

Costa, P. (2018). Conversing with personal digital assistants: On gender and artificial intelligence. *Journal of Science and Technology of the Arts*, 59-72 Páginas. https://doi.org/10.7559/CITARJ.V10I3.563

Curtis, S. (2019). Digital transformation—the silver bullet to public service improvement? Public Money & Management, 39(5), 322–324. https://doi.org/10.1080/09540962.2019.1611233

DALE, R. 2016. The return of the chatbots. *Natural Language Engineering*, 22(5): 811–817. https://doi.org/10.1017/S1351324916000243

Daniulaityte, R., Chen, L., Lamy, F. R., Carlson, R. G., Thirunarayan, K., et al. 2016. "When 'Bad' is 'Good'": Identifying Personal Communication and Sentiment in Drug-Related Tweets. *JMIR Public Health and Surveillance*, *2*(2): e162.

De Freitas, J., Uğuralp, A. K., Oğuz-Uğuralp, Z., & Puntoni, S. (2024). Chatbots and mental health: Insights into the safety of generative AI. *Journal of Consumer Psychology*, *34*(3), 481-491.

Deng, L., Turner, D. E., Gehling, R., & Prince, B. (2010). User experience, satisfaction, and continual usage intention of IT. *European Journal of Information Systems*, *19*(1), 60–75. https://doi.org/10.1057/ejis.2009.50

Djeffal, C., Siewert, M. B., & Wurster, S. 2022. Role of the state and responsibility in governing artificial intelligence: a comparative analysis of AI strategies. *Journal of European Public Policy*, 1–23.

Dudley, E., Lin, D. Y., Mancini, M., & Ng, J. (2015). Implementing a citizen-centric approach to delivering government services. McKinsey & Company. https://www.mckinsey.com/industries/public-sector/our-insights/implementing-a-citizen-centric-approach-to-delivering-government-services

Erkut, B. (2020). From Digital Government to Digital Governance: Are We There Yet? *Sustainability*, *12*(3), 860. https://doi.org/10.3390/su12030860

Evans, D., & Yen, D. C. 2006. E-Government: Evolving relationship of citizens and government, domestic, and international development. *Government Information Quarterly*, *23*(2): 207–235.

Fournier-Tombs, E., & McHardy, J. (2023). A Medical Ethics Framework for Conversational Artificial Intelligence. *Journal of Medical Internet Research*, *25*, e43068. https://doi.org/10.2196/43068

Fu, B., Lin, J., Li, L., Faloutsos, C., Hong, J., & Sadeh, N. (2013). Why people hate your app: Making sense of user feedback in a mobile app store. *Proceedings of the 19th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 1276–1284. https://doi.org/10.1145/2487575.2488202

Fullerton, R. A. (2011). Historical methodology: The perspective of a professionally trained historian turned marketer. *Journal of Historical Research in Marketing*, *3*(4), 436–448. https://doi.org/10.1108/17557501111183608

Google (2025). Understand app privacy & security practices with Google Play's Data safety section - Computer - Google Play Help. *support.google.com*. https://support.google.com/googleplay/answer/11416267?hl=en&visit_id=638319916177498248-660086043&p=data-safety&rd=1#zippy=%2Cdata-types%2Cdata-purposes%2Cunderstand-app-permissions%2Ccontrol-app-permissions-data-collection-after-download, October 25, 2023.

Gutierrez, C. I., & Marchant, G. E. 2021. A Global Perspective of Soft Law Programs for the Governance of Artificial Intelligence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3855171

Hacker, P., Engel, A., & Mauer, M. 2023. Regulating ChatGPT and other Large Generative AI Models. *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*. https://doi.org/10.1145/3593013.3594067

Haque, M. R., & Rubya, S. (2023). An overview of chatbot-based mobile mental health apps: insights from app description and user reviews. *JMIR mHealth and uHealth*, *11*(1), e44838.

Henman, P. (2020). Improving public services using artificial intelligence: Possibilities, pitfalls, governance. *Asia Pacific Journal of Public Administration*, *42*(4), 209–221. https://doi.org/10.1080/23276665.2020.1816188

Javaid, M., Haleem, A., & Singh, R. P. (2023). ChatGPT for healthcare services: An emerging stage for an innovative perspective. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, *3*(1), 100105. https://doi.org/10.1016/j.tbench.2023.100105

Jobin, A., Ienca, M., & Vayena, E. 2019. The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9): 389–399.

Katzenbach, C., & Ulbricht, L. (2019). Algorithmic governance. Internet Policy Review, *8*(4), 1-18.

Lamberti, L. (2013). Customer centricity: the construct and the operational antecedents. Journal of Strategic Marketing, 21(7), 588–612. https://doi.org/10.1080/0965254x.2013.817476

Lampropoulos, G., Siakas, K., Viana, J., & Reinhold, O. (2022). Artificial Intelligence, Blockchain, Big Data Analytics, Machine Learning and Data Mining in Traditional CRM and Social CRM: A Critical Review. *2022 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, 504–510. https://doi.org/10.1109/WI-IAT55865.2022.00080

Leiser, M., & Murray, A. 2016. The role of non-state actors and institutions in the governance of new and emerging digital technologies. *The Oxford Handbook of Law, Regulation and Technology*, 670–704.

Linkov, I., Trump, B., Poinsatte-Jones, K., & Florin, M.-V. (2018). Governance Strategies for a Sustainable Digital World. *Sustainability*, *10*(2), 440. https://doi.org/10.3390/su10020440

Linares-Vásquez, M., Bavota, G., Bernal-Cárdenas, C., Di Penta, M., Oliveto, R., et al. 2013. API change and fault proneness: a threat to the success of Android apps. *Proceedings*

of the 2013 9th Joint Meeting on Foundations of Software Engineering - ESEC/FSE 2013, 477–487.

Martin, S., & Webb, A. (2009). "Citizen-centred" public services: contestability without consumer-driven competition?. Public Money & Management, 29(2), 123–130. https://doi.org/10.1080/09540960902768038

Martinengo, L., Van Galen, L., Lum, E., Kowalski, M., Subramaniam, M., & Car, J. (2019). Suicide prevention and depression apps' suicide risk assessment and management: A systematic assessment of adherence to clinical guidelines. *BMC Medicine*, *17*(1), 231. https://doi.org/10.1186/s12916-019-1461-z

Marwala, T. (2024). Self-regulation Versus Government Regulation. In *The Balancing Problem in the Governance of Artificial Intelligence* (pp. 207-221). Singapore: Springer Nature Singapore.

Mathayomchan, B., & Taecharungroj, V. 2020. "How was your meal?" Examining customer experience using Google maps reviews. *International Journal of Hospitality Management*, 90: 102641.

May, P. J. (2007). Regulatory regimes and accountability. *Regulation & Governance*, *1*(1): 8-26.

Middelweerd, A., Mollee, J. S., Van Der Wal, C. N., Brug, J., & Te Velde, S. J. (2014). Apps to promote physical activity among adults: A review and content analysis. *International Journal of Behavioral Nutrition and Physical Activity*, *11*(1), 97. https://doi.org/10.1186/s12966-014-0097-9

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science*, *11*(1), 35–57. https://doi.org/10.1287/orsc.11.1.35.12567

Moody, G. D., Siponen, M., University of Jyväskylä, Pahnila, S., & University of Oulu. (2018). Toward a Unified Model of Information Security Policy Compliance. *MIS Quarterly*, *42*(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853

Navaratna, A., & Saxena, D. 2023. An Indian Approach to AI Policy: A Comparative Study Between Three Sectors. *Handbook of Evidence Based Management Practices in Business*, *1*(1): 403–408.

Navaratna, A. R. & Saxena. D. (2025). From policy to practice in digital governance: A three-level analysis of citizen-centric applications. *JeDEM - eJournal of eDemocracy and Open Government*, *17*(1), 33–64. https://doi.org/10.29379/jedem.v17i1.906

Noei, E. 2018. Succeeding in Mobile Application Markets (From Development Point of View) - ProQuest. *www.proquest.com*. PhD Dessertation. https://www.proquest.com/openview/8ed25761dafd4e1570f9d2fb3885d23c/1.pdf?pq-origsite=gscholar&cbl=18750

Noei, E., & Lyons, K. 2019. A Survey of Utilizing User-Reviews Posted on Google Play Store. *Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering*, 54–63.

OECD. 2017. "Ministerial Council Meeting 2017, OECD, Paris.", https://www.oecd.org/mcm/ministerial-council-meeting-2017.htm

Pade-Khene, C., Machiri, M., & Thinyane, H. 2017. Building foundations before technology: An operation model for digital citizen engagement in resource constrained contexts. *Proceedings of the European Conference on E-Government, ECEG*, 118–126.

Pugliese, R., Regondi, S., & Marini, R. (2021). Machine learning-based approach: Global trends, research directions, and regulatory standpoints. *Data Science and Management*, *4*, 19–29. https://doi.org/10.1016/j.dsm.2021.12.002

Saklani, S., & Kala, D. (2024). Perception of Gen Z Customers towards Chatbots as Service Agents: A Qualitative Study in the Indian Context. *Journal of Telecommunications and the Digital Economy*, *12*(1), 356–376. https://doi.org/10.18080/jtde.v12n1.781

Saxena, D., Muzellec, L., & McDonagh, J. 2022. From Bureaucracy to Citizen-Centricity. *International Journal of Electronic Government Research*, *18*(1): 1–17.

Seuring, S., Stella, T., & Stella, M. (2021). Developing and Publishing Strong Empirical Research in Sustainability Management—Addressing the Intersection of Theory, Method, and Empirical Field. *Frontiers in Sustainability*, *1*, 617870.

Sharma, M., Kandasamy, I., & Kandasamy, V. 2021. Deep Learning for predicting neutralities in Offensive Language Identification Dataset. *Expert Systems with Applications*, 185: 115458.

Shin, D.-H. (2017). Conceptualizing and measuring quality of experience of the internet of things: Exploring how quality is perceived by users. *Information & Management*, *54*(8), 998–1011. https://doi.org/10.1016/j.im.2017.02.006

Sinclair, D. (1997). Self-Regulation Versus Command and Control? Beyond False Dichotomies. *Law & Policy*, *19*(4), 529–559. https://doi.org/10.1111/1467-9930.00037

Steurer, R. (2013). Disentangling governance: A synoptic view of regulation by government, business and civil society. *Policy Sciences*, *46*(4), 387–410. https://doi.org/10.1007/s11077-013-9177-y

Stix, C. 2021. Actionable Principles for Artificial Intelligence Policy: Three Pathways. *Science and Engineering Ethics*, 27(1). https://doi.org/10.1007/s11948-020-00277-3

Sukhpal Singh Gill, Xu, M., Patros, P., Wu, H., Kaur, R., et al. 2023. Transformative effects of ChatGPT on modern education: Emerging Era of AI Chatbots. *Transformative Effects of ChatGPT on Modern Education: Emerging Era of AI Chatbots*, 4. https://doi.org/10.1016/j.iotcps.2023.06.002

Sun, S., Luo, C., & Chen, J. 2017. A review of natural language processing techniques for opinion mining systems. *Information Fusion*, *36*: 10–25.

Talanquer, V. (2023). Interview with the Chatbot: How Does It Reason? *Journal of Chemical Education*, *100*(8), 2821–2824. https://doi.org/10.1021/acs.jchemed.3c00472

Tan, K. L., Lee, C. P., Lim, K. M., & Anbananthen, K. S. M. 2022. Sentiment Analysis With Ensemble Hybrid Deep Learning Model. *IEEE Access*, 10: 103694–103704.

Van Berkel, N., Hosio, S., & Skov, M. 2020. *A Systematic Assessment of National Artificial Intelligence Policies: Perspectives from the Nordics and Beyond*, 20. https://doi.org/10.1145/3419249.3420106

Verplanken, B., & Sato, A. (2011). The Psychology of Impulse Buying: An Integrative Self-

Regulation Approach. *Journal of Consumer Policy*, *34*(2), 197–210. https://doi.org/10.1007/s10603-011-9158-5

Wallace, R. S. (2009). The Anatomy of A.L.I.C.E. In R. Epstein, G. Roberts, & G. Beber (Eds.), *Parsing the Turing Test* (pp. 181–210). Springer Netherlands. https://doi.org/10.1007/978-1-4020-6710-5_13

Wang, Y., Chen, Q., Hong, T., & Kang, C. 2019. Review of Smart Meter Data Analytics: Applications, Methodologies, and Challenges. *IEEE Transactions on Smart Grid*, *10*(3): 3125–3148.

Warner, K. S. R., & Wäger, M. 2018. Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, *52*(3): 326–349.

Xing, X., Song, M., Duan, Y., & Mou, J. (2022). Effects of different service failure types and recovery strategies on the consumer response mechanism of chatbots. *Technology in Society*, *70*, 102049. https://doi.org/10.1016/j.techsoc.2022.102049

Xiong, K., & Perros, H. (2009). Service Performance and Analysis in Cloud Computing. *2009 Congress on Services - I*, 693–700. https://doi.org/10.1109/SERVICES-I.2009.121

Yadav, A., & Vishwakarma, D. K. (2019). Sentiment analysis using deep learning architectures: a review. *Artificial Intelligence Review*, *53*(6): 4335–4385.

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated Machine Learning. *ACM Transactions on Intelligent Systems and Technology*, *10*(2): 1–19.

Yeung, K., & Bygrave, L. A. 2021. Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. *Regulation & Governance*. https://doi.org/10.1111/rego.12401

Yenkikar, A., Babu, C. N., & Hemanth, D. J. (2022). Semantic relational machine learning model for sentiment analysis using cascade feature selection and heterogeneous classifier ensemble. *PeerJ Computer Science*, 8: e1100.

Zhang, B., & Dafoe, A. (2020). U.S. Public Opinion on the Governance of Artificial Intelligence. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society. https://doi.org/10.1145/3375627.3375827

Zheng, P., wang, H., Sang, Z., Zhong, R. Y., and Liu, Y. (2018). Smart manufacturing systems for Industry 4.0: Conceptual framework, scenarios, and future perspectives. *Frontiers of Mechanical Engineering*, *13*(2): 137–150.

Human and organisational factors influencing the preparedness of small and medium-sized enterprises against cyber attacks in developing countries

Lucia Palacios Moya
Estudiante de Doctorado en Administración, Centro de Investigación Institución Universitaria Escolme

Maria Camila Bermeo Giraldo
Magíster en Ingeniería Administrativa, Instituto Tecnológico Metropolitano

John Alexander Arenas Lozano
Administrador Tecnológico, Facultad de Ciencias Económicas y Administrativas, Instituto Tecnológico Metropolitano

Alejandro Valencia Arias

Vicerrectoría de Investigación y postgrado, Universidad de Los Lagos, Chile

Paula Andrea Rodríguez-Correa
Administradora Tecnológica - Magister en Gestión de la Innovación Tecnológica, Cooperación y Desarrollo Regional, Universidad Ricardo Palma

Abstract: Small and medium-sized enterprises (SMEs) are highly vulnerable to cyber attacks such as phishing, ransomware, denial-of-service, malware, and Trojans that pose severe risks to organisations and the global economy. Despite the growing threat, research on cyber attacks in SMEs remains limited. This study examines factors associated with organisational preparedness against cyber attacks in SMEs within a developing country. A quantitative approach was employed, collecting 112 surveys analysed via SmartPLS 4 using Partial Least Squares Structural Equation Modelling (PLS-SEM). Results reveal that 33% of SMEs have faced cyber attacks, with human talent and resources identified as the most influential factors. The study also highlights the critical role of cyber awareness, supplier relationships, and overall cybersecurity preparedness. These findings offer practical guidance for SMEs, the education sector, and policymakers to enhance resilience. By addressing the research gap, this work contributes to understanding information security challenges for small businesses in emerging economies.

http://doi.org/10.18080/jtde.v13n3.1197

Keywords: Cyber Attack, Computer Intrusion, Cybersecurity, Security Challenges, Human Talent.

Introduction

The prevalence of cyber threats and attacks has increased significantly in the contemporary, interconnected world, affecting the security of information systems in organisations of all sizes and sectors (Thakur, 2024). As posited by Wilson et al. (Wilson *et al.*, 2023), the objective of a cyber attack is to exploit vulnerabilities in an organisation's computer systems or technological infrastructure. This is done with the intention of causing harm through criminal techniques such as unauthorised access, espionage, extortion, theft of data or financial information, and sabotage of assets and physical products. The fraudulent strategies and cybercrimes that are perpetrated are in a state of constant evolution in line with technological advancement. Consequently, the security of existing information systems is inadequate for the assessment of vulnerability in both physical and digital spaces.

The occurrence of cyber attacks has the potential to inflict considerable economic harm, resulting in substantial financial losses, data exposure, reputational damage, and a loss of customer trust. The escalating costs associated with cyber attacks are a matter of particular concern, as they may prompt consumers to exercise caution when engaging with affected companies. As reported by the Federal Bureau of Investigation (FBI) in 2022, the number of cyber attacks reported decreased, yet the victims suffered record losses of approximately $10.3 billion. This emphasises the necessity for enhanced cybersecurity measures to avert such occurrences in the future. The most frequently reported cybercrime is phishing, with corporate email breaches resulting in losses amounting to $2.7 billion. As forecast by Cybersecurity Ventures (Morgan, 2023), the global cost of cyber attacks is expected to reach $10.5 trillion annually by 2025.

The financial implications of cyber attacks can be particularly significant for small and medium-sized enterprises (SMEs), which may face costly recovery processes and legal consequences. It is widely acknowledged that SMEs play a pivotal role in the global economy, representing the majority of companies worldwide. However, they are also increasingly susceptible to cyber attacks that have the potential to compromise their operational stability and security. SMEs are susceptible to cybercriminal activity due to their limited resources. This business segment allocates a smaller proportion of its budget to cybersecurity compared to larger companies, resulting in less robust and effective solutions. Furthermore, there is a shortage of specialised cybersecurity personnel on these platforms. Similarly, relying on external providers or third parties for IT services, data management, and cloud storage

http://doi.org/10.18080/jtde.v13n3.1197

increases the risk of information security breaches and the compromise of the company's privacy.

Consequently, there has been a notable increase in interest within the academic community in the development of studies that seek to enhance the protection of organisations and their clients against potential violations, financial losses, or damage to their reputation. Consequently, cybersecurity in SMEs has emerged as a pivotal area of investigation. Despite the extensive documentation of organisational vulnerability to cyber attacks, a notable deficit persists in our comprehension of the specific factors that contribute to susceptibility to these threats in SMEs in emerging economies.

A number of studies have indicated that SMEs are frequently inadequately equipped to respond to cyber threats. In this regard, Renaud & Ophoff, (2021) emphasise the necessity for further research to be conducted on this particular segment, while Poehlmann *et al.*, (2021a) identify human error as the most significant factor in defending against cyber attacks. For instance, inadequate password management represents a prevalent factor in the occurrence of such attacks in SMEs. This highlights the necessity for the implementation of self-care policies and more robust security strategies, such as the utilisation of strong passwords and their regular updating (Alharbi *et al.*, 2021).

In other words, human capital is a crucial element in the cybersecurity of SMEs. In this context, Chikwendu & Oli (2023) relate it to the set of skills, knowledge and attitudes of employees that are required to prevent, detect and respond to cyber threats. As posited by Carlton *et al.*, (2019), comprehensive cybersecurity training serves to enhance employee comprehension of the risks associated with cyber attacks, whilst simultaneously equipping them with the requisite skills to recognise and report suspicious activity. As evidenced by studies such as Kemper (2019) and Wong *et al.*, (2022a), factors such as a culture of cyber awareness and ongoing employee training are crucial for organisations to act proactively and significantly reduce the vulnerability of SMEs. Research such as that conducted by Alharbi *et al.* (2021) and Quader & Janeja (2021a) has explored various aspects of human talent in cybersecurity, although it has focused on developed country contexts.

It is therefore imperative that research be conducted into the field of cybersecurity and the vulnerabilities of organisations, particularly in the case of SMEs, which are often at a disadvantage in the market. It is crucial to ascertain the requisite elements for safeguarding organisational security, fostering awareness and self-care, and mitigating the economic consequences of cyber attacks. In order to address this issue, this research aims to examine the human and organisational factors that association the preparedness of small and medium-sized enterprises against cyber attacks in developing countries, using structural equation

http://doi.org/10.18080/jtde.v13n3.1197

modelling. In particular, this study will analyse how factors such as cyber awareness, human talent, available resources and relationships with suppliers impact the ability of organisations to respond to cyber threats. The results will also contribute to an understanding of the behaviour of this business segment in the face of constant attacks that breach their online security, identify the constraints faced by SMEs in implementing effective cybersecurity strategies and propose practical solutions adapted to resource-constrained environments.

This study makes a contribution to the existing body of knowledge regarding the factors that can association the preparation of small and medium-sized enterprises (SMEs) for cyber attacks, with the aim of preventing business disruptions and maintaining the confidence of customers and internal employees. These findings also highlight the significance of designing and implementing preparedness plans in response to attacks in the contemporary digital context for practitioners, experts, and academics alike. Consequently, the findings of this study offer pertinent recommendations for government policymakers seeking to safeguard citizens, businesses, and national interests in the context of mounting cyber threats. It is imperative that anticipatory and adaptive policies be implemented in order to address the constantly evolving threats that are inherent to the digital and technological environment. Furthermore, by focusing on a developing country, this study makes a significant contribution to the existing literature on cybersecurity, which has predominantly been conducted in developed country contexts. Consequently, this paper not only contributes to the advancement of academic knowledge but also provides actionable insights for the enhancement of the cyber resilience of SMEs in emerging economies.

This study is developed in Colombia. The Colombian context presents distinctive institutional, economic, and cultural characteristics that may relationship cybersecurity preparedness factors differently than in developed countries. Colombian SMEs operate under more severe resource constraints compared to their counterparts in developed nations (Development Bank of Latin American and The Caribbean, 2023). Limited access to capital and technology infrastructure means that the resources factor may have a disproportionate association on cybersecurity preparedness (Díaz & de Jesus, 2023). Additionally, the prevalence of informal business practices and cash-based transactions in developing economies (de Jesus *et al.*, 2025) creates different risk profiles and security priorities.

Colombia's cybersecurity regulatory framework reflects a gradual development process that, while showing progress in establishing legal instruments to address cybercrime, remains less mature than those found in developed countries, particularly regarding government support programs specifically targeting SME cybersecurity. In response to the serious global cybercrime situation and Colombia's high vulnerability to cyber threats, the country has been progressively working to develop policies, regulatory frameworks, administrative acts, and

http://doi.org/10.18080/jtde.v13n3.1197

legal instruments that incorporate cybercrime into legislation to strengthen judicial, constitutional, criminal, and sanctionary processes. However, despite these ongoing efforts to build a broader legal framework, the practical implementation of comprehensive support mechanisms for small and medium enterprises' cybersecurity preparedness continues to lag behind the standards observed in more developed economies (Ospina & Sanabria, 2020).

On the other hand, Vulnerability to cyber attacks is not limited to technological failures but is also closely linked to human behaviour. In Colombia, a significant share of cyber attacks target weaknesses associated with individuals' behaviour within organisations. Therefore, it is crucial to foster a cybersecurity culture that enables employees to internalise and adopt appropriate behaviours, thereby strengthening the organisation's protection against digital threats (Sánchez, *et al.*, 2023).

The following section outlines the structure of this paper. The initial section presents the model and the proposed hypotheses. The second section outlines the methodology and design of the instrument employed. The third section presents the findings of the study. The fourth section presents the findings of the article. In conclusion, the fifth section presents the study's conclusions, practical implications and limitations.

Literature review

Organisational readiness and cybersecurity challenges in SMEs in developing countries

The diversity of industries and sizes that comprise the SME business sector makes it particularly vulnerable to cyber attacks, which present a multitude of difficulties and challenges. This business segment, comprising micro, small and medium-sized enterprises, is the most diverse in terms of both structure and operational context. It is therefore particularly vulnerable to a range of challenges in the protection of its information and IT systems. The vulnerability of SMEs varies depending on a number of factors, including their size, the sector in which they operate and their ability to implement protective measures.

While an SME in the technology sector may have advanced cybersecurity infrastructures and the requisite resources to implement them, a microenterprise with less than ten employees, or one in the traditional manufacturing sector, often lacks the necessary resources and expertise to deal with cyber attacks (Quader & Janeja, 2021a). This disparity in capabilities renders SMEs more vulnerable to attacks that can result in significant financial losses, the destruction of valuable information, and system failures (Alarifi, 2023a). In developing countries, where SMEs have more vulnerable critical infrastructures, the issue is further compounded by low cybersecurity awareness and a lack of adequate protection policies. The utilisation of wireless

http://doi.org/10.18080/jtde.v13n3.1197

technologies in the absence of robust security measures and a lack of awareness regarding cyber threats serves to exacerbate the inherent risks within this business sector (Aslan *et al.*, 2023).

In accordance with the findings of George *et al.* (2024), a lack of preparedness and absence of preventive practices against cyber attacks, such as the implementation of timely software updates, insufficient protection against malware and reliance on mobile devices with vulnerable passwords, in conjunction with the widespread use of unlicensed software and a lack of employee awareness of cyber risks, serve to exacerbate the situation in SMEs (Kemper, 2019). Furthermore, these companies adopt technologies without adequately prioritising the management of cyber risks. For instance, Nagahawatta *et al.* (2021) discovered that small and medium-sized enterprises (SMEs) employ cloud computing solutions, yet frequently underestimate the associated challenges pertaining to data security and privacy. This emphasises the crucial necessity for the establishment of a comprehensive cybersecurity framework for these organisations.

In contexts where resources are scarce, SMEs frequently lack the capacity to invest in sophisticated cybersecurity measures, leaving them vulnerable to a range of risks, including phishing, ransomware, and identity theft (Aslan *et al.*, 2023). Furthermore, the prevalence of SIM swap fraud and distributed denial of service (DDoS) attacks has increased alongside the expansion of internet access and the weakening of IT infrastructures.

In light of the mounting risks confronting SMEs in developing countries, it is imperative that these organisations formulate efficacious strategies to enhance their resilience to cyber attacks. Consequently, the establishment of a culture of cybersecurity and cyber awareness within the company, accompanied by the provision of ongoing training for employees, is of paramount importance in order to enhance awareness of potential threats and to mitigate the risk of human error (Chang & Coppel, 2020a). Furthermore, the implementation of regular security audits and the adoption of advanced tools, such as multi-factor authentication and data encryption, is imperative for the protection of the most sensitive assets (Polkowski & Dysarz, 2017). The existence of an incident response plan enables companies to act expeditiously and effectively, thereby mitigating the impact of any attack. Collectively, these practices reinforce organisational preparedness and diminish the vulnerability of SMEs to mounting cybersecurity challenges, ensuring the safeguarding of their resources and the continuity of their operations in an increasingly perilous digital environment (Nsoh, 2021).

http://doi.org/10.18080/jtde.v13n3.1197

Background on factors influencing organisational readiness in cyber attacks

From the perspective of organisations, the implementation of cybersecurity measures has been explained through a variety of theoretical frameworks that seek to elucidate the underlying motivations and processes driving the adoption of these practices. The preparedness of companies in the face of cyber attacks and the adoption of cybersecurity measures have been the subject of extensive study from a variety of theoretical perspectives.

On the one hand, some studies have analysed the security of technological infrastructure in sectors such as e-commerce and small and medium-sized enterprises (SMEs), placing special emphasis on the online behaviour of users. It has been demonstrated that users with limited technical expertise tend to rely on the reputation of websites, their interactions with them, and third-party recommendations as a means of ensuring their online security (Mohamad *et al.*, 2022; Ramayah *et al.*, 2016). Furthermore, demographic factors, usage patterns, and previous experiences with technological devices have been identified as influencing risk perception when using the Internet (Bhatti *et al.*, 2021).

With regard to organisations, the adoption of technological solutions in the field of cybersecurity has also been the subject of study. For instance, (Bhatti *et al.*, 2021) posit that sophisticated techniques such as natural language processing (NLP) and artificial intelligence can enhance efficiency in security management. Similarly, the Diffusion of Innovations Theory, as proposed by (Rogers, 2003), suggests that the decision to implement these technologies is dependent on factors such as relative advantage, compatibility, complexity, testability and observability of perceived benefits. In this context, technologies such as artificial intelligence, big data, blockchain, and machine learning have been proposed as means of detecting and minimising security risks in organisations. Furthermore, secure protocols and electronic transaction systems have been developed with the objective of reducing security concerns and optimising communication costs.

Conversely, the Theory of Planned Behaviour (Ajzen, 1991) posits that an organisation's intention to implement security measures to safeguard its information systems is shaped by three key factors: attitudes towards security, perceived social pressure, and control over the necessary resources. This has been corroborated by recent studies such as that conducted by Hasani et al. (Hasani *et al.*, 2023) in SMEs, which concluded that the availability of financial and technical resources, along with threat perception, are pivotal factors that determine the adoption of cybersecurity measures and organisational preparedness, particularly in developed economies (Kabanda *et al.*, 2018).

http://doi.org/10.18080/jtde.v13n3.1197

While some studies have examined the security of technology infrastructure in sectors such as e-commerce, the majority of the literature has focused on online user behaviour. Consequently, it has been observed that users with limited technical knowledge rely on website reputation and third-party recommendations to ensure their online security. However, further research is required to gain a deeper understanding of the security behaviour of companies and their vulnerability to cyber attacks.

Hypothesis and proposed model

In light of the findings of the literature review, on cybersecurity studies in the organisational context, the following hypotheses have been formulated with a view to analysing the factors that are associated with the preparedness of SMEs in developing countries in the context of cyber attacks. Although these hypotheses are based on previous studies, they have been adapted to reflect the particularities of this study, resulting in the following proposition: The variables that explain the level of preparedness of these organisations in cybersecurity are human talent, cyber awareness, resources and relationships with suppliers. Table 1 also presents the definitions of the proposed factors and the studies that provide evidence to support each one.

Table 1: Literature review of factors influencing the preparedness of SMEs organisations in the face of cyber attacks.

Factor	Description	Reference
Human talent	Extent to which staff attitudes may linkage the likelihood of a cyber attack.	(Poehlmann et al., 2021b; Quader & Janeja, 2021b)
Cyber Awareness	Extent to which knowledge about cybersecurity can linkage the implementation of practices to avoid the risk of cyber attack.	(Chang & Coppel, 2020b; Realpe & Cano, 2020)
Resources	Physical, technological, and financial resources necessary to protect the organisation from cyber attacks.	(Saz Dones, 2022; Tam et al., 2021a)
Relationship with Suppliers	Collaboration and type of interactions between suppliers of products or services and companies, which may compromise information.	(Cano, 2022; Wong et al., 2022b)

http://doi.org/10.18080/jtde.v13n3.1197

Organisational Cybersecurity Preparedness	An organisation's ability to prevent, detect, respond to, and mitigate potential cyber attacks.	(Alarifi, 2023b; Blanco Esteban, 2022)

The willingness of employees to adopt new cybersecurity strategies and their awareness of the importance of using strong passwords reflect an understanding that fosters the protection of company information. Awareness of computer security risks entails a proactive stance towards threat prevention. The cybersecurity human talent, defined as the collective set of skills, knowledge, and competencies of employees in the prevention, detection, and response to cyber threats, is a pivotal element in this process. As (Klein & Zwilling, 2024) observe, employee involvement in cybersecurity training and educational programs serves to reinforce this cyber awareness, thereby engendering a workforce that is better prepared and more committed to the digital security of the organisation. (Fonseca-Herrera *et al.*, 2021) posit that the cultivation of cyber awareness among employees can enhance the capacity of SMEs to confront and mitigate the risks associated with cyber attacks, thereby establishing a preventive approach to computer security management. In other words, when employees possess greater awareness of cyber risks, they are better equipped to develop the requisite skills to protect the organisation. In light of the aforementioned evidence, the following hypothesis is put forth for consideration:

H1: There is a positive correlation between cyber awareness and human talent.

As Sánchez & Batista (2023) have pointed out, having resources available is important because it influences how small and medium-sized enterprises (SMEs) respond to cyber attacks and cybersecurity challenges. These resources include both financial and technological assets that the organisation can allocate to IT security, such as budgets for protection software, specialised hardware, and staff training programs (Chidukwani et al., 2024). The availability of these resources improves the level of cyber awareness within the organisation, as it facilitates understanding of the risks associated with cybercrime and access to technologies that prevent attacks (Chang & Coppel, 2020a). Consequently, it can be inferred that when an organisation has greater resources, it is in a better position to promote cybersecurity practices among its employees, strengthening the organisational culture in this area.

H2: There is a positive relationship between the resources available in the organisation and the level of cyber awareness.

It is possible for companies to allocate both financial and technological resources with the objective of enhancing their cybersecurity. (Armenia *et al.*, 2021) posit that an adequate

http://doi.org/10.18080/jtde.v13n3.1197

budget in this area allows organisations to invest in preventive and corrective measures, thereby enhancing their capacity to respond to potential threats. Furthermore, the implementation of transparent and up-to-date cybersecurity policies, when coupled with the company's prioritisation of this aspect, serves to foster a security culture within the organisation. The implementation of well-structured protocols and procedures to mitigate cyber attacks ensures that SMEs are better prepared to respond to online incidents. Therefore, the availability of adequate financial and technological resources markedly enhances the company's capacity to safeguard itself against digital threats. The following hypothesis is formulated based on the considerations:

H3: There is a positive correlation between the resources available to an organisation and its level of cybersecurity preparedness.

The provision of adequate resources within a company facilitates the implementation of more effective cyber protection measures. This, in turn, improves the confidence and credibility perceived by suppliers (Heidt *et al.*, 2019). Wolden *et al.* (2015) argue that building close, collaborative relationships with suppliers enables more secure information sharing and protects the supply chain from potential cyber attacks. This proactive, collaborative approach to cybersecurity responds to the business environment challenges faced by SMEs. Thus, organisations that demonstrate a serious commitment to digital security and have the necessary resources to support their operations are more highly valued by their suppliers. In this sense, having financial, technological, and human resources not only strengthens internal protection but also allows for the establishment of stronger and more secure relationships with suppliers, promoting joint investment in cybersecurity measures that benefit both parties.

H4: There is a positive relationship between the resources available in the organisation and the quality of the relationship with suppliers.

Similarly, resources are vital for organisations seeking to expand their workforce and attract professionals with specific skillsets, including expertise in risk assessment and cybercrime (Parker & Brown, 2019). Furthermore, organisations with greater resources are able to invest in training and professional development, thereby enhancing their preparedness for potential threats, improving their response and mitigation capabilities, and ensuring effective cyber defence for SMEs. Consequently, the greater the resources an SME has at its disposal in the field of cybersecurity, the more effectively it will be able to attract, retain and develop human talent with the requisite specialisation. In light of the above, we put forward the following hypothesis:

http://doi.org/10.18080/jtde.v13n3.1197

H5: There is a positive relationship between resources and human talent.

As Pyke *et al.*, (2021) have observed, the greater the knowledge and training received by human talent in terms of cybersecurity, the greater the effectiveness of the organisation in preventing, detecting and responding to possible cyber attacks. Moreover, a team of employees dedicated to the company's digital security can markedly enhance the organisation's protection measures and protocols, thereby ensuring business continuity and mitigating the risks associated with cybercrime in SMEs (Nyarko & Fong, 2023). This is significant because it is human beings who can relationship the formulation of transparent computer security policies and the provision of ongoing training on cybersecurity issues. Such measures can empower employees to act responsibly and safely when handling information, thereby reducing the vulnerability of the company to attacks. In light of the aforementioned evidence, the following hypothesis is proposed:

H6: There is a positive correlation between human capital and organisational cybersecurity preparedness.

In light of the aforementioned considerations, the proposed model and hypotheses are presented in Figure 1. The latent variable is defined as the level of preparedness of SMEs against cyber attacks. The observable variables are factors that exert a direct relationship on the latent variable, including: The aforementioned factors are as follows: human talent, cyber awareness, resources, and relationships with suppliers.

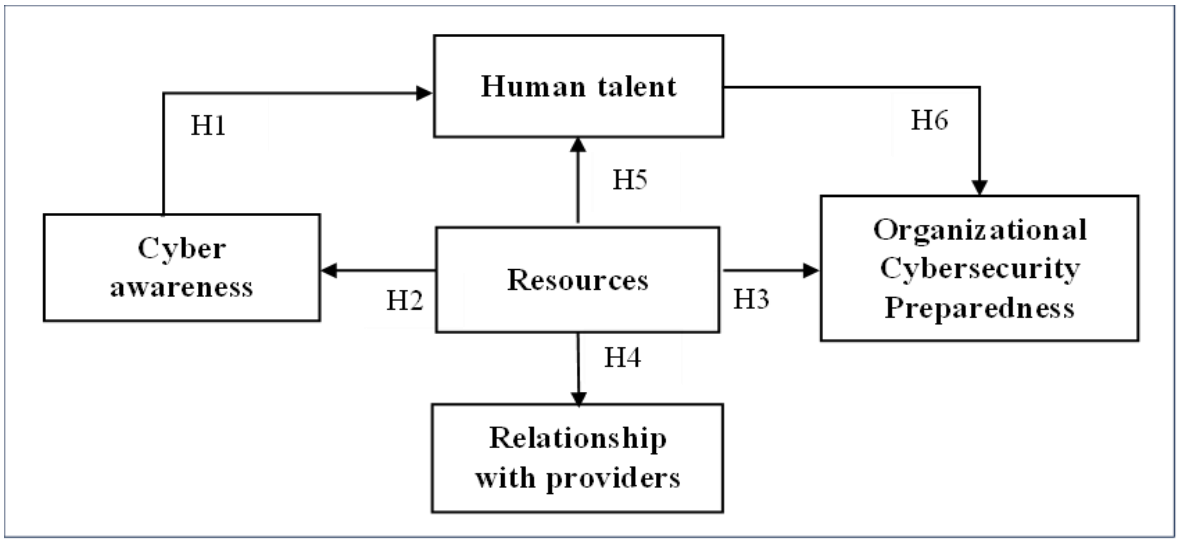


Figure 1: Proposed model of factors influencing the preparedness of SMEs against cyber attacks.

Methodology

A research study was designed with an exploratory and inferential quantitative approach in order to achieve the objective. The study employed a structural equation model (SEM), which

http://doi.org/10.18080/jtde.v13n3.1197

was empirically validated through the administration of a self-report questionnaire. Accordingly, the study is correlational in scope. The target population comprised small and medium-sized enterprises (SMEs) based in the city of Medellín, Colombia. Consequently, the individuals responsible for completing the survey were those occupying leadership roles within the organisations in question. The objective of this study is to validate a model proposed from a theoretical background and tested experimentally with SME decision-makers using a statistical technique focused on prediction.

The data was gathered via a survey distributed to 112 participants employed in SMEs within the products and services sector, situated in Medellín, Colombia. The study participants were selected using a non-probability convenience sampling method (Tobi & Kampen, 2018). This method was based on the ease of access to the source of information and entailed the selection of willing participants who met the specified criteria. The criteria for participation included being over the age of 18, having a minimum of six months' work experience in the company, and occupying a position that involved the use of information and communication technologies. The confidentiality and anonymity of the participants were upheld throughout the data collection and analysis process.

Instrument development

The questionnaire was structured into three sections. The first part addressed participants' perceptions of cyber threats in SMEs, including their knowledge of attacks suffered, access to confidential information, and the most common types of threats. The second part focused on the protection mechanisms implemented by companies, such as password updates or security policies in communication channels. The third part measured the main constructs analysed in the study: human talent, cyber awareness, organisational resources, and supplier relationships.

The questionnaire was structured into three sections. The first part addressed participants' perceptions of cyber threats in SMEs, including their knowledge of attacks suffered, access to confidential information, and the most common types of threats. The second part focused on the protection mechanisms implemented by companies, such as password updates or security policies in communication channels. The third part measured the main constructs analysed in the study: human talent, cyber awareness, organisational resources, and supplier relationships.

Although the questionnaire is original, its development was based on empirical findings reported in previous studies on cybersecurity in SMEs, as summarised in Table 2. All items were evaluated using a five-point Likert scale (1 = strongly disagree to 5 = strongly agree), following the structure proposed by Rezaei *et al.* (2020). Likewise, and in accordance with the

http://doi.org/10.18080/jtde.v13n3.1197

methodological recommendations of Bagozzi & Heatherton (1994), each construct was measured with a minimum of three and a maximum of five items, ensuring the reliability and validity of the instrument.

Subsequently, a professional with experience in cybersecurity consulting for SMEs reviewed the questionnaire to assess its relevance and clarity. A pilot test was then conducted with a sample of ten employees and managers from SMEs located in Medellín, Colombia, who met the study's inclusion criteria. Participants were asked to complete the questionnaire and provide feedback on the clarity, relevance, and ambiguities of the questions. Based on these two reviews, minor adjustments were made to both the wording of the items and the general instructions of the instrument. This process ensured that the questionnaire was conceptually sound and contextualised for application in companies in developing countries.

Table 2: Questionnaire items used in the study.

Construct	Measured items		Reference
Human talent	TAH1	I feel that in my company the computer security policies to avoid cyber attacks are clear.	(Poehlmann et al., 2021b; Quader & Janeja, 2021b)
	TAH2	Continuous staff training on cybersecurity is essential to reduce SMEs' vulnerability to attacks.	
	TAH3	I exhibit responsible and secure behaviour in managing information and preventing cyber- attacks.	
	TAH4	I am able to identify potential cyber attacks, such as suspicious emails or requests for confidential information.	
Cyber awareness	COC1	If the company implements new cybersecurity strategies, I am willing to adopt them.	(Chang & Coppel, 2020b; Realpe & Cano, 2020)
	COC2	I understand the importance of using strong passwords and changing them regularly to protect my company's information.	
	COC3	I consider myself aware of the computer security risks that the company may suffer.	
	COC4	You would attend training and education to learn about how to protect against potential cyber attacks.	
Resources	REC1	There are updated tools and technologies to detect and prevent cyber attacks on the organisation.	(Saz Dones, 2022; Tam

http://doi.org/10.18080/jtde.v13n3.1197

	REC2	There is an adequate cybersecurity budget to invest in preventive measures and corrective solutions.	et al., 2021a)
	REC3	The organisation provides equipment and devices with adequate security measures to prevent possible cyber attacks.	
	REC4	The organisation has trained and specialised personnel to deal with possible threats and attacks.	
Relationship with suppliers	RCP1	There are strong confidentiality policies within the company that ensure the security of third-party information.	(Cano, 2022; Wong et al., 2022b)
	RCP2	The organisation monitors suppliers in terms of cybersecurity before establishing business relationships.	
	RCP3	Staff are informed of the measures necessary to safeguard supplier information.	
	RCP4	The organisation has mechanisms to communicate and share relevant information about cyber threats and vulnerabilities with suppliers.	
Organizational Cybersecurity Preparedness	ORG1	The organisation is prepared because it has clear and up-to-date cybersecurity policies in place.	(Alarifi, 2023b; Blanco Esteban, 2022)
	ORG 2	The company gives the importance it deserves to computer security.	
	ORG 3	There are established protocols and procedures for the detection, response, and mitigation of cyber attacks in the organisation.	
	ORG 4	Staff are constantly trained to prevent cyber attacks.	

Collection and processing of information

Following the collection of data through the survey, an analysis was conducted using the proposed model, specifically the Partial Least Squares Structural Equation Modelling (PLS-SEM) technique. Huang (2021) posits that PLS-SEM is a superior technique to the General Linear Structural Relationship Model for the development of predictive models and the

http://doi.org/10.18080/jtde.v13n3.1197

examination of causality between latent variables, particularly in exploratory research and social sciences.

In other words, PLS-SEM is employed to ascertain significant and bidirectional causal relationships between variables of interest, rendering it an appropriate instrument for the construction of theoretical models (Tobi & Kampen, 2018). This study employed the Partial Least Squares Structural Equation Modelling (PLS-SEM) technique to investigate the interrelationships between the following variables: Cyber Awareness, Human Talent, Organisational Resources, Organisations, and Relationship with Suppliers. The study employed the PLS algorithm and bootstrapping to obtain path coefficients and ascertain their significance through 5,000 repetitive iterations utilising the SmartPLS 4 program (Becker *et al.*, 2023).

The PLS-SEM is a more appropriate technique for analysing smaller samples than the Covariance-based Structural Equation Model (CB-SEM), which is evaluated using the covariance matrix (Hair *et al.*, 2017). Lee *et al.* (2011) posit that the sample size for PLS should be a minimum of ten times that of the majority of the question items. In this study, the majority of questions comprise four items, thereby necessitating a minimum sample size of 40. The sample size employed in this study was 112, which fulfils the requisite minimum.

The Ethics Committee of the ESCOLME University Institution has issued a report on the research project entitled 'Factors Influencing Cyber Attacks'. The research project entitled 'A Quantitative Analysis in Small and Medium Enterprises in a Developing Country' was approved on the condition that it complied with the standards set forth in Resolution 8430 of 1993 and Resolution 2378 of 2008. Furthermore, the project was required to align with the institutional values outlined in the Institutional Educational Project, including transparency, equity, justice, responsibility, righteousness, and inclusion. In accordance with Articles 15 and 16 of Resolution 08430 of 1993, informed consent is a prerequisite. The participants were furnished with a comprehensive information document that elucidated the objectives, procedures, potential risks, and anticipated benefits of the study, as well as their rights as research participants. The document was provided in advance of the research, and participants were given sufficient time to read and digest its contents. Any queries or concerns were addressed in a comprehensive and transparent manner.

Once the participants had been furnished with the requisite information and had consented to participate, they signed an informed consent form. This document provided a summary of the information presented in the information document and confirmed the participants' explicit consent to participate in the study. The confidentiality of participants' personal data was safeguarded through the implementation of rigorous anonymisation procedures at all

http://doi.org/10.18080/jtde.v13n3.1197

stages of the research process. This research is classified as having no risk, as it employs research methods that do not involve intervention or intentional modification of biological, physiological, psychological, or social variables of the individuals who will participate in the study. The recruitment period for this study was from June to August 2023. The approval code is ACTA 02, dated 10042023.

Analysis of results

The initial two sections of the survey were designed to ascertain respondents' knowledge and perception of the vulnerability of SMEs to cyber attacks. Table 3 presents the frequency distribution of the collected data, indicating that despite the presence of security policies, vulnerabilities are present among the 112 SME employees. Specifically, 35.7% of respondents indicated that they were unaware of the occurrence of cyber attacks, 33% confirmed that such attacks had taken place, and 31.3% denied that any attacks had occurred. Furthermore, 62.5% of the respondents have access to confidential information, which increases the risk, this result highlights the need to implement robust access control mechanisms, such as Role-Based Access Control (RBAC), which restricts access to confidential information strictly to authorised personnel according to their organisational roles. The cyber threats identified by the SMEs under study include phishing (81%), as Sharma *et al.* (2022) emphasise, the efficacy of anti-phishing strategies is considerably augmented when organisations implement multi-layered defence mechanisms, such as heuristic-based filters, machine learning detection models, and real-time blacklisting. Furthermore, the implementation of simulation tools and phishing awareness campaigns is of paramount importance in the enhancement of human factors. These tools effectively expose employees to realistic threat scenarios, thereby enhancing their ability to recognise and report malicious attempts. The incorporation of these technological and behavioural defence dimensions provides a more comprehensive framework for addressing phishing within cybersecurity preparedness models. PDF or Word scams (62%), malware (60%), fake antivirus software (54%), and tech support scams (44%).

As illustrated in Table 3, the results indicate that 60.7% of SMEs update their passwords to prevent unauthorised access to servers, while 39.3% do not implement this practice. Moreover, as illustrated in Table 3, 50% of companies have implemented security policies for their communication channels.

In terms of the technological devices used in the workplace, these are typically safeguarded against cyber attacks. The results indicate that 51.4% of respondents indicated that their devices are always protected, while 18% stated that this is almost always the case. Additionally, 10.8% of respondents indicated that their devices are sometimes protected, while 5.4% and 3.6% of respondents, respectively, indicated that their devices are rarely and never protected.

http://doi.org/10.18080/jtde.v13n3.1197

In light of these findings, the participants were queried as to whether they were aware of the appropriate contact for reporting a cyber attack. The results indicated that 57.1% of respondents were informed of the relevant contact, while 42.9% admitted to being unaware. This indicates a deficiency in employee awareness regarding the pertinent individuals within the relevant departments responsible for addressing such incidents, including the individual directly tasked with cybersecurity. As Deutrom et al., (2022), discuss, the SeBIS is particularly effective in measuring employees' security behaviours and intentions, providing a clear and reliable method for understanding how personal factors, such as life satisfaction or problematic internet use, association cybersecurity practices. The incorporation of such validated instruments into future research endeavours has the potential to enhance the accuracy of assessments of the relationship between employees' awareness of security practices and their actual security behaviours. This enhanced accuracy would offer a more profound insight into the factors that drive or hinder secure practices in the workplace.

Table 3: Results on knowledge of cyber attacks, access to information, and protection mechanisms in SMEs.

Knowledge about cyber attacks				
Have your SMEs experienced cyber attacks?			**Do you have access to confidential information?**	
Yes 33%	**No** 31.3%	**Unknown** 35.7%	**Yes** 62.5 %	**No** 37.5%
		Yes	**No**	**Maybe**
Phishing		81%	12%	7%
Fake antivirus software		54%	38%	8%
Tech Support Scams		44%	41%	15%
PDF or Word scams		62%	22%	16%
Malware		60%	28%	12%
Protection Mechanisms Employed by SMEs to Mitigate Cyber Attacks				
Do you update passwords?			**Do they use security channels and policies?**	
Yes 60.7%		**No** 39.3%	**Yes** 50%	**No** 50%
Technological devices commonly used in the workplace are typically safeguarded against cyber attacks.				
Always			51.4%	
Almost always			18%	
Sometimes			10.8	
Do not know not answer			10.8%	

http://doi.org/10.18080/jtde.v13n3.1197

Rarely		5.4%
Never		3.6%.
Do you know who they should contact in the event of a cyber attack?		
Yes 57.1%		**No** 42.9%

Measurement model evaluation

Two analyses were conducted using the SmartPLS 4 program to process the data. The initial analysis was conducted with the objective of ensuring the reliability and construct validity of the measurement model. The second analysis was conducted to assess the structural model and evaluate the hypotheses. In their study, Rožman et al., (2020) asserted that SmartPLS 4 is one of the most effective statistical calculation tools currently available. The software boasts an intuitive graphical user interface that facilitates the utilisation of analytical and graphical techniques based on partial least squares or component-based approaches.

The evaluation of the measurement model comprises an analysis of the construct's reliability, as well as an examination of its convergent and discriminant validity. The initial stage of the analysis entails an examination of the factor loadings of the indicators, which are the observable variables. It is advised that factor loadings (CL) be maintained at a minimum of 0.6 throughout the model (Amora, 2021). Furthermore, the analysis is supplemented with the values of the variance inflation factor (VIF), which serve to identify any potential issues with multicollinearity. The optimal value for each construct is less than 5, as proposed by (J. Hair et al., 2017).

In the same analysis, the average variance extracted (AVE) is estimated for each construct in order to evaluate the convergent validity. In accordance with the (Cheung & Wang, 2017) measure, the degree of convergence represents the extent to which the variability of the indicators is related to the underlying concept being measured. The calculation is performed by extracting the variance from all indicators that comprise the construct. An AVE value exceeding 0.5 typically signifies adequate convergence. The indicator exhibits more than 50% of its variability in the construct score.

The reliability of the constructs was evaluated using both the Composite Reliability Criterion (CR) and Cronbach's Alpha (CA). Cronbach's Alpha is regarded as a more conservative approach, as it gauges internal consistency in a relatively conservative manner, thereby establishing a lower limit of reliability. The CR represents an upper limit of reliability and is more permissive. In accordance with the instructions set forth by (Hair et al., 2019), values exceeding 0.7 were sought for both measures. As evidenced in Table 4, the presented results demonstrate that the measures of (CL), VIF, CA, CR, and AVE satisfy the established

http://doi.org/10.18080/jtde.v13n3.1197

parameters. It is noteworthy that all constructs exhibited a composite reliability exceeding 0.7, obviating the necessity for item elimination.

Table 4: Convergent validity and reliability of the measurement model

Factor	Item	Factor Loading	Variance inflation factor (VIF)	Cronbach's Alpha (CA)	Composite Reliability Criterion (CR)	Average Variance Extracted (AVE)
Human talent	TAH1	0.757	1.295	0.703	0.716	0.527
	TAH2	0.641	1.262			
	TAH3	0.750	1.569			
	TAH4	0.750	1.592			
Cyber awareness	COC1	0.841	2.361	0.873	0.883	0.722
	COC2	0.869	2.672			
	COC3	0.833	1.761			
	COC4	0.855	2.213			
Organisational Cybersecurity Preparedness	ORG1	0.836	2.114	0.898	0.900	0.766
	ORG2	0.898	3.352			
	ORG3	0.923	3.901			
	ORG4	0.841	2.188			
Resources	REC1	0.909	3.387	0.899	0.905	0.769
	REC2	0.808	1.894			
	REC3	0.888	2.645			
	REC4	0.899	3.133			
Relationship with suppliers	RCP1	0.816	1.821	0.869	0.869	0.719
	RCP2	0.839	2.083			
	RCP3	0.887	2.869			
	RCP4	0.849	2.341			

http://doi.org/10.18080/jtde.v13n3.1197

Source: own elaboration based on SmartPLS 4. Note: CL > 0.6; VIF < 5; CA > 0.7; CR > 0.7; AVE > 0.5.

In order to verify the discriminant validity, the approach proposed by Fornell and Larcker is employed. According to this approach, the square root of the average extracted variance (AVE) must be greater than the correlation of the construct against the other constructs. This standard is validated for all constructs, as evidenced by the data presented in Table 5. It can therefore be confirmed that the measurement model satisfies the requirements of discriminant validity.

Table 5: Discriminant validity of the measurement model

	Cyber Awareness	Organisational Cybersecurity Preparedness	Resources	Relationship with Suppliers	Human talent
Cyber Awareness	0.849				
Organisational Cybersecurity Preparedness	0.359	0.885			
Resources	0.396	0.846	0.977		
Relationship with Suppliers	0.408	0.834	0.868	0.848	
Human talent	0.703	0.693	0.704	0.663	0.726

Source: own elaboration based on SmartPLS 4.

Structural model evaluation

Once the measurement model has been validated, the subsequent phase of the analysis entails examining the hypotheses derived from the theory. The bootstrapping technique is employed in SmartPLS for the evaluation of causal relationships based on path coefficients (path value), T values, and p values. Similarly, the PLS-SEM framework employed the following metrics to validate the hypotheses: a path value exceeding 0.005, a T value exceeding 1.96 (with a 95% confidence level), and a p value less than 0.05 (Asis et al., 2020). Table 6 corroborates the findings pertaining to the six original hypotheses.

http://doi.org/10.18080/jtde.v13n3.1197

The employment of Partial Least Squares Structural Equation Modelling (PLS-SEM) in this study is particularly well-suited to the exploratory nature of the research and the complexity of the model, which involves multiple latent constructs and indicators. PLS-SEM has gained recognition for its efficacy in contexts where theoretical development remains in its nascent stages, sample sizes are modest, and the primary objective is prediction or theory building rather than theory testing (Hair et al., 2021). In this context, PLS-SEM allows for greater flexibility in estimating complex models and provides robust results even when data do not meet the stringent assumptions of covariance-based approaches. This methodological choice is strategically appropriate for exploring the relationships examined in the study.

Table 6: Hypothesis testing of the proposed model

	Vpath	T value	p-values	Acceptance
H1=Cyber Awareness -> Human Talent	0.504	7.669	0.000	Yes
H2=Resources -> Cyber Awareness	0.396	5.419	0.000	Yes
H3=Resources -> Organizational Cybersecurity Preparedness	0.729	11.019	0.000	Yes
H4=Resources -> Relationship with Suppliers	0.878	40.046	0.000	Yes
H5=Resources -> Human Talent	0.504	8.667	0.000	Yes
H6=Human Talent -> Organisational Cybersecurity Preparedness	0.180	2.616	0.009	Yes

Source: own elaboration based on SmartPLS 4. Note: Path > 0.005; T statistics > 1.96; p value < 0.05.

The evidence presented in Hypothesis H1 indicates a positive correlation between cyber awareness and human talent. With a p-value of 0.000, which is less than the significance level, the null hypothesis is rejected. The evidence is significant and suggests a positive relationship between cyber awareness and human talent. Hypothesis H2 suggests that resources exert a

http://doi.org/10.18080/jtde.v13n3.1197

positive association on cyber awareness. With a p-value of 0.000, which is less than the significance level, the null hypothesis is rejected.

It can therefore be concluded that there is sufficient evidence to support the assertion that there is a positive relationship between resources and cyber awareness.

Hypothesis H3 indicates that resources exert a positive relationship on human talent. With a p-value of 0.000, which is less than the significance level, the null hypothesis is rejected. The evidence is significant and suggests a positive relationship between resources and human talent. Hypothesis H4 indicates that resources exert a positive relationship on the relationship with suppliers. With a p-value of 0.000, which is less than the significance level, the null hypothesis is rejected.

It can therefore be concluded that there is significant evidence to suggest a positive relationship between resources and the relationship with suppliers.

With regard to hypothesis H5, it can be seen that there is a positive effect of resources on organisational cybersecurity preparedness. With a p-value of 0.000, which is less than the significance level, the null hypothesis is rejected.

Therefore, there is compelling evidence to suggest a positive relationship between resources and organisational cybersecurity preparedness.

In conclusion, hypothesis H6 suggests that human talent has a positive effect on organisational cybersecurity preparedness. With a p-value of 0.009, less than the significance level, the null hypothesis is rejected. Therefore, there is substantial evidence to suggest a positive correlation between human talent and organisational cybersecurity preparedness.

It can therefore be concluded that all the proposed hypotheses indicate the existence of valid relationships. There is a positive association between cyber awareness and human talent, which in turn is positively associated with the organisational factor.

There is a positive association between resources and human talent, as well as with the relationship with suppliers, the organisational factor and cyber awareness. Moreover, these relationships are corroborated by an examination of the coefficient of determination (R^2). The coefficient indicates the percentage of total variability in the response variable (endogenous variable) that can be explained by the predictor variables in the model. Subsequently, the coefficient is analysed in relation to the endogenous constructs. As illustrated in Figure 2, the variables of human talent, cyber awareness, organisational capability, and the relationship with suppliers are represented by the blue circle. The values represented by the arrows in

http://doi.org/10.18080/jtde.v13n3.1197

Figure 2 indicate the p-values, which signify the degree of statistical significance associated with the relationships between the variables.

The R^2 coefficient is employed for the purpose of analysing the model's efficacy in elucidating the data, with a range of values extending from 0 to 1. Purwanto & Sudargini, (2021) have distinguished three categories of R^2 values: those with a value of 0.25 are deemed to be low, those with a value of 0.5 are considered to be moderate, and those with a value of 0.75 are regarded as high. In this instance, Cyber Awareness was assigned a low value of 0.2, categorised as an exogenous (independent) variable, given that it is not influenced by other variables within the model. Conversely, the remaining endogenous (dependent) constructs yielded considerable values. The relationship with suppliers was found to have an R^2 value of 0.8, while the relationship with human talent and organisational cybersecurity preparedness had R^2 values of 0.7. These endogenous variables are dependent, insofar as their variance is explained by other variables within the model.

Similarly, the f^2 is calculated, which measures the size of the effects within the model and is interpreted in a similar manner to the R^2 values. In accordance with the categorisation proposed by Fey et al., (2023), values can be classified as follows: values of 0.02 indicate a small magnitude effect, values of 0.15 indicate a moderate magnitude effect, and values of 0.35 indicate a large magnitude effect. Thus, the greater the value of f^2, the more significant the impact of the predictor variables on the response variable, indicating a larger effect size. In this study, the majority of relationships exhibited medium and large effects, with one exception: the relationship between human and organisational talent, which reached a coefficient of 0.1.

The predictive model generated using partial least squares structural equation modelling (PLS-SEM) in SmartPLS 4 employs path coefficients (β) to quantify the strength and direction of relationships between latent variables. R^2 values indicate the proportion of variance in the endogenous constructs that is explained by the model. The f^2 effect sizes are calculated using the following formula:

$$f2 = \frac{R^2included - R^2excluded}{1 - R^2included}$$

In the context of the endogenous construct, the R^2 value when the predictor variable is included is represented by R^2. Conversely, the R^2 value when the predictor variable is excluded is represented by R^2. The f^2 values offer insights into the extent to which the predictor variable contributes to the explanation of the variance in the dependent variable. The analysis of path coefficients, in conjunction with the f^2 effect sizes, substantiated the assertion that the majority of relationships exhibited considerable predictive capacity, particularly those with

http://doi.org/10.18080/jtde.v13n3.1197

medium to large effect sizes. The model's predictive accuracy was additionally validated through blindfolding procedures utilising the Q^2 statistic, which confirmed its robustness.

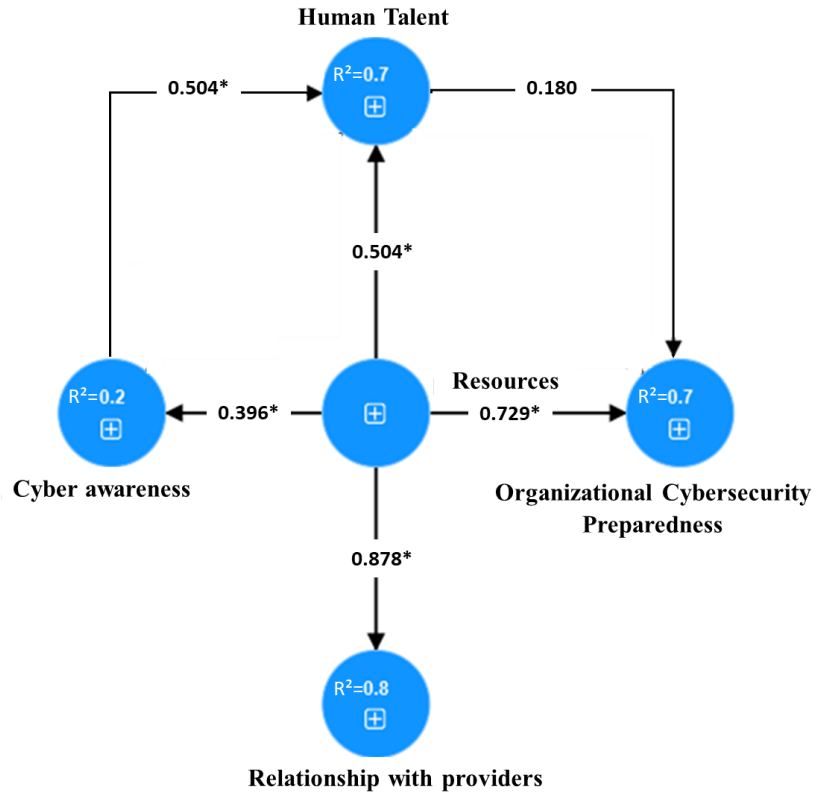


Figure 2: Results of structural equation modelling and relationships between cybersecurity factors in SMEs. Source: own elaboration based on SmartPLS 4

Note. Path coefficients (β) are shown in the arrows. R^2 values are shown within the constructs. Significance levels: *p < 0.05, **p < 0.01, ***p < 0.001.

The Q^2 statistic was subsequently employed to assess the model's predictive capacity in comparison to the utilisation of a mere mean value for the dependent variable. A value greater than zero indicates enhanced predictive capacity. This estimation was based on the PLSpredict technique, as demonstrated by Fadilah & Putranto, (2023), which is used in SmartPLS. This estimation was based on the PLSpredict technique used in SmartPLS, as demonstrated by Fadilah & Putranto, (2023). The constructs with the highest predictive power were Relationship with Suppliers (0.8), Organisational (0.7) and Human Talent (0.5), followed by a smaller but equal value. Cyber Awareness (0.1) was also identified as a significant predictor.

In comparison with a purely numerical assessment of the AVE, approaches that incorporate applied examples and benchmark values offer a more comprehensive interpretive framework for analysing construct variability. While the AVE values obtained in this study confirm adequate convergent validity, studies such as that of dos Santos and Cirillo, (2023)

http://doi.org/10.18080/jtde.v13n3.1197

demonstrate how comparative references can deepen the understanding of how strongly indicators reflect their latent constructs across different models or sample contexts. This perspective suggests that moving beyond threshold-based validation towards a comparative, context-sensitive interpretation may enhance the explanatory power of AVE within structural equation modelling, contributing to a more nuanced assessment of theoretical constructs.

In addition to the internal reliability analysis using CR and AVE, the PLS Predict procedure with k-fold cross-validation was applied to verify the predictive validity of the constructs. The positive Q^2 values obtained confirm the empirical robustness of the model and reinforce the consistency of the indicators observed against data not used in the direct estimation.

Discussion

The findings of this study indicate that the most pertinent relationship is that between the resources of small and medium-sized enterprises (SMEs) and their relationship with suppliers. This may indicate that SMEs' financial, technological, and human resources are of paramount importance for the effective management of security in supplier interactions. These findings are consistent with those of the Green study, which highlights the necessity for organisations to adopt optimal practices in the management of supplier relationships in order to enhance their resilience to disruptions, particularly those resulting from cyber attacks. In particular, the importance of establishing clear guidelines and policies for data sharing is emphasised. Similarly, this hypothesis is also supported by the findings of Kaur *et al.*, (2024), who emphasise the necessity for companies to assess the cyber risk associated with their suppliers and to make investments in cybersecurity in order to develop the capabilities required to protect their networks.

An unexpected finding in the Colombian context is that, unlike evidence from SMEs in developed economies where cyber awareness and human talent are often the strongest predictors of preparedness, our results indicate that organisational resources play the most decisive role. This suggests that in resource-constrained environments, awareness and human capabilities, although necessary, cannot be effectively translated into concrete cybersecurity practices without a minimum level of financial and technological support. Such evidence challenges prevailing theories predominantly built on SMEs in developed countries and highlights the need to refine existing frameworks to account for structural constraints that condition the effectiveness of human and organisational factors in developing economies.

Organisational resources were found to be the strongest predictor of preparedness, underscoring the importance of financial, technological, and infrastructure support. This

http://doi.org/10.18080/jtde.v13n3.1197

finding shows that the use of convenience sampling may have increased the importance of resource-related factors. This suggests that the company's capacity to procure security technologies, train personnel, and develop appropriate cybersecurity protocols is directly correlated with the availability of resources.

The decision to place organisational resources as the central factor in our model is supported by two theoretical foundations. First, the Resource-Based View (RBV) argues that resources constitute the fundamental basis through which firms develop capabilities, implement practices, and respond to external pressures (Barney, 1991; Wernerfelt, 1984). In the SME context, the availability of financial, technological, and human resources directly conditions their ability to adopt cybersecurity measures, enhance digitisation, or respond effectively to external threats. Second, research in technology adoption and cybersecurity emphasises that, while awareness and risk perception are important, the effective implementation of protective actions ultimately depends on the availability of resources. For example, without allocated budgets, skilled staff, or appropriate tools, even high levels of awareness rarely translate into tangible security practices (Chen *et al.*, 2021; Ifinedo, 2012).

Nevertheless, we acknowledge that an alternative model in which cyber awareness acts as the initial trigger for resource allocation is also plausible. In fact, in certain contexts, incidents or sector-wide alerts may raise awareness and subsequently motivate firms to assign more resources to cybersecurity. Considering such alternative dynamics could shift the interpretation of findings by emphasising awareness as a catalyst rather than resources as the enabler. For this reason, we have expanded the *Discussion* section to recognise this complementarity and highlight it as a promising avenue for future research. This adjustment strengthens the contribution of our study by showing that the interrelationships among resources, awareness, and preparedness may differ depending on contextual conditions.

This finding is consistent with that reported by Hasan *et al.*, (2021), who found that cybersecurity preparedness has a positive impact on organisational security performance. This, in turn, has a positive effect on financial performance, which is dependent on the resources available to the organisation.

Prior research has underscored the pivotal role of the human element in cyber attacks, particularly in the context of small and medium-sized enterprises (SMEs), where a tendency has been observed to prioritise technical solutions over human factors, despite the latter representing a significant vulnerability (Aschwanden *et al.*, 2024). Research conducted by Alhayani *et al.*, (2021) has identified the most effective strategies for addressing cyber threats as being related to human capital. These strategies include the development of cyber talent and the allocation of resources towards their education and training. This is consistent with

http://doi.org/10.18080/jtde.v13n3.1197

the findings of this study, which suggests that SMEs with greater resources can invest in ongoing training, security tools, and incentives for their employees, thereby enhancing the preparedness of their team.

It is also worthy of note that the level of cybersecurity awareness has a significant impact on the relationship with human talent. This indicates that the extent of employee knowledge and awareness of cyber threats is a crucial factor in developing a culture of security within the organisation. This finding is consistent with the assertion put forth by Baker, (2016) that cybersecurity awareness represents an indispensable component of fundamental training for the cyber workforce, thereby establishing a causal relationship. Similarly, the availability of resources was found to have a positive impact on cyber awareness. This finding is consistent with the results of the studies conducted by Ho & Gross (2021) and Chaudhary *et al.* (2023), who emphasise that cybersecurity awareness can be a crucial element in the development of an effective cyber defence strategy. It is therefore incumbent upon organisations to invest resources in order to reinforce this aspect.

Human talent was identified as a determining factor in preparedness, highlighting the importance of training and awareness. This suggests that staff capacity and competencies are crucial factors in the implementation and maintenance of effective security measures. This is also reflected in the findings of Meduri & Prasad (2018). These authors posit that as technological advances have transformed the way people live their daily lives, especially in the workplace, there is a need for individuals, organisations and the nation to enhance their automation and cybersecurity capabilities to effectively mitigate cyber attacks. Consequently, for the successful implementation of these changes in the workplace, small and medium-sized enterprises (SMEs) must first identify the necessity for personnel to undergo training and acquire new skills. This must be accompanied by organisational readiness and flexibility. However, the absence of a structured model, such as the Human Factors Analysis and Classification System (HFACS), limits the granularity of this analysis. Therefore, incorporating such a framework could provide a more comprehensive context for understanding human error and its implications for SME cybersecurity.

There is a growing tendency for business activities to be conducted online, with an increasing reliance on cloud services. This transition may result in an elevated prevalence and financial burden of cybercrime. Poehlmann *et al.* (2021a) posit that small and medium-sized businesses are the primary targets of cyber attacks. It is therefore imperative that research be conducted in this area in order to develop effective cybersecurity procedures and practices. The paucity of robust research in this field renders it even more imperative to prioritise this topic.

http://doi.org/10.18080/jtde.v13n3.1197

The significance of this issue lies in the fact that SMEs are frequently ill-prepared for potential threats. Consequently, researchers must accord this phenomenon greater attention. Cybercrime can have adverse consequences for the organisational performance of small and medium-sized companies and can also have implications for the global economy as a whole. Considering the aforementioned characteristics, it is imperative to address the growing security demands resulting from the increased risk of cyber attacks and threats with greater commitment.

Furthermore, other studies have identified human talent as a crucial factor in combating cybercrime against organisations. A systematic review conducted by Poehlmann *et al.*, (2021a) indicates that human error represents the most significant factor in successfully defending against cyber attacks. Similarly, Quader & Janeja (2021a) demonstrated in their research on the lessons learned from cyber attack case studies that human behaviour represents the weakest link in the enabling of cyber attacks. It is therefore recommended that employees receive regular training and communication on how to prevent and detect cyber threats.

Similarly, Alharbi *et al.* (2021) identified three factors that contribute to the loss of sensitive data, all of which are closely related to the human factor: awareness of cybersecurity, knowledge of cybersecurity risks, and professional salaries. It is noteworthy that the researchers identified a positive correlation between knowledge of cybersecurity risks and the loss of confidential data among small businesses. In a similar vein, Alarifi (2023a) put forth a proposal for a study to assess the preparedness of SMEs in Saudi Arabia in the event of a cyber attack. One of the factors with a positive association is cyber awareness, which is also linked to human behaviour. The findings indicate that this awareness has a significant and positive impact on the preparedness of SMEs against cyber attacks. Consequently, some companies are implementing measures to encourage the adoption of secure practices among their employees.

Conversely, research has demonstrated that the absence of regulations, standards, procedures, and comprehensive guidelines to foster optimal cybersecurity practices in SMEs contributes to the prevalence of inadequate cybersecurity measures. Furthermore, employees of SMEs frequently lack the requisite knowledge to effectively respond to cyber attacks, resulting in considerable deficiencies in this area (Ncubukezi *et al.*, 2020).

As Lis & Mendel (2019) observe, economic and managerial constraints frequently impede the development and implementation of technological solutions designed to combat cyber attacks. This is due to the allocation of scarce resources and the necessity for processes and organisational culture to be aligned with the objective of prevention. The role of resources in the context of cyber attacks has been the subject of extensive study in a number of articles.

http://doi.org/10.18080/jtde.v13n3.1197

In their study, Tam *et al.*, (2021b) identified several key factors that negatively impact the ability of small businesses to protect themselves from potential cyber attacks. These factors include resource limitations, organisational process maturity, and legal structures. Hasani *et al.* (2023) investigated the factors that relationship the adoption of cybersecurity and its impact on organisational performance. This study identifies compatibility, perceived usefulness, ease of use, and the possibility of testing solutions for SMEs as key factors that organisations must consider in order to protect their non-tangible assets, such as information. While Hasani *et al.* (2023) concentrate on the elements that facilitate the adoption of cybersecurity, this article examines the factors that can render SMEs more susceptible to cyber attacks. These two perspectives are mutually reinforcing and contribute to a comprehensive understanding of the cybersecurity challenges and opportunities facing SMEs, as well as the risk of cyber attacks on these organisations. Small businesses frequently fail to assume a proactive role in preventing and detecting cyber attacks (Yudhiyati *et al.*, 2021). Effective management of factors related to cyber attacks and the adoption of cybersecurity can assist these companies in meeting the necessary requirements for successful cybersecurity implementation.

While the analysis provides valuable insights into the human and organisational factors influencing cybersecurity preparedness in SMEs, it would be relevant to consider fundamental concepts such as incident response and threat modelling. Threat modelling is crucial for identifying potential attack vectors, assessing vulnerabilities, and establishing prioritised protective measures, allowing organisations to proactively manage cybersecurity risks (Zografopoulos *et al.*, 2021). On the other hand, a well-structured incident response framework is essential for early detection, containment, and recovery from the effects of cyber attacks, ensuring operational resilience in the face of security incidents (Schlette *et al.*, 2021). The omission of these approaches could limit the practical applicability of the findings in terms of developing robust cybersecurity strategies for SMEs.

In conclusion, these findings contribute to the understanding of the factors that linkage cyber attacks on SMEs and provide information for cybersecurity researchers and managers to help organisations improve in this area. It is therefore essential that SMEs are able to detect, respond to and recover from cyber attacks. In the absence of research in this area, they may lack the guidance required to take appropriate action.

In conclusion, the findings contribute to our understanding of the factors influencing cyber attacks on SMEs. The findings provide valuable information for cybersecurity researchers and administrators, enabling them to enhance organisational capabilities in this domain. It is imperative that small and medium-sized enterprises (SMEs) are able to detect, respond to and

http://doi.org/10.18080/jtde.v13n3.1197

recover from cyber attacks. In the absence of research in these areas, there is a paucity of guidance on how to act (Chidukwani *et al.*, 2022).

Moreover, this research makes novel contributions by focusing on developing countries and addressing the gap in empirical research on cybersecurity for small businesses. In contrast, a substantial body of research has been conducted on this topic with respect to large companies.

Limitations and recommendations

In terms of the limitations of the study, it is crucial to underscore that the correlations were established exclusively with the factors put forth in the existing literature, without incorporating socio-demographic variables. It would be beneficial for future studies to include correlations with socio-demographic variables, such as the size of the organisation, experience, and economic sector, among others, about the constructs proposed in the literature.

A further limitation of the study is the sampling technique employed, as although convenience sampling is a practical and straightforward method, it may also lead to some drawbacks that could potentially compromise the quality of the findings.

Firstly, the participants in this study were selected according to their availability and accessibility to answer the survey (and also considering other criteria). However, it should be noted that the study is not free from selection bias, as the sample is not representative of the entire SME population. The findings cannot be extrapolated to other companies or sectors. Consequently, the participants may exhibit similar characteristics that do not reflect the diversity of the total universe, such as experience, attitude towards cybersecurity, or company size. Therefore, the absence of randomisation may result in the over-representation of specific groups and the under-representation of others. It is therefore recommended that future studies implement random sampling in order to avoid such problems.

In this regard, an additional limitation of this study lies in the use of a non-probabilistic convenience sampling technique, which restricts the generalisability of the findings. While this method was appropriate for exploratory purposes and ensured accessibility to SME decision-makers in Medellín, it does not allow for statistical inference for the broader population of SMEs in Colombia or other developing countries. Thus, the absence of probabilistic sampling may have generated selection bias and limited representation of diverse organisational profiles across different sectors and regions. Therefore, future studies should employ probabilistic or stratified sampling designs that include SMEs from different industries and geographic areas in order to strengthen external validity and allow for broader comparisons and generalisation of results.

http://doi.org/10.18080/jtde.v13n3.1197

Furthermore, the use of a convenience sample may have introduced bias into the results. The sample may have disproportionately included companies with a greater technological orientation or greater concern for cybersecurity practices. This over-representation may have exaggerated the strength of the relationships observed between human and organisational factors and levels of preparedness, while under-representing companies with lower digital maturity. Therefore, the findings should be interpreted with caution, as the sample may not fully reflect the diversity of SMEs in the general population.

Conversely, prior to answering the questionnaire, participants were informed about the distinction between phishing and fake software. However, no formal assessment was conducted to evaluate their existing knowledge on the subject. At this juncture, our objective was to ascertain that all respondents had a minimum and consistent understanding of these terms before responding to the questions. However, this may have affected the validation of the results, as prior knowledge was not considered as a measurable variable in the study. It is therefore recommended that this point be considered in future studies on the topic and that a measure of participants' prior knowledge level be included before they are provided with any information.

The analysis of employee actions related to cyber hygiene could greatly benefit from the integration of behavioural models, such as the TPB. This theory, widely used in security behaviour research, suggests that employees' intentions to engage in cybersecurity practices are influenced by three key factors: attitude toward the behaviour, subjective norm (perceived social pressure), and perceived behavioural control (the ability to perform the action). By incorporating TPB into the study, a deeper understanding could be gained of the psychological determinants underlying employees' decisions regarding cyber hygiene practices. This would allow researchers and practitioners to design more targeted and effective interventions, aligned with the factors that truly linkage security behaviour.

Furthermore, it is important to include a limitation that stems from the possible omitted variable bias, derived from the non-incorporation of constructs proposed by established frameworks, such as the 'subjective norms' of the TPB or the 'Identify/Protect' functions of the NIST Cybersecurity Framework. Their absence could have increased the explanatory power of the factors considered in this study. In this regard, future research should integrate these variables to ensure more robust and comprehensive models.

With this in mind, another limitation of this study is the omission of key operational and regulatory cybersecurity concepts that could enrich the analysis. While the research focused on the human and organisational factors that influence preparedness, it did not address in depth approaches such as incident response processes, threat modelling, or the adoption of

http://doi.org/10.18080/jtde.v13n3.1197

international frameworks such as the NIST Cybersecurity Framework or ISO/IEC 27001. The omission of these perspectives may have limited the practical applicability of the findings for SMEs seeking structured guidelines to strengthen their cybersecurity posture. Therefore, future research should integrate these frameworks and methodologies to offer more comprehensive and practical recommendations.

A notable limitation of the study is its omission of specific metrics to systematically assess human error, despite its analysis of the linkage of human talent on organisational preparedness against cyber attacks. The HFACS is a model that facilitates the identification and categorisation of human failures at various levels. These levels include individual errors, organisational factors, and latent conditions. The dearth of such analyses impedes a comprehensive understanding of how human behaviour contributes to cybersecurity gaps in SMEs. It is recommended that subsequent research endeavours integrate methodologies of this nature to improve the precision of identifying vulnerabilities associated with the human element.

For this reason, an additional limitation of this study is the absence of specific human factor metrics to systematically evaluate human error. While the role of human talent as a determinant of cybersecurity preparedness was examined, established models such as the HFACS were not applied. Thus, the lack of these methodological tools could limit the accuracy of human-centred analysis, as it does not allow for the categorisation of errors at the individual, organisational, and latent levels. Therefore, future studies should also incorporate validated frameworks such as the HFACS.

In the current landscape of digital transformation, it is valuable to consider the role of advanced technologies such as Artificial Intelligence-enabled Intrusion Detection Systems (AI-IDS) and blockchain-based cybersecurity solutions, which represent promising approaches to strengthening the protection of critical infrastructures and business environments. AI-IDS are particularly effective due to their ability to learn from large datasets and detect anomalous behaviours with high accuracy, enabling proactive responses to threats in complex cyber-physical systems, especially within Industry 4.0 contexts (Alohali *et al.*, 2022). Complementarily, balockchain-based solutions provide a decentralised architecture that enhances the security, integrity, and traceability of information, offering a robust framework to address challenges such as unauthorised access, data tampering, and lack of transparency in existing systems (Yadav *et al.*, 2022). Conceptually integrating these emerging technologies into the analysis of cybersecurity preparedness contributes to a more innovative perspective that aligns with the evolving nature of digital defence strategies.

http://doi.org/10.18080/jtde.v13n3.1197

On the other hand, it is worth noting that, although the theoretical model applied in this study identifies structural factors that influence cyber attack preparedness, the existence or implementation of real-time incident escalation processes was not explicitly addressed. In that sense, this constitutes a key operational component in threat management within organisations. Therefore, it is suggested to include escalation processes in further research and practical guidelines, especially for the design of escalation response plans in SMEs.

Furthermore, while this study contributes to the understanding of the human and organisational factors that linkage cyber attack preparedness in SMEs, no exploration of proactive cybersecurity frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001 or the CIS Controls was conducted. In fact, these frameworks offer structured guidelines for the prevention and early management of cyber risks. However, this study did not focus on them, therefore, it is suggested that future research should integrate these normative and operational references as an opportunity to strengthen the practical application of the findings and at the same time, guide SMEs in the implementation of robust threat preparedness and response strategies.

In conclusion, it is essential to enhance and tailor the items of the study to the context in which the questionnaire will be administered. This is crucial from an economic, political, environmental and social standpoint, as in this study, the items were applied in accordance with our context in Colombia and specifically in the city of Medellín.

This finding confirms that in contexts with limited capital and technology – such as many SMEs in developing countries – the availability of resources is a key determinant of cybersecurity resilience. This is consistent with previous studies indicating that the scarcity of technological and financial infrastructure reduces the ability to implement systematic and sustained security measures.

The relationship between human talent and organisational preparedness is shaped differently in resource-constrained environments. Evidence indicates that, rather than directly impacting preparedness, organisational capacity to manage resources effectively for security purposes is strengthened by human talent. In contexts such as Colombia, where human factors constitute the main entry points for cyber attacks, it is emphasised that organisations should invest not only in talent development but also in transforming that knowledge into operational resources and tangible processes.

In developed countries, human talent development is commonly achieved through formal training programs and specialised hiring. By contrast, in resource-limited environments, cybersecurity capabilities need to be strategically developed within existing staff.

http://doi.org/10.18080/jtde.v13n3.1197

Consequently, the resource–talent relationship becomes more critical and direct, as tangible resources are prioritised over human development due to immediate organisational needs.

Conclusions

The survey findings indicated that 33% of SMEs had experienced cyber attacks, underscoring the necessity of addressing suspicious behaviour at the organisational level to prevent exploitation and negative impacts. SMEs are exposed to a multitude of cyber threats, including phishing, malware, and scams, underscoring the necessity for robust prevention protocols. The capacity for resilience in the context of cyber threats is contingent upon the availability of human talent and resources. It is therefore essential that organisations implement continuous cybersecurity training and implement adequate security measures. In light of these findings, it is recommended that SMEs develop awareness plans and promote information security among decision-makers, even with limited resources. It is incumbent upon academic institutions to ensure that future professionals are well versed in cybersecurity, with a view to mitigating risks and supporting business sustainability.

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2): 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Alarifi, S. H. (2023a). Small and Medium Businesses Readiness towards cyber attacks in Saudi Arabia. *Global Economics Review*, *VIII*, 113–126. https://doi.org/10.31703/ger.2023(VIII-I).11

Alarifi, S. H. (2023b). Small and Medium Businesses Readiness towards cyber attacks in Saudi Arabia. *Global Economics Review*, *VIII*(I), 113–126. https://doi.org/10.31703/ger.2023(VIII-I).11

Alharbi, F., Alsulami, M., AL-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The Impact of Cybersecurity Practices on cyber attack Damage: The Perspective of Small Enterprises in Saudi Arabia. *Sensors*, *21*, 6901. https://doi.org/10.3390/s21206901

Alhayani, B., Abbas, S. T., Khutar, D. Z., & Mohammed, H. J. (2021). *WITHDRAWN: Best ways computation intelligent of face cyber attacks*. https://doi.org/10.1016/j.matpr.2021.02.557

Alohali, M. A., Al-Wesabi, F. N., Hilal, A. M., Goel, S., Gupta, D., & Khanna, A. (2022). Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment. *Cognitive Neurodynamics*, *16*(5), 1045–1057. https://doi.org/10.1007/S11571-022-09780-8/METRICS

Amora, J. T. (2021). Convergent validity assessment in PLS-SEM: A loadings-driven approach. *Data Analysis Perspectives Journal*, *2*, 1–6.

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decis Support Syst*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580

Aschwanden, R., Messner, C., Höchli, B., & Holenweger, G. (2024). Employee behavior: the psychological gateway for cyber attacks. *Organizational Cybersecurity Journal: Practice, Process and People*, *4*, 32–50. https://doi.org/10.1108/OCJ-02-2023-0004

Asis, E. H. R., Maguiña, M. R. E., infantes, S. M. E., & Toro, M. E. N. (2020). Inteligencia emocional, competencias y desempeño del docente universitario: Aplicando la técnica mínimos cuadrados parciales SEM-PLS. *Revista Electrónica Interuniversitaria de Formación Del Profesorado*, *23*, 99–114. https://doi.org/10.6018/reifop.428261

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics (Basel*, *12*. https://doi.org/10.3390/electronics12061333

Bagozzi, R. P., & Heatherton, T. F. (1994). A general approach to representing multifaceted personality constructs: Application to state self-esteem. *Struct Equ Modeling*, *1*, 35–67. https://doi.org/10.1080/10705519409539961

Baker, M. (2016). *Striving for effective cyber workforce development*.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120. https://doi.org/10.1177/014920639101700108

Becker, J.-M., Cheah, J.-H., Gholamzade, R., Ringle, C. M., & Sarstedt, M. (2023). PLS-SEM's most wanted guidance. *International Journal of Contemporary Hospitality Management*, *35*, 321–346. https://doi.org/10.1108/IJCHM-04-2022-0474

Bhatti, B. M., Mubarak, S., & Nagalingam, S. (2021). Information security implications of using NLP in IT outsourcing: a Diffusion of Innovation theory perspective. *Automated Software Engineering*, *28*, 12. https://doi.org/10.1007/s10515-021-00286-x

Blanco Esteban, L. F. (2022). Bailando con lobos: la estrategia de ciberseguridad en la organización. *RUIDERAe: Revista de Unidades de Información*, *19*, 1–9.

Cano, J. J. (2022). La cadena de suministro digital. *Revista Sistemas*, *164*, 53–63. https://doi.org/10.29236/sistemas.n164a6

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & Computer Security*, *27*, 101–121. https://doi.org/10.1108/ICS-11-2016-0088

Chang, L. Y. C., & Coppel, N. (2020a). Building cyber security awareness in a developing country: Lessons from Myanmar. *Comput Secur*, *97*, 101959. https://doi.org/10.1016/j.cose.2020.101959

Chang, L. Y. C., & Coppel, N. (2020b). Building cyber security awareness in a developing country: Lessons from Myanmar. *Computers & Security*, *97*, 101959. https://doi.org/10.1016/j.cose.2020.101959

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Comput Sci Rev*, *50*, 100592. https://doi.org/10.1016/j.cosrev.2023.100592

Chen, J.-K., Lin, Y.-H., & Chang, C.-H. (2021). Cyber security training and awareness for small and medium enterprises. In *2021 IEEE International Conference on Consumer Electronics-Taiwan (GCCE)* (pp. 1–2). IEEE. https://doi.org/10.1109/GCCE53005.2021.9621945

Cheung, G. W., & Wang, C. (2017). Current Approaches for Assessing Convergent and Discriminant Validity with SEM: Issues and Solutions. *Academy of Management Proceedings 2017*, 12706. https://doi.org/10.5465/AMBPP.2017.12706abstract

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, *10*, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Chidukwani, A., Zander, S., & Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Comput Secur*, *145*. https://doi.org/10.1016/j.cose.2024.104026

Chikwendu, S. C., & Oli, N. P. (2023). Human Factors influencing Compliance to Cyber Security Practices by Employees of Public Universities in Southeast Nigeria. *International Journal of Information Security, Privacy and Digital Forensics*, *7*, 1–10.

Development Bank of Latin American and The Caribbean. (2023). *Supporting SMEs*

for more productive countries. *https://www.caf.com/media/4663668/impacto-caf-support-to-smes-full-report.pdf?utm_source=chatgpt.com*

De Jesús Zambrano Miranda, M., De la Cruz Almanza, S. A., Villamizar, J. A. P., Uribe, S. M. B., & Arias, I. C. R. (2025). Informalidad empresarial en micronegocios de colombia: evidencia desde cúcuta y su área metropolitana. *Semestre Económico*, *28*(65), 1-24. https://doi.org/10.22395/seec.v28n65a5054

Deutrom, J., Katos, V., & Ali, R. (2022). Loneliness, life satisfaction, problematic internet use and security behaviours: re-examining the relationships when working from home during COVID-19. *Behaviour & Information Technology*, *41*(14), 3161–3175. https://doi.org/10.1080/0144929X.2021.1973107

Díaz-Piraquive, F. N., De Jesús Muriel-Perea, Y., & González-Crespo, R. (2023). Cybersecurity Management in Micro, Small, and Medium Enterprises in Colombia. En *Communications in computer and information science* (pp. 74-85). https://doi.org/10.1007/978-3-031-34045-1_8

dos Santos, P. M., & Cirillo, M. Â. (2023). Construction of the average variance extracted index for construct validation in structural equation models with adaptive regressions. *Communications in Statistics: Simulation and Computation*, *52*(4), 1639–1650. https://doi.org/10.1080/03610918.2021.1888122

Fadilah, A. N., & Putranto, N. A. R. (2023). Influence of Employer Branding Dimensions on Generation Z Women's Intention to Apply For a Job with Person-Organization Fit as Mediating Variable. *Journal Integration of Social Studies and Business Development*, *1*, 91–101. https://doi.org/10.58229/jissbd.v1i2.110

Fey, C. F., Hu, T., & Delios, A. (2023). The Measurement and Communication of Effect Sizes in Management Research. *Management and Organization Review*, *19*, 176–197.

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG Int J Comput Sci*, *48*, 1–10.

George, A. S., Baskar, T., & Srikaanth, B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal(PUIIJ*, *2*, 51–75.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*, 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J., Hollingsworth, C. L., Randolph, A. B., & Chong, A. Y. L. (2017). An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems*, *117*, 442–458. https://doi.org/10.1108/IMDS-04-2016-0130

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*. https://doi.org/10.1016/j.jisa.2020.102726

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*, 97. https://doi.org/10.1007/s43546-023-00477-6

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. *Information Systems Frontiers*, *21*, 1285–1305. https://doi.org/10.1007/s10796-019-09959-1

Ho, S. M., & Gross, M. (2021). Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness. *Comput Secur*, *108*, 102357. https://doi.org/10.1016/j.cose.2021.102357

Huang, C.-H. (2021). Using PLS-SEM Model to Explore the Influencing Factors of Learning Satisfaction in Blended Learning. *Educ Sci (Basel*, *11*, 249. https://doi.org/10.3390/educsci11050249

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.07.007

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*, 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kaur, H., Gupta, M., & Singh, S. P. (2024). Integrated model to optimize supplier selection and investments for cyber resilience in digital supply chains. *Int J Prod Econ*, *275*, 109338. https://doi.org/10.1016/j.ijpe.2024.109338

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, 11–14. https://doi.org/10.1016/S1361-3723(19)30085-5

Klein, G., & Zwilling, M. (2024). The Weakest Link: Employee Cyber-Defense Behaviors While Working from Home. *Journal of Computer Information Systems*, *64*, 408–422. https://doi.org/10.1080/08874417.2023.2221200

Lee, L., Petter, S., Fayard, D., & Robinson, S. (2011). On the use of partial least squares path modeling in accounting research. *International Journal of Accounting Information Systems*, *12*, 305–328. https://doi.org/10.1016/j.accinf.2011.05.002

Lis, P., & Mendel, J. (2019). cyber attacks on Critical Infrastructure: an Economic Perspective. *Economics and Business Review*, *5*, 24–47. https://doi.org/10.18559/ebr.2019.2.2

Meduri, Y., & Prasad, S. C. (2018). Designing the Strategies for Preparing Talent for Change: A Special Focus on Automation, Digital Security and Demographics. *Gavesana Journal of Management*, *10*, 94–108.

Mohamad, A., Rizal, A. M., Kamarudin, S., & Sahimi, M. (2022). Exploring the Co-Creation of Small and Medium Enterprises, and Service Providers Enabled by Digital Interactive Platforms for Internationalization: A Case Study in Malaysia. *Sustainability*, *14*, 16119. https://doi.org/10.3390/su142316119

Morgan S. (2023). *Cybercrime To Cost The World 10.5 Trillion Annually By 2025, Special Report: Cyberwarfare In The C-Suite*. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Nagahawatta, R., Lokuge, S., Warren, M., & Salzman, S. (2021). Cybersecurity Issues and Practices in a Cloud Context: A Comparison Amongst Micro. *Small and Medium Enterprises*.

Ncubukezi, T., Mwansa, L., & Rocaries, F. (2020). A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses. *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE*, 1–6. https://doi.org/10.23919/ICITST51030.2020.9351339

Nsoh, J. (2021). *Exploring the Strategies Cybersecurity Managers Need to Bolster Industry 4.0 from cyber attacks*. Doctoral dissertation, Colorado Technical University.

Nyarko, D. A., & Fong, R. C. (2023). Cyber Security Compliance Among Remote Workers. In H. Jahankhani (Ed.), *Cybersecurity in the Age of Smart Societies*. *Advanced Sciences and Technologies for Security Applications* (pp. 343–369). Springer. https://doi.org/10.1007/978-3-031-20160-8_18

Ospina, M., y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, 62(2), 199-217. https://doi.org/10.47741/17943108.168

Parker, A., & Brown, I. (2019). Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa. In H. Venter, M. Loock, M. Coetzee, M. Eloff, & J. Eloff (Eds.), *Information Security*. *ISSA 2018*. *Communications in Computer and Information Science* (pp. 176–192). Springer. https://doi.org/10.1007/978-3-030-11407-7_13

Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., & Merz, T. (2021a). The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review. In K. Daimi, H. R. Arabnia, L. Deligiannidis, M. S. Hwang, & F. G. Tinetti (Eds.), *Advances in Security, Networks, and Internet of Things*. *Transactions on Computational*

Science and Computational Intelligence (pp. 377–395). https://doi.org/10.1007/978-3-030-71017-0_27

Poehlmann, N., Caramancion, K. M., Tatar, I., Li, Y., Barati, M., & Merz, T. (2021b). The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review. In K. Daimi, H. R. Arabnia, L. Deligiannidis, M. S. Hwang, & F. G. Tinetti (Eds.), *Advances in Security, Networks, and Internet of Things. Transactions on Computational Science and Computational Intelligence* (pp. 377–395). https://doi.org/10.1007/978-3-030-71017-0_27

Polkowski, Z., & Dysarz, J. (2017). It security management in Small and Medium Enterprises. *Scientific Bulletin – Economic Sciences*, *16*, 134–148.

Purwanto, A., & Sudargini, Y. (2021). Partial Least Squares Structural Squation Modeling (PLS-SEM) Analysis for Social and Management Research : A Literature Review. *Journal of Industrial Engineering & Management Research*, *2*, 114–123.

Pyke, A., Rovira, E., Murray, S., Pritts, J., Carp, C. L., & Thomson, T. (2021). Predicting individual differences to cyber attacks: Knowledge, arousal, emotional and trust responses. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *15*, 9. https://doi.org/10.5817/CP2021-4-9

Quader, F., & Janeja, V. P. (2021a). Insights into Organizational Security Readiness: Lessons Learned from cyber attack Case Studies. *Journal of Cybersecurity and Privacy*, *1*, 638–659. https://doi.org/10.3390/jcp1040032

Quader, F., & Janeja, V. P. (2021b). Insights into Organizational Security Readiness: Lessons Learned from cyber attack Case Studies. *Journal of Cybersecurity and Privacy*, *1*(4), 638–659. https://doi.org/10.3390/jcp1040032

Ramayah, T., Ling, N. S., Taghizadeh, S. K., & Rahman, S. A. (2016). Factors influencing SMEs website continuance intention in Malaysia. *Telematics and Informatics*, *33*, 150–164. https://doi.org/10.1016/j.tele.2015.06.007

Realpe, M. E., & Cano, J. (2020). Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia. In R. A. Méndez Romero, J. Cano, J. Ramió Aguirre, & L. E. Sánchez Crespo (Eds.), *Seguridad Informática: X Congreso Iberoamericano, CIBSI 2020*.

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*, *1*, 24–46. https://doi.org/10.1108/OCJ-03-2021-0004

Rezaei, R., Safa, L., & Ganjkhanloo, M. M. (2020). Understanding farmers' ecological conservation behavior regarding the use of integrated pest management- an application of the technology acceptance model. *Glob Ecol Conserv*, *22*, 941. https://doi.org/10.1016/j.gecco.2020.e00941

Rogers, E. M. (2003). *Diffusion of Innovations* (5th ed.). Free Press.

Rožman, M., Tominc, P., & Milfelner, B. (2020). A Comparative Study Using Two SEM Techniques on Different Samples Sizes for Determining Factors of Older Employee's Motivation and Satisfaction. *Sustainability*, *12*, 2189. https://doi.org/10.3390/su12062189

Sánchez, D. A. G., Duran, D. E. S., Valencia, L. E. P., Jaimes, A. E. V., González, I. A. D., & Alegría, F., Alonso Vidal. (2023). Modelo de madurez de cultura organizacional de ciberseguridad para el sector financiero basado en buenas prácticas. *Revista Ibérica De Sistemas e Tecnologias De Informação,* 362-375.

Sánchez, M. A., & Batista, M. (2023). Business continuity for times of vulnerability: Empirical evidence. *Journal of Contingencies and Crisis Management*, *31*, 431–440. https://doi.org/10.1111/1468-5973.12449

Saz Dones, M. (2022). *Ciclo de Vida de un Ciberataque: Ataque y Defensa*. Universidad de Alcalá.

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys and Tutorials*, *23*(4), 2525–2556. https://doi.org/10.1109/COMST.2021.3117338

Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-Phishing Techniques – A Review of Cyber Defense Mechanisms. *IJARCCE*, *11*(7). https://doi.org/10.17148/ijarcce.2022.11728

Tam, T., Rao, A., & Hall, J. (2021a). The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Tam, T., Rao, A., & Hall, J. (2021b). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Comput Secur*, *109*, 102385. https://doi.org/10.1016/j.cose.2021.102385

Thakur, M. (2024). Cyber Security Threats and Countermeasures in Digital Age. *Journal of Applied Science and Education (JASE*, *4*, 1–20. https://doi.org/10.54060/a2zjournals.jase.42

Tobi, H., & Kampen, J. K. (2018). Research design: the methodology for interdisciplinary research framework. *Qual Quant*, *52*, 1209–1225. https://doi.org/10.1007/s11135-017-0513-8

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal*, *5*(2), 171–180. https://doi.org/10.1002/smj.4250050207

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It Won't Happen to Me: Surveying SME Attitudes to Cyber-security. *Journal of Computer Information Systems*, *63*, 397–409. https://doi.org/10.1080/08874417.2022.2067791

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine*, *48*(3), 1846–1852. https://doi.org/10.1016/j.ifacol.2015.06.355

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022a). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *Int J Inf Manage*, *66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022b). The role of cybersecurity and policy awareness in shifting employee compliance attitudes:

Building supply chain capabilities. *International Journal of Information Management*, *66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Yadav, S. K., Sharma, K., Kumar, C., & Arora, A. (2022). Blockchain-based synergistic solution to current cybersecurity frameworks. *Multimedia Tools and Applications*, *81*(25), 36623–36644. https://doi.org/10.1007/S11042-021-11465-Z/METRICS

Yudhiyati, R., Putritama, A., & Rahmawati, D. (2021). What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society*, *19*, 446–462. https://doi.org/10.1108/JICES-03-2021-0035

Zografopoulos, I., Ospina, J., Liu, X., & Konstantinou, C. (2021). Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies. *IEEE Access*, *9*, 29775–29818. https://doi.org/10.1109/ACCESS.2021.3058403

The Impact of 5G on Business Models for Mobile Operators in Emerging Markets

Laurence Banda
University of the Witwatersrand

Etienne Alain Feukeu
University of South Africa

Abstract: The advent of 5G wireless technologies has created new opportunities and challenges for mobile operators in emerging markets. However, the disruptive nature of 5G networks is likely to transform existing value chains and impact the current mobile operator-centric ecosystem, rendering traditional business models inadequate. The introduction of 5G networks therefore requires the adoption of new business models or the reconfiguration of existing ones to ensure that mobile operators can achieve both economic value and technological innovation in a sustainable way. This study investigates the factors that impact business models of mobile operators in emerging markets as a result of 5G deployment. The study was conducted using the qualitative research method by adopting an interpretivist research philosophy. Primary data was collected inductively through a case study approach with 10 semi-structured online interviews conducted in 8 emerging markets in the Sub-Saharan Africa region. The results show that when 5G is commercially deployed, several aspects, including internal, external and hybrid factors impact the business models of mobile operators.

Keywords: 5G, Business Models, Emerging Markets, Impacting Factors, Mobile Operators

Introduction

The evolution of mobile communication technologies towards ubiquitous broadband and seamless connectivity has been accelerated by the deployment of fifth generation (5G) networks. Unlike previous generations of mobile networks, 5G offers myriad technical and economic opportunities (Campbell *et al.*, 2017). Furthermore, apart from advancing the wireless technology space, 5G networks envision to deliver economic value to all key stakeholders in the mobile ecosystem: mobile operators, equipment suppliers, device manufacturers, public institutions, private enterprises and vertical industries (Banda, *et al.*, 2022). However, the techno-economic disruptive nature of 5G networks is likely to reshape the current mobile value chain and impact the existing mobile operator-centric ecosystem,

http://doi.org/10.18080/jtde.v13n3.1230

making conventional business models ineffective (Oughton & Lehr, 2022). As a result, the introduction of 5G networks requires the adoption of novel business models or the reconfiguration of the existing ones to achieve techno-economic value for mobile operators in a sustainable manner (Ahokangas, *et al.*, 2023; Banda *et al.*, 2022; Camps-Aragó, *et al.*, 2019).

Emerging markets are attractive for both technological advancement and economic growth as they are strategically located between the under-developed and the developed economies and more engaged in global market growth (Shankar & Narang, 2020). However, the experience from previous wireless network generations has shown that advanced economies such as Western Europe, North America, and Asia Pacific regions have been technological front-runners. Emerging markets such as Sub-Saharan Africa, India, and Latin America have always been regarded as mere consumer markets (Garba, *et al.*, 2022).

Focusing specifically on Sub-Saharan Africa (SSA), the context becomes particularly nuanced. The region encompasses diverse economies ranging from low- to upper-middle-income, with many fragile or conflict-affected states and small, resource-constrained nations. According to the World Bank Group (2024), growth is projected to remain modest but steady, rising from 3.3% in 2024 to 3.5% in 2025, and further to 4.3% by 2026-27. Yet pervasive challenges including high debt servicing, weak infrastructure, widespread poverty (with over 460 million people living in extreme poverty), and recurrent climate and conflict shocks continue to suppress broad-based development and digital investment (World Bank Group, 2024).

Within this environment, mobile broadband is a key lever for productivity and inclusion. According to GSMA (2024), by 2030 4G will account for about 50% of connections, while 5G will expand from near-zero today to roughly 17% of total connections, contributing an estimated US $10 billion to regional GDP. Larger economies such as South Africa, Nigeria, and Kenya are expected to lead this uptake with Fixed-Wireless Access (FWA) playing a crucial role in bridging gaps where fibre penetration is low (Okeleke, *et al.*, 2019). These dynamics highlight how spectrum policy, infrastructure-sharing models, and device affordability will be decisive for mobile operators as they reconfigure business models to capture 5G opportunities in emerging markets (Banda *et al.*, 2022).

Research on 5G and business models has focused mostly on mobile operators in developed countries with less focus on emerging markets (Banda *et al.*, 2022; Chochliouros *et al.*, 2017; Schneir *et al.*, 2019). Moreover, the integration of 5G and business models has mainly targeted individual business model components such as cost structures, revenue models, product and services, customers and infrastructure (Ahokangas *et al.*, 2019; Banda, 2025; Yrjölä, *et al.*, 2018). This article explores the impact of 5G on business models for mobile operators in emerging markets using a qualitative research method. The study envisages to uniquely

http://doi.org/10.18080/jtde.v13n3.1230

contribute to the body of knowledge in the fields of telecommunications engineering and management science as it examines 5G and business models from the perspective of emerging markets. The main research question of the study is:

What factors impact business models for mobile operators in enabling 5G networks in emerging markets?

This paper explores the impact of 5G networks on business models of mobile operators in the context of emerging markets. The current study contributes significantly to the development and adoption of sustainable business models for mobile operators deploying 5G networks. In theoretical terms, the study complements the extant literature and leads to a better understanding of the underlying constructs and theories on 5G networks and the business model concept. Practically, the study will benefit industry practitioners in implementing sustainable and viable business models that can support the deployment and operation of 5G networks.

Figure 1 is a flow chart showing the main steps used to organise the research study. This includes, problem identification, research question(s) formulation, selection of sampling methods, data collection procedures, data analysis and results, and interpretation and discussion of the results.

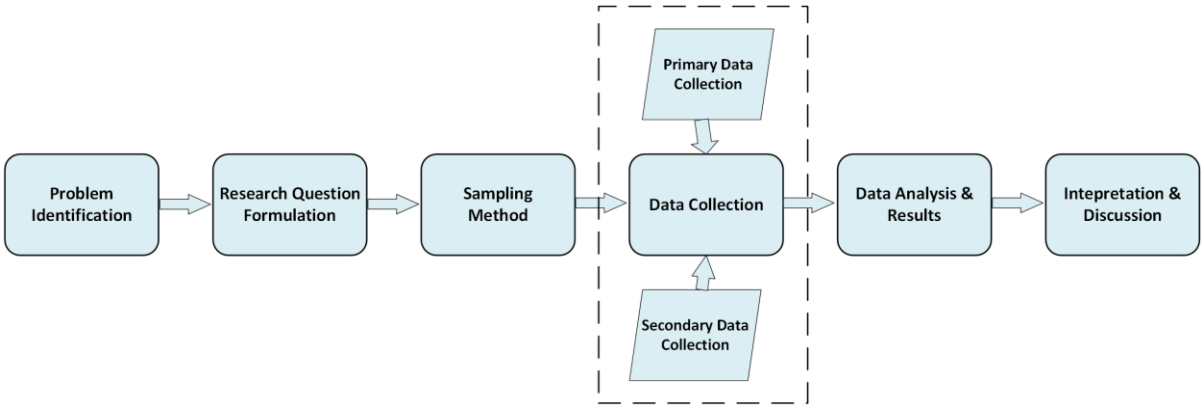


Figure 1: Main steps of the study

The rest of the paper is structured as follows: Section 2 reviews the related work in the extant literature. Section 3 presents the adopted research methodology while Section 4 presents the research results and analysis. Section 5 discusses the research findings and Section 6 concludes the article.

http://doi.org/10.18080/jtde.v13n3.1230

Related Work

The connection between economic growth and technological advancement in emerging markets can be potentially driven by the introduction of relevant 5G use cases, together with viable 5G business models and supportive regulatory frameworks (Coetzee, Mekuria, & du Toit, 2018; GSM-Association, 2016). In light of the academic publications on 5G networks and the business model concept, relevant related work has been reviewed to position the current study within the extant literature.

A comprehensive survey article on 5G business models for mobile operators was presented by Banda et al. (2022). The survey outlines several business models that are applicable to diverse types of mobile network operators including primary, secondary (virtual) public, private and micro mobile operators. Additionally, the survey authors highlighted the disruptive impact of non-cellular service providers such as over-the-top (OTT) service providers on existing and conventional business models for mobile operators. However, no primary data collection and analysis was conducted as the study was a theoretical survey.

Frank, *et al.* (2022) conducted a techno-economic analysis of business models for private 5G networks. The study focused on the cost structures and financial implications of deploying private 5G networks in rural and remote areas. However, in their analysis, the authors did not include other business model components such as value proposition, customer interface, infrastructure management and revenue models. Moreover, the study focused only on private 5G networks and therefore cannot apply to public 5G networks, which are prevalent in emerging markets.

A quantitative analysis of 5G business model components for mobile operators in Sub-Saharan Africa was conducted by Banda (2025). In this study, the author formulates a conceptual framework and related research hypothesis based on four 5G business model components: 5G services, 5G infrastructure management, 5G customer interface and 5G financial aspects. The study involved quantitative data collection through online survey questionnaires. Of the six research hypotheses formulated, four were significantly supported, while two were insignificant and therefore, rejected. The sample size of the study was only 62 participants, which is substantially small to yield valid and reliable findings when using a qualitative research approach.

An in-depth review article on 5G business models, use cases and cybersecurity has been outlined by Aranda, *et al.* (2021). The study conducts and presents computer simulation methods using physical testbeds for the research and development of potential 5G network proposals for the benefit of mobile operators, research institutions and policymakers. However, the study focused on the 5G business model based on network slicing technology.

http://doi.org/10.18080/jtde.v13n3.1230

Other emerging technologies such as the Internet of Things (IoT), artificial intelligence, machine learning, green communication, and digital platforms outlined in the standards by ITU-R (2015) were not considered.

The study by Pandian, *et al.* (2023) investigates a green business model ecosystem for 5G and 6G technologies. This work contributes by concluding that that while 5G and 6G technologies envision to inter-connect devices through the Internet, the study incorporates the aspects of environmental, social and financial sustainability. However, the proposed green business model framework was not elaborated in detail as the business model elements were not outlined.

Given the promise of 5G to deliver a range of services designed to address not only consumer-based smartphone applications, but also the diverse needs of vertical markets, several vertical markets partnership business models have been suggested (Banda *et al.*, 2022; Rao & Prasad, 2016). This includes smart learning (education), e-health (healthcare), smart farming (agriculture), smart grids (energy), smart cities (public), smart airports (aviation), smart factories (manufacturing), and so forth. These business models are applicable to various use cases where a mobile operator enters into a partnership with a specific industrial customer and develops a business-to-business-to-consumer (B2B2C) model. However, due to the lack of well-defined business cases for vertical-sectoral markets in emerging markets, the B2B2C model has not been fully exploited.

To contribute and complement the existing literature on 5G business models, this study is ideally placed to specifically address the impact of 5G networks on business models of mobile operators in emerging markets. Furthermore, the study uniquely combines the business model concept with technological innovation enabled by emerging 5G networks. Based on the literature reviewed and to the author's best knowledge, this research gap has received less attention from the scholarly community. Additionally, the use of MAXQDA24 software for qualitative data analysis on business models of 5G mobile operators in the context of emerging markets has rarely been considered in the existing literature. Therefore, this study makes a unique contribution in that respect.

Research Methodology

This study was conducted using a qualitative research method to investigate the factors that affect business models for mobile operators in enabling 5G networks in emerging markets. The study adopted an interpretivist research philosophy which is commonly used in qualitative research (Saunders, *et al.*, 2019). The theory development approach employed the inductive research method, which begins with data collection to investigate a phenomenon in order to develop a theory (Creswell & Creswell, 2018).

http://doi.org/10.18080/jtde.v13n3.1230

Population and Sampling Strategy

The population of interest for this study included, top executives (e.g. CEOs, CTOs, VPs and senior managers) as well as middle-level executives (e.g. project managers, principal engineers and technical specialists) of well-established mobile operators in emerging markets. A well-established company is described as a business with more than 1,000 employees (Jain, 2006).

LoBiondo-Wood & Haber (2017) define a sample as a subset of the research population selected to participate in a study for the purpose of data collection and analysis. Snowball sampling, a non-probability sampling technique was employed in this study as it is applicable to cases where samples with target characteristics are not easily accessible (Naderifar, *et al.*, 2017), which is typical in mobile communication environments. During snowball sampling, data is collected on a few located members of the target population. The researcher then asks these individuals to provide information from their known professional network (Babbie, 2020).

Research Design

The study was conducted in three phases using the qualitative research method proposed by Creswell & Creswell (2018). The study examined the factors that influence existing business models of 5G mobile operators in the context of emerging markets using a case study approach. The three phases of research design included, qualitative data collection, qualitative data analysis, and interpretation as illustrated in Figure 2.

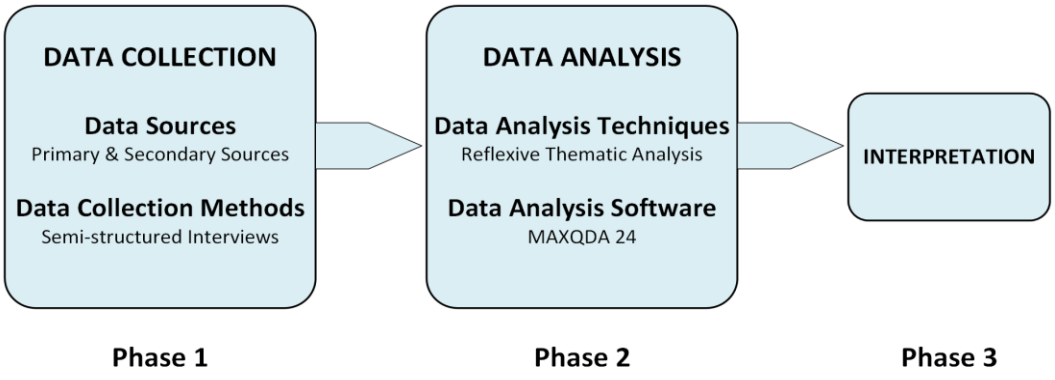


Figure 2: Research design of the study

Data Collection Method

Research data can generally be categorised into primary and secondary data (Ajayi, 2017; Saunders *et al.*, 2019). Primary data is one that is collected by researchers directly from the main sources, while secondary data is one that has already been collected through primary

http://doi.org/10.18080/jtde.v13n3.1230

sources and made readily available for researchers to use for their own investigation (Ajayi, 2017). This study incorporated both primary and secondary data sources.

Secondary data collection procedure

An extensive investigation and analysis of secondary data was undertaken on all relevant and current information regarding 5G business models for mobile operators in the context of emerging markets. Secondary data sources included: peer reviewed journal articles, conference proceedings, book chapters, academic books, equipment vendor publications, technical reports, and so forth. Secondary data was used to identify the research gap and to theorise the aim of the study.

Primary data collection procedure

A case study approach was used for primary data collection with 10 online semi-structured interviews planned and executed within eight emerging markets of the Sub-Saharan African region. This was an appropriate sample size to achieve the saturation recommended by (Glaser & Strauss, 2017). Research interviewing has the advantage of flexibility in terms of adapting, adopting and changing the questions as the researcher proceeds with the interviews (Creswell & Creswell, 2018). In addition, as observed by Bell, *et al.* (2022), primary data collection via interviews allows to obtain the latest and accurate data directly from the sampling population for the purpose of the research study. This ensures data accuracy and reliability since data is collected objectively with careful planning by the researcher in order to gather information aimed at attaining the study's objective (Morse, *et al.*, 2002; Saunders *et al.*, 2019). Table 1 summarises the profiles of the research interview participants indicating the mobile operator (MO) case, position of the participant in company, participant's years of experience in the mobile industry and the duration of the interview.

Table 1: Profiles of the research interview participants

No.	MO Case	Position of Interviewee	Experience (Years)	Interview Duration
1	MO-A	Chief Technical Officer: Wireless Networks	25	50 min
2	MO-B	Managing Executive: Central Region	20	65 min
3	MO-B	Head of Department: Radio Networks	22	77 min
4	MO-C	Senior Manager: Strategic Network Planning	12	52 min
5	MO-D	Director: Corporate Strategy & Planning	17	70 min
6	MO-D	Chief Technical Officer (CTO)	15	42 min
7	MO-E	Managing Executive: Core & Transport Networks	19	53 min
8	MO-F	Project Director (PD)	18	52 min
9	MO-G	Manager: Radio Access Network Support	15	52 min
10	MO-H	Senior Manager: Network Design	17	58 min

http://doi.org/10.18080/jtde.v13n3.1230

Data Analysis and Results

Data analysis and interpretation techniques

According to Creswell & Creswell (2018), data analysis is the process of examining and moulding collected data for interpretation so as to discover relevant information, draw or propose conclusions and support decision-making to solve a research problem. Besides, data interpretation involves attaching meaning and significance to the analysis, explaining descriptive patterns, and looking for relationships and linkages among descriptive dimensions (Krueger, 2014).

The data analysis of this qualitative research study was conducted using reflexive thematic data analysis method proposed by Braun & Clarke (2019) and was implemented using the MAXQDA24 software. The six phases of reflexive thematic analysis suggested by Braun & Clarke (2019) were followed. These include data familiarisation, generation of initial codes, searching for themes, reviewing potential themes, defining and naming themes, and report writing. The six phases of reflexive thematic analysis are shown in Figure 3.

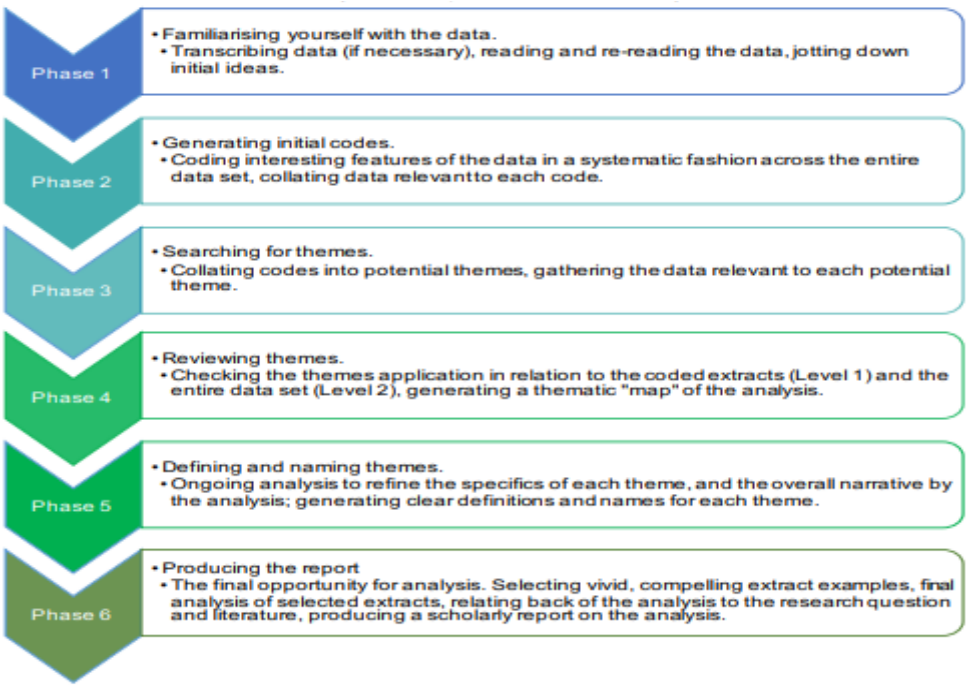


Figure 3: Reflexive thematic analysis (source: (Braun & Clarke, 2019))

http://doi.org/10.18080/jtde.v13n3.1230

Coding and theme generation in MAXQDA24 Software

Step 1: Creation of a project in MAXQDA24 software

A new project was created in the MAXQDA24 software and documents of transcribed data of the 10 research interviews were loaded into the software project. All the initial software parameters were set to their default values at this stage. The MAXQDA24 software project setup is shown in Figure 4.

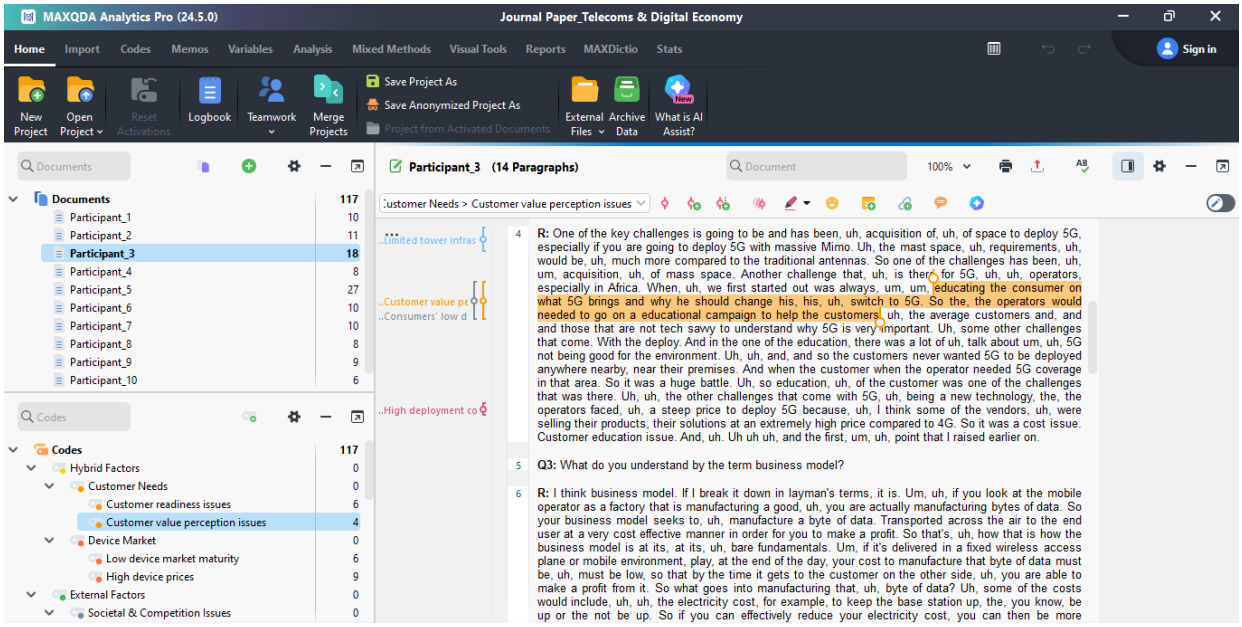


Figure 4: MAXQDA24 Software Project of the Current Study

Step 2: Coding Procedures

Initial codes were generated from transcribed data through an induction approach using the following MAXQDA 24 software features: *Paraphrasing* to ensure concise, precise and clear meaning of the coded data segments; *Memos* to assist in tracing back the original rationalisation when a new code is created from the previous coded segment; and *Comments* to give a high-level summary of the coded segment. The coding process involved reading the coded segment to ensure that overlapping codes are merged while the unnecessary ones are discarded. Figure 5 shows the final code frequency from the MAXDDA 24 software.

http://doi.org/10.18080/jtde.v13n3.1230

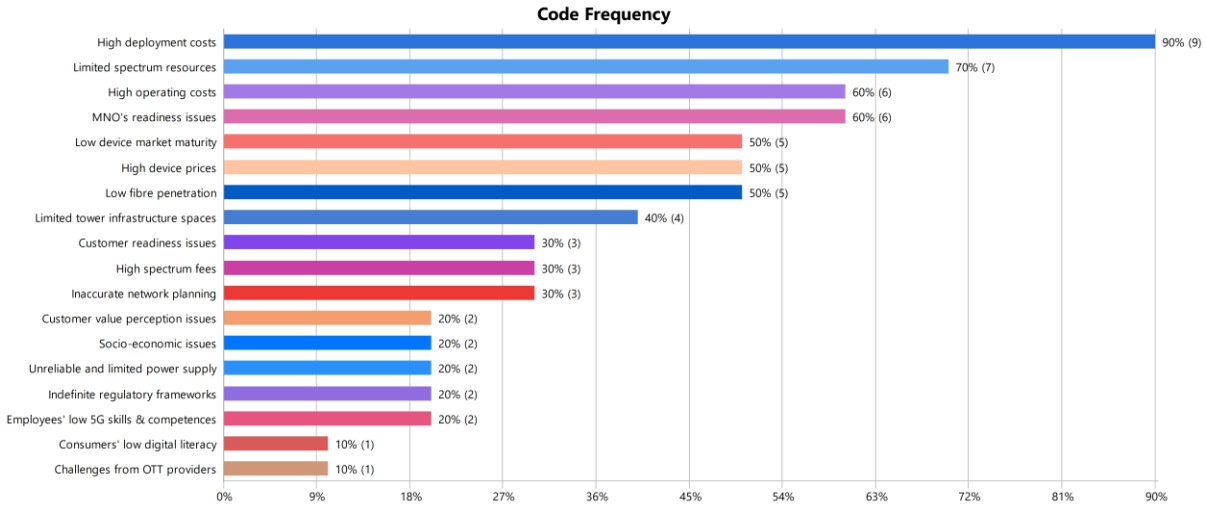


Figure 5: Final code frequency of the generated codes

Step 3: Assignment of codes to sub-themes and main themes

The generated codes were inductively grouped into sub-themes based on the factors impacting 5G mobile operators from the literature reviewed. The identified sub-themes included, customer needs, device market, societal and competition issues, infrastructure readiness, regulatory environment, financial resources, and organisational capabilities. In generating and reviewing emerging themes, it should be ensured that the main themes are not repeated and that overlapping themes and sub-themes are merged. To this end, Braun, *et al.* (2023) suggest that researchers should define and name themes only when they have a clear focus and address the research question(s) or objective(s). The Questions, Themes & Theories (QTT) visualisation feature of MAXQDA24 software assisted in maintaining focus on the study's research question after reaching the three main themes of the study: *Internal Factors*, *External Factors* and *Hybrid Factors*.

Figure 6 shows the relationship between the codes, sub-themes and main themes from the Code Matrix Browser of MAXQDA24 software.

http://doi.org/10.18080/jtde.v13n3.1230

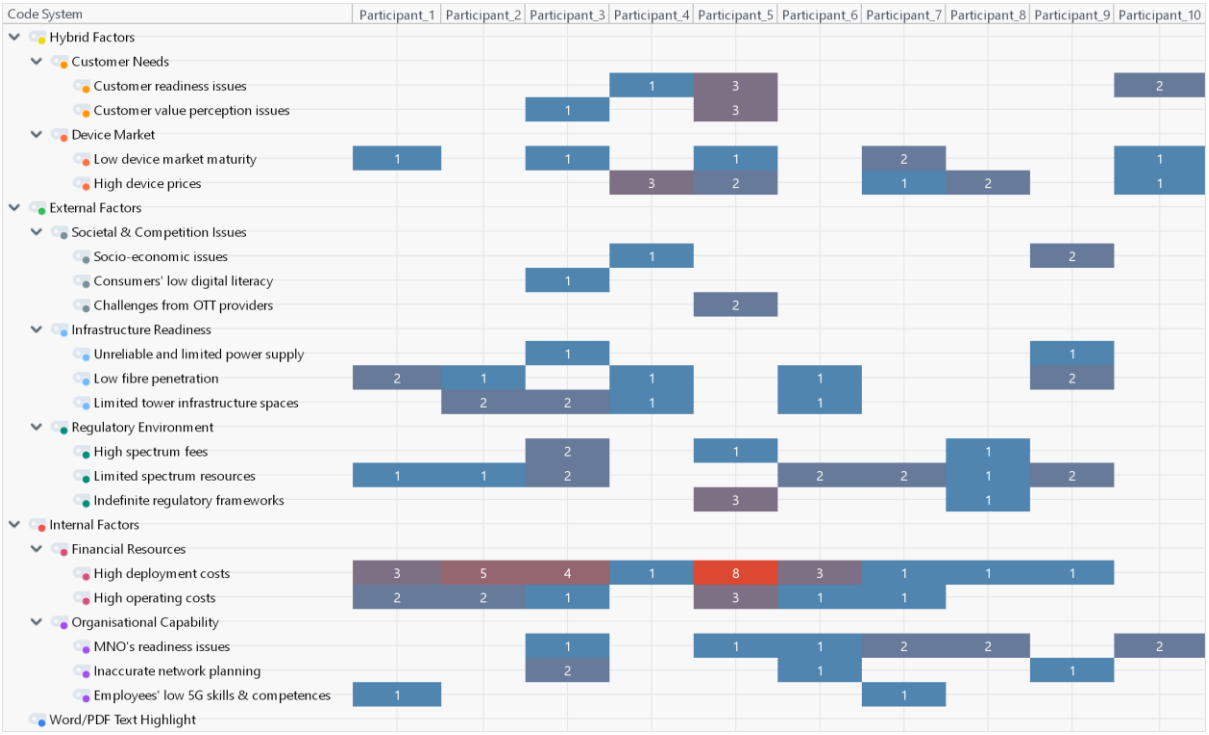


Figure 6: Code Matrix Browser showing codes, sub-themes and main themes

Figure 7 is the final thematic map of the study indicating the relationships between main themes and sub-themes.

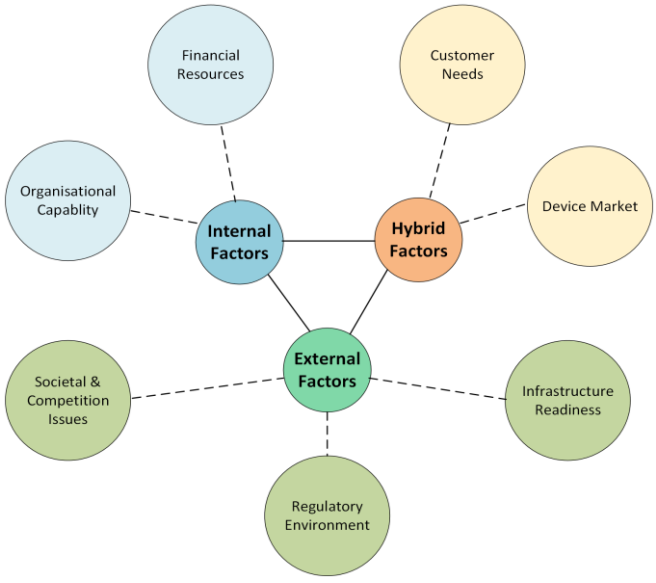


Figure 7: Final thematic map

Table 2 summarises the analysis table showing main themes, sub-themes, codes and the sample quotes of the interview participants.

http://doi.org/10.18080/jtde.v13n3.1230

Table 2: Summary of data analysis: Main Themes, Sub-Themes, Codes and Sample Quotes

Main Theme	Sub-Theme	Code	Sample Quote
Internal Factors	Financial Resources	High deployment costs	*The cost of deploying 5G will be high, and if the cost of deploying 5G is high, we will have to pass on that cost to the customers* (Participant_5, Pos. 10)
		High operating costs	*What I have observed that the OpEx for 5G is substantially higher that of 4G* (Participant_3, Pos. 6)
	Organisational Capability	Inaccurate network planning	*Due to wrong site design, you find that some 5G sites get congested due to high traffic while other sites carry low traffic, which affect operators revenues* (Participant_3, Pos. 6)
		MNO's readiness issues	*Challenges include the rapid pace of technological change which catches most operators unprepared* (Participant_8, Pos. 6)
		Employees' low 5G skills & competences	*Most engineers and technicians lack the technical skills on 5G. Operators must engage with vendors for staff knowledge transfer via training and on-site knowledge sharing* (Participant_1, Pos. 10)
External Factors	Societal & Competition Issues	Socio-economic issues	*Most 5G towers are built in densely populated areas where there is high youth unemployment which results in theft and vandalism of site tower equipment* (Participant_9, Pos. 15)
		Consumers' low digital literacy	*Another key challenge is low digital literacy in most African regions, especially in rural areas* (Participant_10, Pos. 9)
		Challenges from OTT providers	*OTTs are a threat to operator's revenues as they use operator's infrastructure for free. It is high time we started charging them* (Participant_5, Pos. 17)
	Infrastructure Readiness	Unreliable and limited power supply	*Loadshedding is a problem we have been grappling with for some years now. We need alternative energy solutions* (Participant_2, Pos. 12)
		Low fibre penetration	*Key challenges include spectrum shortages and pricing, as well as the lack of sufficient back-haul transmission resources due to limited fibre deployment* (Participant_9, Pos. 6)
		Limited tower infrastructure spaces	*Tower space is always an issue to deploy 5G, especially if you are going to deploy 5G with massive MIMO* (Participant_3, Pos. 4)
	Regulatory Environment	High spectrum fees	*Key challenges include spectrum shortages and pricing, as well as the lack of sufficient back-haul or transmission resources due to limited fibre deployment* (Participant_9, Pos. 6)
		Limited spectrum resources	*Key challenges include spectrum shortages and pricing, as well as the lack of sufficient back-haul or transmission resources due to limited fibre deployment* (Participant_9, Pos. 6)
		Indefinite regulatory frameworks	*As a continent, we are always lagging when it comes to regulation. As new technologies come onto the market, you will find that on the*

http://doi.org/10.18080/jtde.v13n3.1230

			regulatory side we are not prepared to provide a regulatory framework that governs the introduction and use of this new technology (Participant_5, Pos. 7)
Hybrid Factors	Customer Needs	Customer readiness issues	*Some people don't even know what 5G is about. So, there is a need to make them aware of 5G is. This can be done via roadshows and promotions such as TV or radio commercials as well as billboard advertisement* (Participant_10, Pos. 8)
		Customer value perception issues	*The best approach is to conduct in-depth research on the type and needs of a particular industry before loading them with multiple 5G services, some of which they may not even need* (Participant_10, Pos. 4)
	Device Market	Low device market maturity	*Most devices on the African market are not 5G-capable due to low market demand as 5G is still new on the continent* (Participant_1, Pos. 3)
		High device prices	*The cost of 5G-supporting devices is extremely high for most subscribers. Mostly because we don't manufacture 5G devices in Africa but rely on foreign devices from America, Europe, China, South Korea or Japan* (Participant_4, Pos. 4)

Result Presentation and Analysis of Main Themes and Sub-Themes

Main Theme 1: Internal Factors

This theme refers to the factors which affect mobile operator's business models internally as a result of 5G deployment. These factors arise from within the confines of the mobile operator and are not influenced by external sources. Two sub-themes have been identified on the basis of internal factors: financial resources and organisational capacity.

Financial Resources: This sub-theme summarises the financial implications of the resources used in the business model, including the high deployment costs and the high operating costs. Figure 8a and Figure 8b show the qualitative results of the financial resources sub-theme.

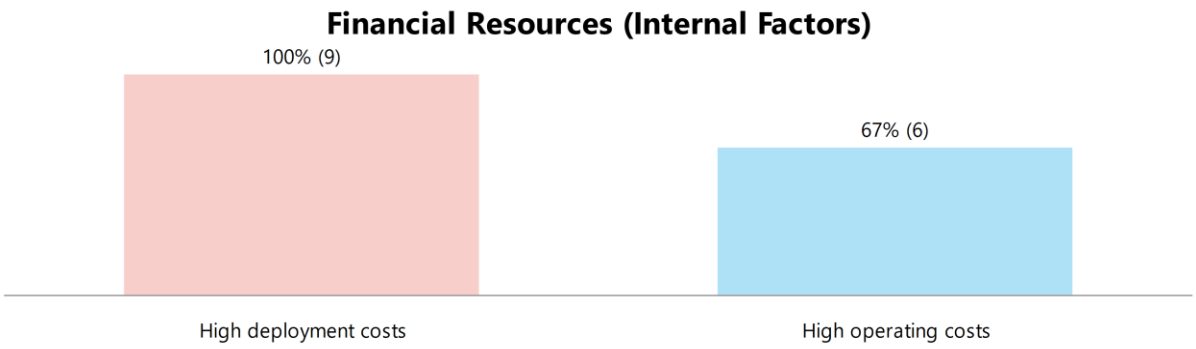


Figure 8a: Code Distribution for the Financial Resources Sub-Theme

http://doi.org/10.18080/jtde.v13n3.1230

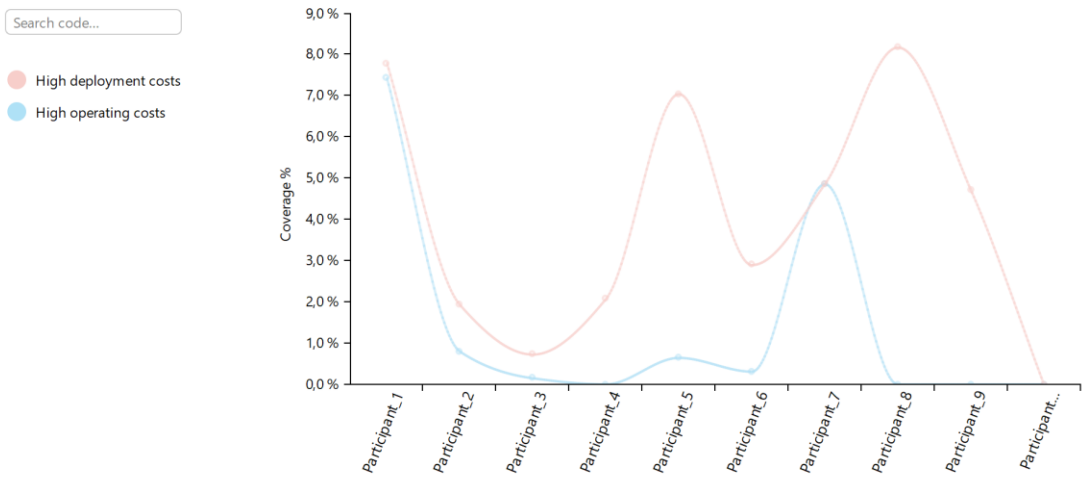


Figure 8b: Code Trends across Multiple Documents for the Financial Resources Sub-Theme

Organisational Capability: This sub-theme outlines the factors that influence a particular mobile network operator (MNO) to effectively perform its functions in order to meet its business objectives in the deployment of 5G. This includes, MNO's readiness issues, inaccurate network planning, and employees' low 5G skills and competencies.

Figure 9a and Figure 9b show the qualitative results of the organisational capability sub-theme.

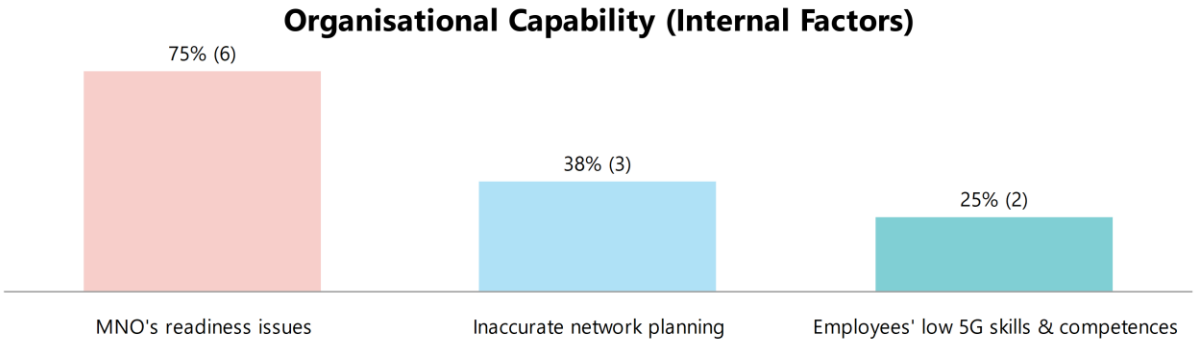


Figure 9a: Code Distribution for the Organisational Capability Sub-Theme

http://doi.org/10.18080/jtde.v13n3.1230

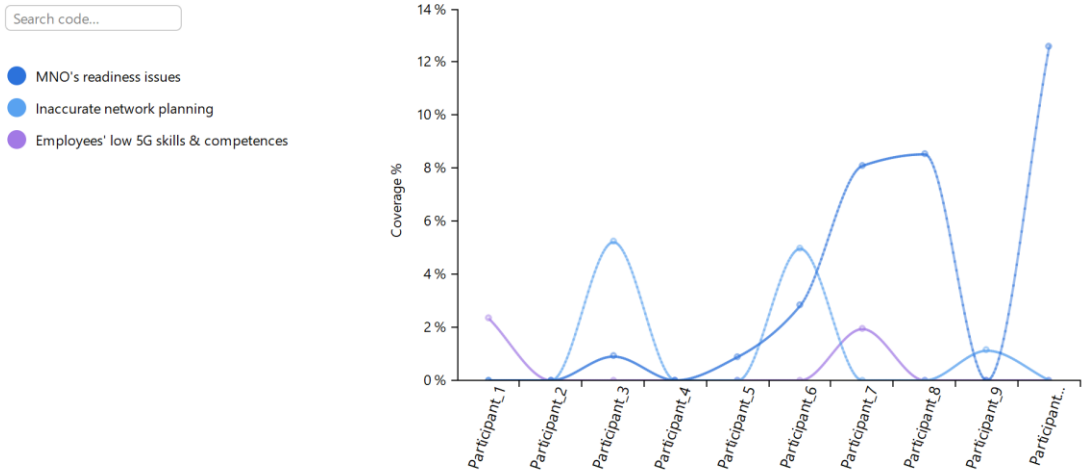


Figure 9b: Code Trends across Multiple Documents for the Organisation Capability Sub-Theme

Main Theme 2: External Factors

This theme refers to the factors which externally affect mobile operator's business models as a result of 5G deployment. External factors exist outside the confines of a specific MNO organisation. Three sub-themes were identified under this theme: Societal and Competition Issues, Infrastructure Readiness, and Regulatory Environment.

Societal and Competition Issues: This sub-theme highlights two external factors that influence the business models of mobile operators during the deployment of 5G networks. Societal issues are mainly related to the socio-economic challenges, inadequate communication infrastructure, high unemployment rate, unfavourable business and political atmosphere in several emerging economies. Competition issues arise from external market competitors including, non-traditional service providers such as over-the-top (OTT) service providers. Figure 10a and Figure 10b show the qualitative results of the societal and competition issues sub-theme.

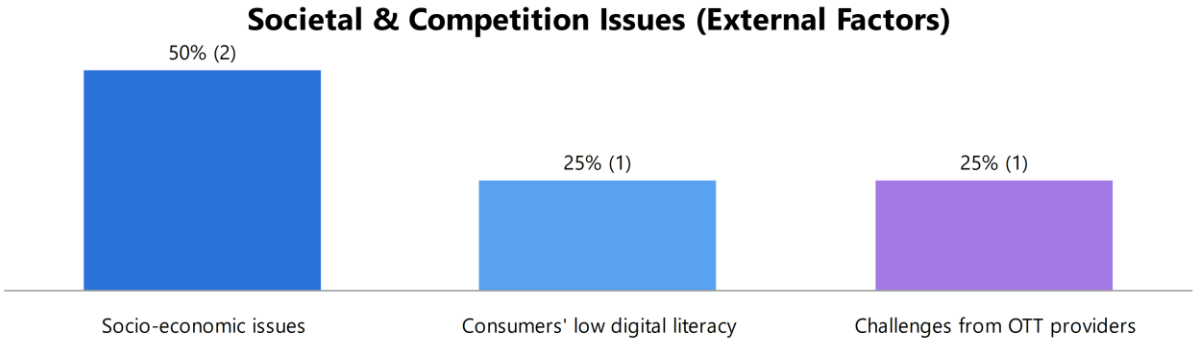


Figure 10a: Code Distribution for the Societal and Competition Issues Sub-Theme

http://doi.org/10.18080/jtde.v13n3.1230

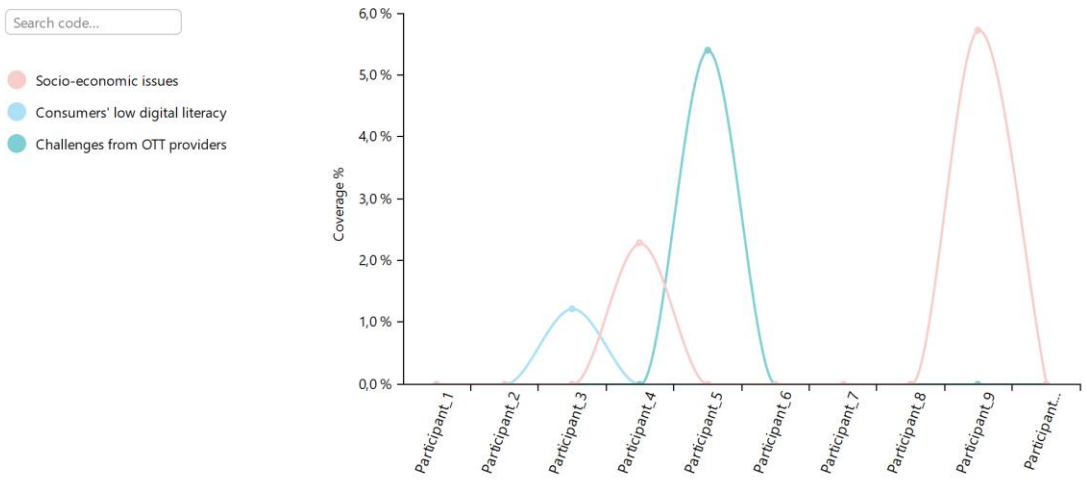


Figure 10b: Code Trends across Multiple Documents for the Societal and Competition Issues Sub-Theme

Infrastructure Readiness: This sub-theme identifies factors that impact MNO's business models due to inadequate or sub-standard communication infrastructure during the rollout of 5G networks. Examples include unreliable and limited power supply due to load-shedding, low fibre penetration for the 5G back-haul network and limited tower space infrastructure for installing 5G equipment such as radios and antennas.

Figure 11a and Figure 11b show the qualitative results of the infrastructure readiness sub-theme.

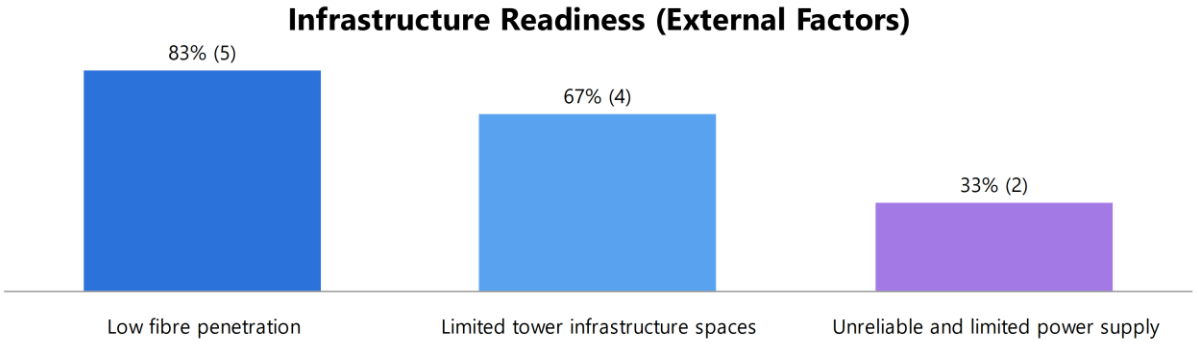


Figure 11a: Code Distribution for the Infrastructure Readiness Sub-Theme

http://doi.org/10.18080/jtde.v13n3.1230

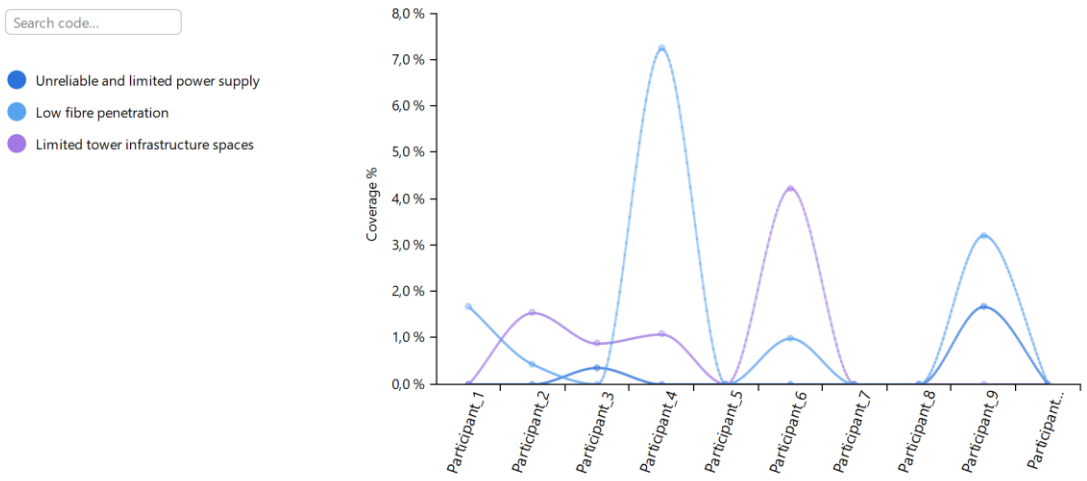


Figure 11b: Code Trends across Multiple Documents for the Societal and Competition Issues Sub-Theme

Regulatory Environment: This sub-theme indicates the factors that impact MNO's business models arising from the existing national regulations and policies when 5G deployment takes effect. Regulatory environment factors include high spectrum fees, limited spectrum resources, and indefinite regulatory frameworks.

Figure 12a and Figure 12b shows the qualitative results of the regulatory environment sub-theme.

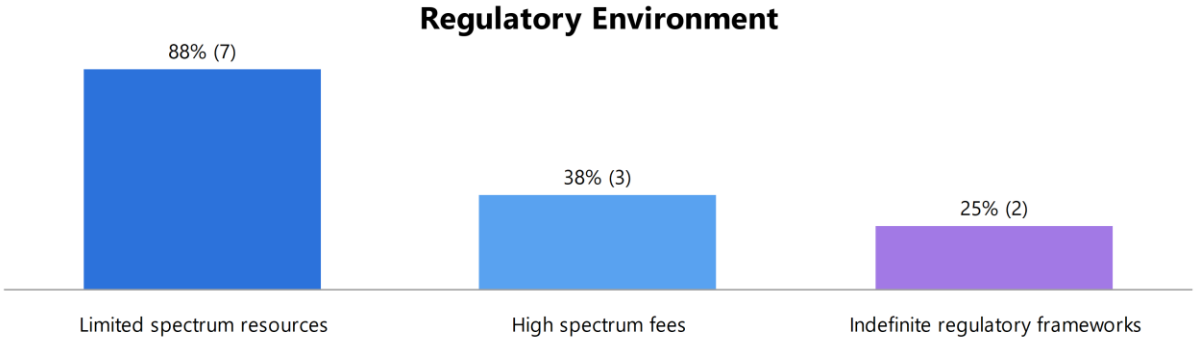


Figure 12a: Code Distribution for the Regulatory Environment Sub-Theme

http://doi.org/10.18080/jtde.v13n3.1230

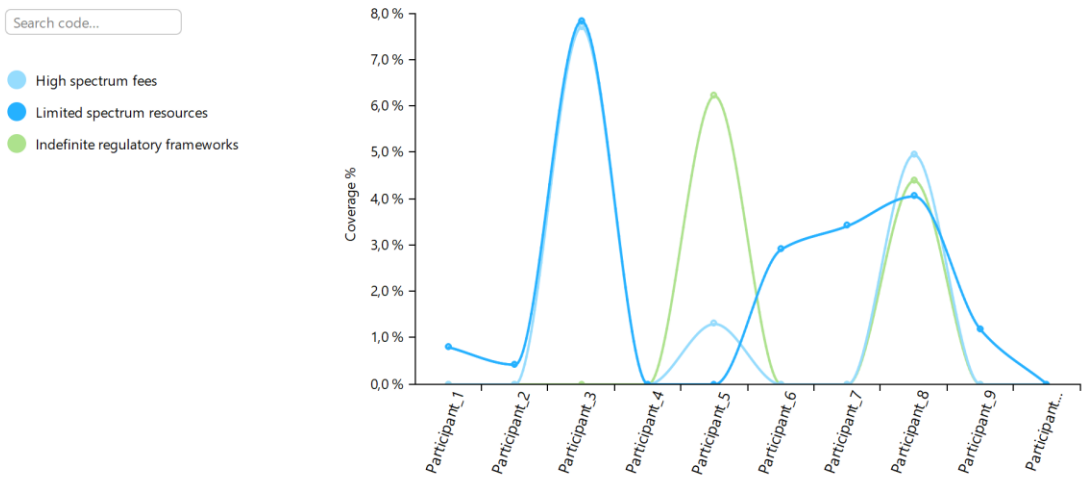


Figure 12b: Code Trends across Multiple Documents for the Regulatory Environment Sub-Theme

Main Theme 3: Hybrid Factors

This theme indicates the factors that simultaneously exhibit both internal and external impacts on the business models of mobile operators enabled by 5G deployment. Therefore, hybrid factors can be triggered either from within or from outside the boundaries of a particular MNO organisation. The following hybrid factors' sub-themes were identified: Customer's Needs and Device Market.

Customer's Needs: This sub-theme describes the factors that impact the MNO's business models due to specific customer's needs and requirements. Customer's needs vary based on customer categories including commercial, industrial, residential or individual. Customer's needs are influenced by customer's readiness and value perception issues in the era of 5G.

Figure 13a and Figure 13b show the qualitative results of the customer's needs sub-theme.

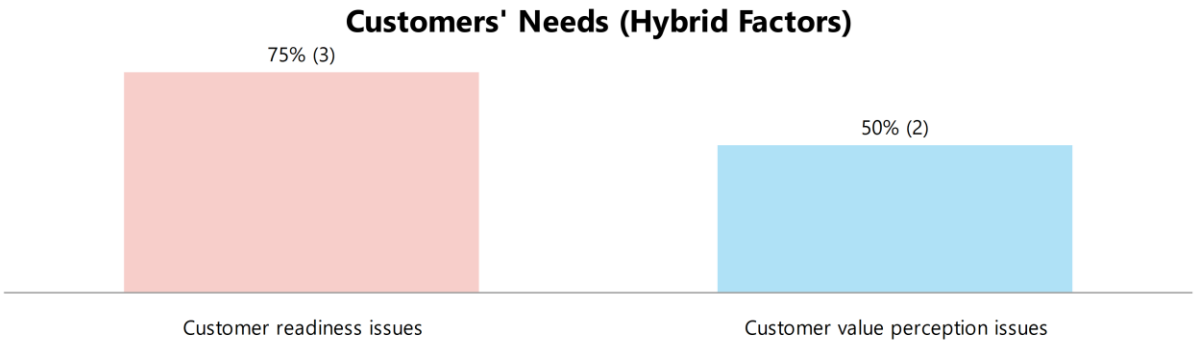


Figure 13a: Code Distribution for the Customer's Needs Sub-Theme

http://doi.org/10.18080/jtde.v13n3.1230

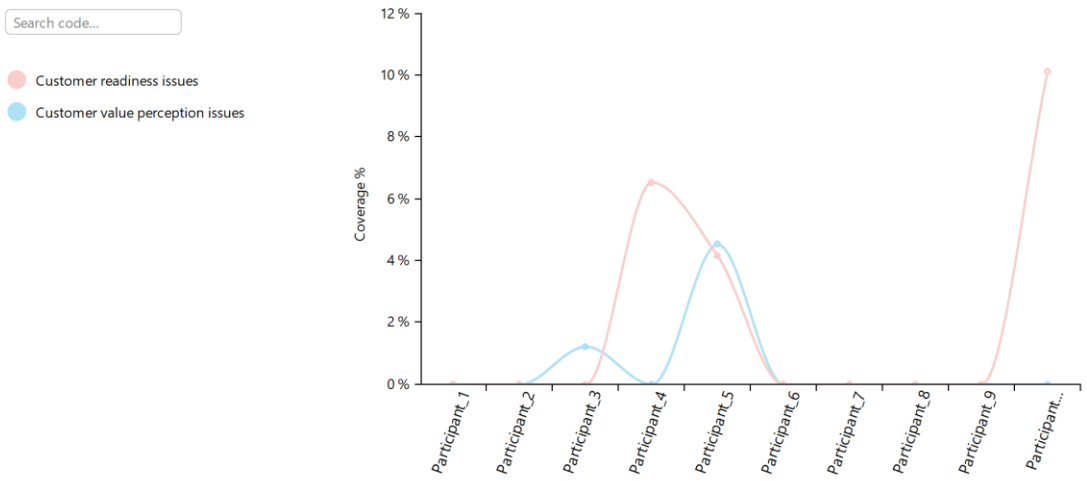


Figure 13b: Code Trends across Multiple Documents for the Customer's Needs Sub-Theme

Device Market: This sub-theme indicates the factors that impact the MNO's business models as the result of market penetration of 5G-enabled in emerging economies. Key identifies influences are low device market maturity leading to low device availability and high device prices resulting in low device affordability among the mass market customers.

Figure 14a and Figure 14b show the qualitative results of the device market sub-theme.

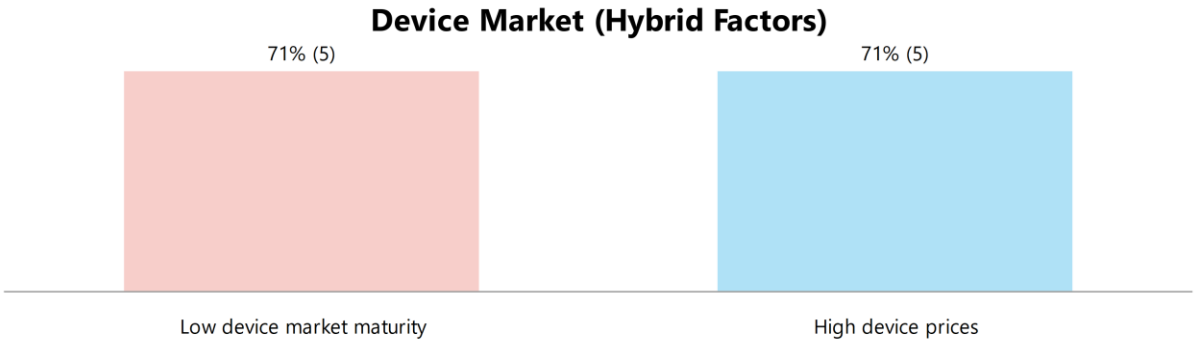


Figure 14a: Code Distribution for the Device Market Sub-Theme

http://doi.org/10.18080/jtde.v13n3.1230

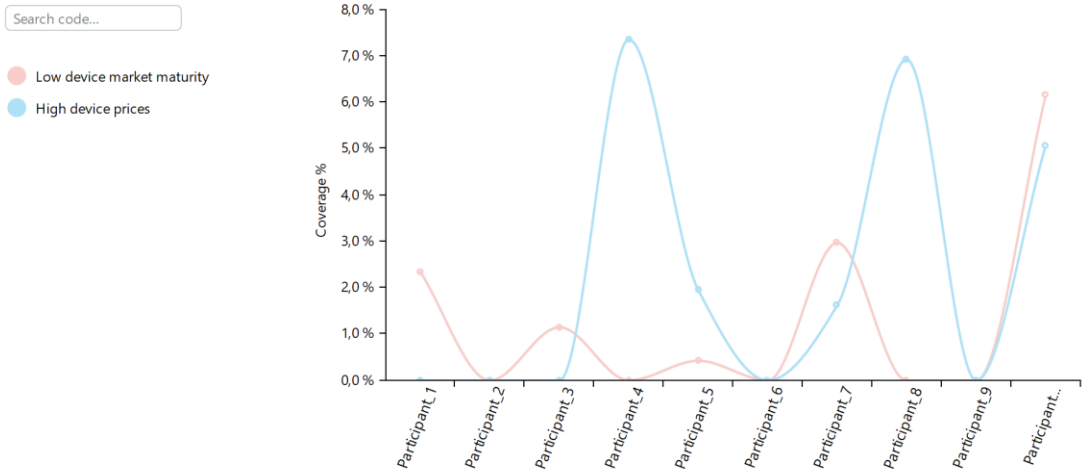


Figure 14b: Code Trends across Multiple Documents for the Device Market Sub-Theme

Code Frequencies Across 10 Interview Participants per Theme

The code frequencies across all the 10 interviews per theme were categorised and summarised within the MAXQDA24 software project and results are shown in Figure 15a, Figure 15b, and Figure 15c.

Theme 1: Internal Factors

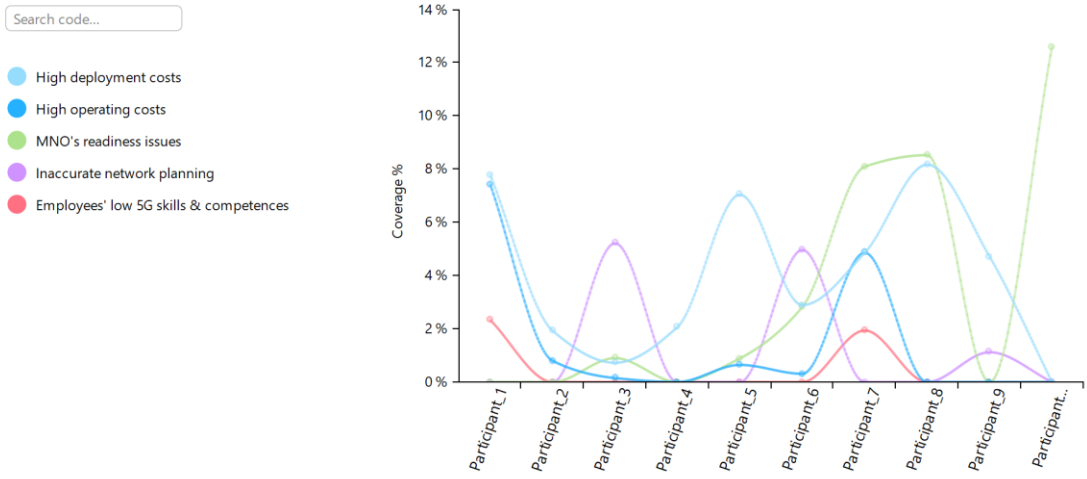


Figure 15a: Code Trends across 10 participants for the Internal Factors Main Theme

http://doi.org/10.18080/jtde.v13n3.1230

Theme 2: External Factors

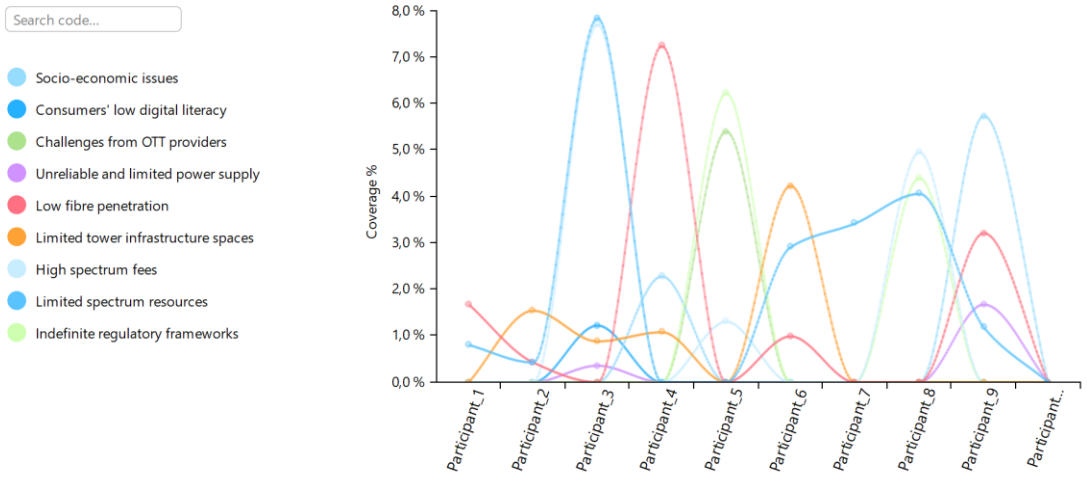


Figure 15b: Code Trends across 10 participants for the External Factors Main Theme

Theme 3: Hybrid Factors

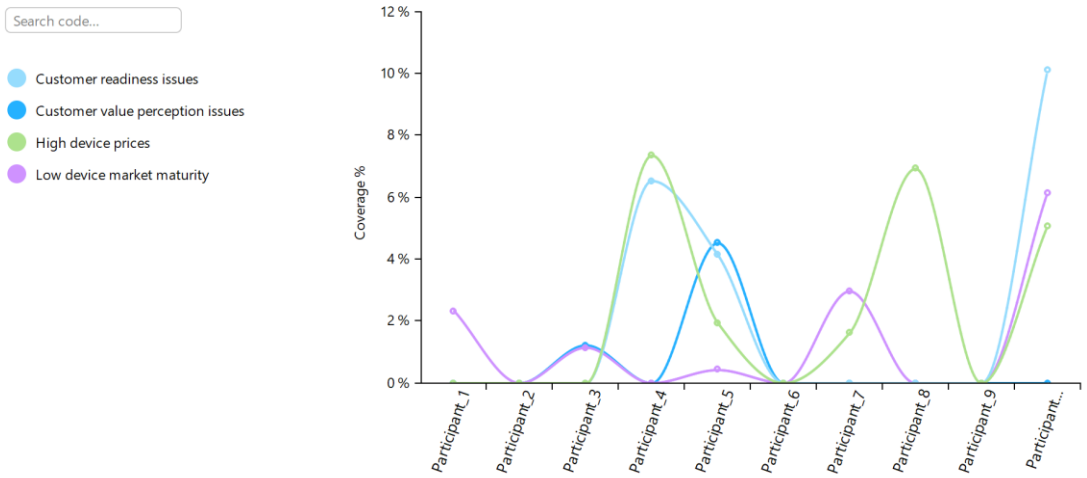


Figure 15c: Code Trends across 10 participants for the Hybrid Factors Main Theme

Descriptive Statistics – Main Themes, Sub-Themes and Codes

The descriptive statistics showing the main themes, sub-themes and codes generated during the data analysis of the study were compiled and summarised using the 'stats' functionality window of the MAXQDA24 software projects. Table 3 illustrates the descriptive statistics of the main themes, sub-themes and codes from the MAXQDA24 software.

http://doi.org/10.18080/jtde.v13n3.1230

Table 3: Descriptive Statistics – Main Themes, Sub-Themes and Codes

Theme	Sub-Theme	Code	N	Mean	SD (samp.)	Mean lower b. (95%)	Mean upper b. (95%)	Missing	Missing (%)
Internal Factors	Financial Resources	High operating costs	10	1,00	1,000	0,25	1,75	0	0,00
		High deployment costs	10	2,70	2,326	0,95	4,45	0	0,00
	Organisational Capability	Employees' low 5G skills & competences	10	0,20	0,400	-0,10	0,50	0	0,00
		Inaccurate network planning	10	0,40	0,663	-0,10	0,90	0	0,00
		MNO's readiness issues	10	0,90	0,831	0,27	1,53	0	0,00
External Factors	Infrastructure Readiness	Unreliable and limited power supply	10	0,20	0,400	-0,10	0,50	0	0,00
		Limited tower infrastructure spaces	10	0,60	0,800	0,00	1,20	0	0,00
		Low fibre penetration	10	0,70	0,781	0,11	1,29	0	0,00
	Regulatory Evironment	High spectrum fees	10	0,40	0,663	-0,10	0,90	0	0,00
		Indefinite regulatory frameworks	10	0,40	0,917	-0,29	1,09	0	0,00
		Limited spectrum resources	10	1,10	0,831	0,47	1,73	0	0,00
	Societal & Competition Issues	Consumers' low digital literacy	10	0,10	0,300	-0,13	0,33	0	0,00
		Challenges from OTT providers	10	0,20	0,600	-0,25	0,65	0	0,00
		Socio-economic issues	10	0,30	0,640	-0,18	0,78	0	0,00
Hybrid Factors	Customer Needs	Customer value perception issues	10	0,40	0,917	-0,29	1,09	0	0,00
		Customer readiness issues	10	0,60	1,020	-0,17	1,37	0	0,00
	Device Market	Low device market maturity	10	0,60	0,663	0,10	1,10	0	0,00
		High device prices	10	0,90	1,044	0,11	1,69	0	0,00

Summary analysis of primary and secondary data sources

Regarding the challenges and limitations impacting business models for mobile operators, both the primary data sources (interview respondents) and secondary data sources (literature review) covered comparable aspects: deployment costs, exorbitant spectrum prices, unavailability and unaffordability of 5G devices, inadequate 5G infrastructure (e.g., low fibre penetration), societal issues (e.g., crime and vandalism), unreliable power supply (e.g., frequent loadshedding) and impact of over-the-top (OTT) service applications on the operator's current business models (Agubor, *et al.*, 2021; Ahmad *et al.*, 2024; Banda *et al.*, 2022; Gupta, 2024; Indoria, 2020). However, some topics covered in the literature review were not addressed by any of the interview participants. These include impact of disruptive non-cellular broadband technologies such as WiFi-6 (Oughton *et al.*, 2021), challenges posed by outsourced and managed service models (Rao & Prasad, 2016), challenges caused by new market acquisition models (Dhir, *et al.*, 2020), and limitations of current business-to-business (B2B) and business-to-consumer (B2C) models (Iankova, *et al.*, 2019).

Discussion of Research Findings

The three main themes (i.e. internal factors, external factors and hybrid factors) describe the factors that impact business models of mobile operators due to the disruptive nature of 5G networks in emerging markets. Internal factors are challenges and constraints that arise within a specific mobile operator organisation. External factors refer to the challenges and constraints that exist outside the boundaries of a particular mobile operator organisation. Hybrid factors are those that exhibit both internal and external influences the business models of mobile operators enabled by the deployment of 5G networks.

http://doi.org/10.18080/jtde.v13n3.1230

Internal Factors

Financial Resources (High 5G Deployment Costs and high Operating Costs)

The results in Figure 8a and Figure 8b show that in terms of financial resources, high deployment costs impact the operator's business models more than the related high operating costs during the deployment and operation of 5G networks. The deployment of 5G and its use cases are capital intensive because during network integration, many legacy network nodes need to be replaced or upgraded before the full potential of 5G can be realised (El Rhayour & Mazri, 2019; Liu *et al.*, 2020). This is a major challenge in emerging markets where most mobile operators are price-sensitive (Elaluf-Calderwood, 2024). Furthermore, the investment capital in 5G is substantially high because the equipment and service solutions are significantly more expensive compared to the previous 4G and 3G networks (Sirotkin, 2020). In addition, the challenge of 5G as a new technology is that mobile operators face high costs of introducing 5G as some equipment manufacturers sell their products and solutions at extremely high prices compared to the previous 4G and 3G technologies (Sirotkin, 2020). Finally, most operators in developing economies incur higher operating costs due to equipment theft, unstable power supply and other socio-economic challenges (Garba *et al.*, 2022). Therefore, the high deployment and operational costs faced by mobile operators have a significant impact on their cost structures.

Organisational Capability (Inaccurate Network Planning, MNO's Readiness Issues, and Employees' Low 5G Skills and Competences)

From the results on organisational capability shown in Figure 9, when 5G is deployed, the mobile operator's readiness issues have a significant impact on the operator's business models. Inaccurate network planning has a moderate impact while employees' low 5G skills and competences have a marginal impact on the business models.

Employees' Low 5G skills and competences

As an emerging network technology, the deployment and adoption of 5G requires the cultivation and development of new skills and competences in the mobile operator's staff. However, most mobile operators face an internal challenge of insufficient 5G technical skills and competences in their staff. This is partly due to the low human development indices (HDIs) in most emerging markets and low investment in research and development (R&D) by most operators (Okeleke *et al.*, 2019). 5G skills and competencies can be enhanced through partnerships and exchange programs between operators in emerging markets and their counterparts in developed markets (Forge & Vu, 2020).

http://doi.org/10.18080/jtde.v13n3.1230

Mobile operator's readiness issues

The disruptive and peculiar nature of 5G for established business models presents mobile operators with a major challenge. Therefore, the lack of preparation and reluctance to embrace the techno-economic transformation resulting from 5G without compromising the interests of key stakeholders remains one of the biggest challenges for mobile operators. A mobile operator's lack of preparation or improper strategic planning can significantly impact the key activities of the business model's infrastructure management (Banda *et al.*, 2022). Therefore, to remain competitive and contribute to the growth of emerging 5G networks, operators should have the flexibility to rethink their current business model.

Inaccurate network planning

An incorrect approach to network planning by the mobile operator could lead to one of these two internal challenges (Mishra, 2018): (1) the deployed base stations can hardly transmit mobile traffic and therefore generate only minimal revenue, which affects the revenue model of the business model; or (2) the deployed base stations carry overwhelmingly high mobile traffic and are therefore congested resulting in customer service dissatisfaction, which impacts the customer interface component of the business model. To address such challenges, the business model should consider incorporating scientific principles in network planning and dimensioning (Moreno-Cardenas, *et al.*, 2024).

External Factors

Societal and Competition Issues (Socio-economic Issues, Consumers' Low Digital Literacy, and Challenges from OTT Providers)

Regarding societal and competition issues during 5G deployment, Figure 10 shows that socio-economic issues have a significant impact on the operator's business models, as compared to consumers' low digital literacy or challenges posed by OTT providers.

Socio-economic issues: Most of radio base stations are deployed in densely populated areas facing socio-economic challenges such as high levels of unemployment and poverty. Mobile operators face challenges such as limited access to sites during network rollout or network maintenance (Garba *et al.*, 2022). In addition, the implementation of security measures negatively leads to higher OpEx for operators due to equipment theft and vandalism, which impacts the cost structures of the business models. The other challenge for mobile operators is the significant infrastructure investments required given the scepticism about favourable business environments due to political instability in most developing countries (Ahmad *et al.*, 2024). Furthermore, 5G has been the subject of misconceptions in many countries, including emerging markets such as Sub-Saharan Africa. This has led to potential customers expressing

http://doi.org/10.18080/jtde.v13n3.1230

concerns about the technology and being reluctant to adopt 5G services once available in their markets (Okeleke, *et al.*, 2022). One of the concerns was the alleged link between COVID-19 and 5G mobile technology. Flaherty, *et al.* (2022) noted that this alleged link was promoted and widely shared on social media between 2020 and 2022, often in the form of maps showing the distribution of COVID-19 cases in 5G hotspots.

Consumers' low digital literacy

The low digital literacy of consumers in most developing countries, particularly in rural areas, represents is a key issue for most mobile operators when developing their business models (Ahmad *et al.*, 2024). Although there is relatively high mobile internet coverage in most parts of the emerging markets, most consumers in these regions cannot afford to go online as they lack the necessary digital skills and knowledge (Radovanović *et al.*, 2020). Mobile operators should therefore educate consumers on the importance of 5G and the variety of opportunities it can offer. This can be achieved through partnership networks with key stakeholders such as local authorities and national governments.

Challenges from OTT providers

The emergence of over-the-top (OTT) service applications (e.g., Facebook and WhatsApp) is impacting the mobile operator's business ecosystem as OTT players can offer these services without owning, leasing or operating the network infrastructure (Rao & Prasad, 2016). Therefore, the impact of OTT service applications, where operator's infrastructure is simply used as a pipe to run OTT services, poses a major challenge to the viability of existing business models. Mobile operator's business models are significantly impacted as their revenues are mainly from traditional mobile data consumption and not from OTT applications (Banda *et al.*, 2022). Additionally, traditional mobile voice and SMS business has decreased dramatically, which has led to further declines in mobile operator's revenues (Rao & Prasad, 2018).

Infrastructure Readiness (Low Fibre Penetration, Limited Tower Infrastructure Spaces, and Unreliable and Limited Power Supply)

As regards infrastructure readiness, the results in Figure 11a and Figure 11b show that the introduction of 5G significantly impacts operator's business model due to low fibre penetration, followed by limited tower infrastructure space and least influenced by unreliable and limited power supply in emerging markets.

Low fibre penetration

Fibre infrastructure, which predominantly supports the 5G transport network, has low penetration some emerging markets, particularly the Sub-Saharan African region (Handforth,

http://doi.org/10.18080/jtde.v13n3.1230

2019). Low fibre penetration significantly impacts the infrastructure management component of mobile operator's business model (DotEcon & Axon, 2018). In addition, the skewed socio-economic imbalance in many emerging economies leads mobile operators to target wealthy suburbs where fibre infrastructure is available, while ignoring the underdeveloped rural outskirts where fibre infrastructure is almost non-existent. Therefore, limited transmission resources due to low fibre penetration pose a major challenge for most operators in reinventing their business models in the 5G era.

Limited tower infrastructure spaces

The space requirements and load capacity of towers pose further major challenge, as most towers/masts are already overloaded with antennas and other radio equipment, exceeding the tower utilisation factor (Agiwal, *et al.*, 2016). In such cases, the operator should recover and replace the existing antennas with modern 5G-capable antennas, which are relatively costly to install. When using massive MIMO antennas, the problem of limited tower space is exacerbated as the space required would be much larger than traditional antennas (López-Pérez *et al.*, 2022). To this end, developing regions are witnessing a new wave of tower deals as operators explore new network infrastructure models and seek further operational efficiencies in the context of the network densification requirements of 5G (Okeleke & Joiner, 2023). Mobile operators are now partnering with tower companies who are playing a vital role in the rollout of 5G services in developing and emerging economies. Apart from managing tower assets acquired from operators, several tower companies are also involved in the construction of new sites, which is essential for network densification, as well as investing in fibre infrastructure to connect new and existing sites (Okeleke *et al.*, 2022). For example, IHS Towers, which has completed the acquisition of a significant number of towers from MTN in South Africa and Airtel Africa, has entered into a sale-lease-back agreement with Helios Towers for some of its towers in Madagascar, Malawi, Chad, and Gabon (Okeleke *et al.*, 2022).

Unreliable and limited power supply

The energy consumption of 5G hardware equipment is relatively higher than that of previous technologies such as 3G and 4G (ITU-R, 2015). Most Sub-Saharan African countries have been experiencing energy deficits over the years, mainly due to industrialisation, urbanisation and population explosion (Kaseke & Hosking, 2013). Moreover, Kaseke & Hosking (2013) observed that most rural places in developing and emerging markets have no electricity at all. The unreliable and limited power supply has resulted in increased operating expenditure (OpEx) for operators as fuel-based generators and expensive batteries are used as backup power sources (Okeleke *et al.*, 2019). This ultimately has a significant impact on the cost structures of operator's existing business models (DotEcon & Axon, 2018).

http://doi.org/10.18080/jtde.v13n3.1230

Regulatory Environment (Limited Spectrum Resources, High Spectrum Fees, and Indefinite Regulatory Frameworks)

The results in Figure 12 show that from a 5G regulatory environment perspective, limited spectrum resources have a significant impact on operator's business models, followed by high spectrum fees, while indefinite regulatory frameworks have minimal impact.

Limited spectrum resources

The limited availability of spectrum is a major challenge for new entrants to the mobile communications market, such as micro-operators and private networks that require to develop their own business models (Ahokangas *et al.*, 2019). Regulators and policymakers should closely monitor the allocation and use of limited spectrum resources to ensure that the dominance of incumbent operators is not perpetuated (Taheribakhsh, *et al.*, 2020). Therefore, to meet users' growing and varying demands for services, dynamic and shared spectrum allocation mechanisms should be implemented between traditional mobile operators and new entrants (Mekuria & Mfupe, 2019). As a key resource component of infrastructure management, efficient spectrum allocation and utilisation is crucial for the viability of operator's business models. Regulatory authorities must therefore ensure in advance that relevant frequencies are retained for telecommunications players. This will avoid the delay in the auction process caused by disputes between industry and the regulator.

High spectrum fees

The acquisition of spectrum resources and operating licences by operators remains prohibitively expensive due to the enormous prices and fees charged by most regulators in emerging markets (Okeleke *et al.*, 2019). Furthermore, spectrum prices and operating licence fees in emerging markets are largely determined by regulations and policies aimed at maximising revenues for communication regulators and policymakers (Agubor *et al.*, 2021). This may result in lower investment by mobile operators, which may in turn lead to higher service prices for end-users. The exorbitant spectrum prices and licence fees have a drastic impact on the operator's cost structures and business models (DotEcon & Axon, 2018). To this end, regulators in emerging markets need to make policy changes such as allocating relevant spectrum and reducing tariffs to enable faster rollout of 5G.

Indefinite regulatory frameworks

The tendency of developing and emerging economies to lag behind in technological advancement can be partly attributed to the lack of clearly defined and supportive regulatory frameworks (Suryanegara, 2016). Since the standardisation of 5G, which was followed by mass global rollout, most developing countries have not yet established the necessary policies and regulations that would govern the deployment and adoption of these emerging technologies

http://doi.org/10.18080/jtde.v13n3.1230

(GSMA, 2019). Therefore, the regulatory uncertainties surrounding the deployment of 5G and underlying technologies such as cloud computing, edge computing, IoT, artificial intelligence and machine learning present challenges that extend beyond the boundaries of specific mobile operators. Uncertain regulatory frameworks have a huge impact on the key strategic partnerships between mobile operators and regulatory authorities (Banda *et al.*, 2022).

Hybrid Factors

Customer's Needs (Customer Readiness Issues and Customer Value Perception Issues)

According to the results in Figure 13a and Figure 13b, in terms of factors related to customer's needs, it was found that during 5G deployment, customer readiness issues impact operator's business models more than customer value perception issues.

Customers readiness issues

The low levels of customers readiness in adopting 5G is another challenge impacting operator's current business models. According to Okeleke *et al.* (2019), market factors such as urbanisation, digital literacy and GDP per capita have contributed to the lack of customer readiness for 5G adoption in emerging markets. Additionally, as previously outlined, complex issues related to device affordability, device availability and socio-economic challenges have significantly contributed to customer's unpreparedness for 5G adoption.

Customer value perception issues

Existing business models of mobile operators have long assumed that customers place value solely on data consumption. However, with the advent of 5G, the perception of customer value has evolved beyond mere data consumption, particularly for enterprise businesses and industry verticals whose goals include value delivery in the form of end-to-end solutions (DotEcon & Axon, 2018). Therefore, it is necessary to redesign and reinvent current business models in order to keep up with this shift in customer's value perception behaviour.

Device Market (High Device Prices and Low Device Market Maturity)

As regards the device market factors, the results in Figure 14a and Figure 14b show that both high device prices and low device market maturity have an equal impact on operator's business models in the deployment of 5G in emerging markets.

High device prices

Most users in emerging markets, particularly prepaid subscribers, find the cost of 5G-capable devices to be prohibitively high (Gepko, 2023). Therefore, affordability of devices is a challenge for most users, as 5G-enabled devices are relatively expensive on the mass market. Furthermore, Hatt & Jarich (2020) predict that the cost of 5G devices will remain excessively

http://doi.org/10.18080/jtde.v13n3.1230

high for most consumers in developing economies for the foreseeable future. This will impact operator's 5G revenues due to low mobile traffic for 5G services. The biggest challenge for device manufacturers in emerging markets is to produce devices at a low enough cost to gain market share, particularly in the 5G and 4G markets where devices remain extremely expensive for most regional consumers (GSMA, 2023). Some operators are trying to reach the low-income base by making 5G devices affordable by offering monthly contracts, thereby accommodating prepaid subscribers who are the majority of mobile service consumers (Maluleke, *et al.*, 2022).

Low device market maturity

Aside from the exorbitant costs, the maturity of the device market in developing countries is relatively low compared to other regions of the world. Slow network rollout in emerging markets has resulted in limited availability of 5G-supporting devices as device manufacturers are sceptical about achieving revenue growth in seemingly smaller and immature markets in emerging economies (Okeleke *et al.*, 2019). For instance, according to Okeleke *et al.* (2022), the adoption of 5G by consumers in Africa will depend to a large extent on the availability of devices. Moreover, Okeleke *et al.* (2022) emphasise that it is essential for tax authorities to reduce or eliminate import and exercise duties on 5G devices to accelerate the transition to enhanced broadband connectivity in emerging economies. Low device maturity impacts operator's mobile traffic profiles, which ultimately impacts their revenue generation.

Conclusions

5G networks and related technologies are envisaged to enable sustainable digital transformation and thus drive an inclusive digital economy, particularly in emerging markets. However, the adoption of 5G technologies has a disruptive effect on business models of mobile operators. This article presented the factors that impact business models of mobile operators in emerging markets due to the introduction of 5G. The study was conducted using a qualitative research method. Primary data was collected inductively through a case study approach with 10 semi-structured online interviews conducted from eight emerging markets in the Sub-Saharan region of Africa.

Based on the qualitative data collection and analysis procedures, the study concluded that internal, external and hybrid factors impact mobile operator's business models in the commercial deployment of 5G networks. The study identified internal factors that arise from with a particular mobile operator firm and include, (i) *financial resources* such as high 5G deployment and operating costs; and (ii) *organisational capability* such as mobile operator's readiness issues, inaccurate network planning, and employees' low 5G skills and competences. Furthermore, the study pointed out external factors as those that occur outside the boundaries

http://doi.org/10.18080/jtde.v13n3.1230

of a particular mobile operator organisation. External factors include, (i) *societal and competition issues* such as socio-economic challenges, consumers' low digital literacy, and challenges from OTT providers; (ii) *infrastructure readiness* such as low fibre penetration, limited tower infrastructure spaces, and unreliable and limited power supply; and (iii) *regulatory environment* such as limited spectrum resources, high spectrum fees, and indefinite regulatory frameworks. Finally, hybrid factors were identified as those that exhibit attributes of both internal and external factors. These include, (i) *customer's needs* such as customer's readiness issues and customer value perception; and (ii) *device market* factors such as low device market maturity and high devices prices.

In addition, this qualitative study observed some similarities and variations between primary data sources (interview respondents) and secondary data sources (literature review) on factors that impact business models of mobile operators in deploying 5G networks. Similarities included factors such financial resources (high deployment costs), regulatory environment (high spectrum fees), device market (high device prices), infrastructure readiness (low fibre penetration), societal and competition issues (unreliable power supply and impact of OTT providers. Nonetheless, variations between primary and secondary data sources observed as some topics covered in the literature review were not addressed by the interview respondents. These included the impact of non-cellular broadband technologies such as WiFi-6, impact of outsourced and managed service models, and the influence of new market acquisitions models.

Future research should consider developing a business model framework that can be quantitatively analysed by incorporating the identified factors of the current study to ensure that mobile operators in emerging markets remain economically viable and competitive with their counterparts in developing markets. In addition, the population sample for data collection should be extended beyond Sub-Saharan Africa to other emerging markets such as Latin America and South-East Asia.

References

Agiwal, M., Roy, A., & Saxena, N. (2016). Next generation 5G wireless networks: A comprehensive survey. *IEEE communications surveys & tutorials, 18*(3), 1617-1655. https://doi.org/10.1109/COMST.2016.2532458

Agubor, C. K., Chukwuchekwa, N., & Ezema, L. S. (2021). 5G Network Deployment in Nigeria: Key Challenges and The Way Forward. *European Journal of Engineering and Technology Research, 6*(3), 16-19. https://doi.org/10.24018/ejeng.2021.0.0.2068

Ahmad, I. A. I., Dawodu, S. O., Osasona, F., Akagha, O. V., Anyanwu, A. C., & Onwusinkwue, S. (2024). 5G deployment strategies: Challenges and opportunities: A comparative

review for Africa and the USA. *World Journal Of Advanced Research And Reviews, 21*(1), 2428-2439.

Ahokangas, P., Aagaard, A., Atkova, I., Yrjölä, S., & Matinmikko-Blue, M. (2023). Business models in 5G/6G mobile communications. In *The Changing World of Mobile Communications: 5G, 6G and the Future of Digital Services* (pp. 137-165): Springer International Publishing Cham. https://doi.org/10.1007/978-3-031-33191-6_6

Ahokangas, P., Matinmikko-Blue, M., Yrjölä, S., Seppänen, V., Hämmäinen, H., Jurva, R., & Latva-aho, M. (2019). Business models for local 5G micro operators. *IEEE Transactions on Cognitive Communications and Networking, 5*(3), 730-740. https://doi.org/10.1109/TCCN.2019.2902547

Ajayi, V. O. (2017). Primary sources of data and secondary sources of data. *Benue State University, 1*(1), 1-6.

Aranda, J., Sacoto Cabrera, E. J., Haro Mendoza, E. D., & Astudillo Salinas, F. (2021). 5G networks: A review from the perspectives of architecture, business models, cybersecurity, and research developments. *Novasinergia, 4*.

Babbie, E. R. (2020). *The practice of social research*: Cengage learning.

Banda, L. (2025). Analysis of 5G business model components for mobile network operators in Sub-Saharan Africa. *Journal of Engineering Research and Sciences, 4*(2), 1-10. https://doi.org/10.55708/js0402001

Banda, L., Mzyece, M., & Mekuria, F. (2022). 5G Business Models for Mobile Network Operators - A Survey. *IEEE Access, 10*(1), 94851-94886. https://doi.org/10.1109/ACCESS.2022.3205011

Bell, E., Bryman, A., & Harley, B. (2022). *Business research methods*: Oxford university press. https://doi.org/10.1093/hebz/9780198869443.001.0001

Braun, V., & Clarke, V. (2019). Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health, 11*(4), 589-597. https://doi.org/10.1080/2159676X.2019.1628806

Braun, V., Clarke, V., Hayfield, N., Davey, L., & Jenkinson, E. (2023). Doing reflexive thematic analysis. In *Supporting research in counselling and psychotherapy: Qualitative, quantitative, and mixed methods research* (pp. 19-38): Springer. https://doi.org/10.1007/978-3-031-13942-0_2

Campbell, K., Diffley, J., Flanagan, B., Morelli, B., O'Neil, B., & Sideco, F. (2017). The 5G economy: How 5G technology will contribute to the global economy. *IHS Economics and IHS Technology, 4*, 16.

Camps-Aragó, P., Delaere, S., & Ballon, P. (2019). *5G business models: Evolving mobile network operator roles in new ecosystems*. Paper presented at the 2019 CTTE-FITCE: Smart Cities & Information and Communication Technology (CTTE-FITCE). https://doi.org/10.1109/CTIT.2019.8894822

Chochliouros, I. P., Kostopoulos, A., Spiliopoulou, A. S., Dardamanis, A., Neokosmidis, I., Rokkas, T., & Goratti, L. (2017). *Business and market perspectives in 5G networks*. Paper presented at the 2017 Internet of Things Business Models, Users, and Networks. https://doi.org/10.1109/CTTE.2017.8260997

Coetzee, W., Mekuria, F., & du Toit, Z. (2018). Making 5G a reality for Africa. Retrieved from https://www.ericsson.com/assets/local/press-releases/africa/2018/5g-africa-report-11-2018.pdf

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.): Sage publications.

Dhir, S., Ongsakul, V., Ahmed, Z. U., & Rajan, R. (2020). Integration of knowledge and enhancing competitiveness: A case of acquisition of Zain by Bharti Airtel. *Journal of Business Research, 119*, 674-684. https://doi.org/10.1016/j.jbusres.2019.10.045

DotEcon, & Axon. (2018). *Study on Implications of 5G Deployment on Future Business Models*. Retrieved from https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/8008-study-on-implications-of-5g-deployment-0_0.pdf

El Rhayour, A., & Mazri, T. (2019). *5G Architecture: Deployment scenarios and options*. Paper presented at the 2019 International Symposium on Advanced Electrical and Communication Technologies (ISAECT). https://doi.org/10.1109/ISAECT.2019.9069723

Elaluf-Calderwood, S. (2024). *5G Telecom Infrastructure Investment in Technology Emergent Markets: An Economic Revision for Vendor Partners Selection*. Paper presented at the TPRC Conference Proceedings.

Flaherty, E., Sturm, T., & Farries, E. (2022). The conspiracy of Covid-19 and 5G: Spatial analysis fallacies in the age of data democratization. *Social science & medicine, 293*, 114546. https://doi.org/10.1016/j.socscimed.2021.114546

Forge, S., & Vu, K. (2020). Forming a 5G strategy for developing countries: A note for policy makers. *Telecommunications Policy, 44*(7), 101975. https://doi.org/10.1016/j.telpol.2020.101975

Frank, H., Colman-Meixner, C., Assis, K. D. R., Yan, S., & Simeonidou, D. (2022). Techno-economic analysis of 5G non-public network architectures. *IEEE Access, 10*, 70204-70218. https://doi.org/10.1109/ACCESS.2022.3187727

Garba, I. M., Oshiga, O., & Moriki, L. B. (2022). *Deployment, Standardization and Regulatory Challenges Of 5G Services In Africa: Nigeria As A Case Study*. Paper presented at the 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Lagos, Nigeria. https://doi.org/10.1109/NIGERCON54645.2022.9803120

Gepko, I. (2023). 5G Rollout Challenges and Opportunities for Frontier and Emerging Markets. *Radioelectronics and Communications Systems, 66*(3), 105-122. https://doi.org/10.3103/S0735272723040040

Glaser, B. G., & Strauss, A. L. (2017). *Discovery of grounded theory: Strategies for qualitative research*: Routledge. https://doi.org/10.4324/9780203793206

GSMA. (2016). 5g spectrum-public policy position. *GSM Assoc., London, UK, Tech. Rep*.

GSMA. (2019). *The 5G guide a reference for operators*. Retrieved from https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf

GSMA. (2023). *The Mobile Economy: Sub-Saharan Africa 2023*. Retrieved from https://www.gsma.com/mobileeconomy/wp-content/uploads/2023/10/20231017-GSMA-Mobile-Economy-Sub-Saharan-Africa-report.pdf

GSMA. (2024). *The Mobile Economy Sub Saharan Africa 2024*. Retrieved from https://www.gsma.com/mobileeconomy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf

Gupta, K. P. (2024). Understanding the challenges of 5G deployment in India. *Digital Policy, Regulation and Governance, 26*(1), 1-17. https://doi.org/10.1108/DPRG-02-2023-0031

Handforth, C. (2019). Closing the coverage gap: How innovation can drive rural connectivity. *GSMA Connected Society (GSMA)*. Retrieved from https://www.gsma.com/mobilefordevelopment/resources/closing-the-coverage-gap-how-innovation-can-drive-rural-connectivity/

Hatt, T., & Jarich, P. (2020). *Global Mobile Trends 2021. Navigating COVID-19 and beyond*. Retrieved from https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=58621970&file=141220-Global-Mobile-Trends.pdf

Iankova, S., Davies, I., Archer-Brown, C., Marder, B., & Yau, A. (2019). A comparison of social media marketing between B2B, B2C and mixed business models. *Industrial Marketing Management, 81*, 169-179. https://doi.org/10.1016/j.indmarman.2018.01.001

Indoria, S. (2020). *Deployment of 5G networks challenges for developing countries*. Paper presented at the ICT Analysis and Applications: Proceedings of ICT4SD 2019, Volume 2. https://doi.org/10.1007/978-981-15-0630-7_23

ITU-R. (2015). *IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond*. Retrieved from https://www.itu.int/rec/R-REC-2083

Jain, S. C. (2006). *Emerging economies and the transformation of international business: Brazil, Russia, India and China (BRICs)*: Edward Elgar Publishing. https://doi.org/10.4337/9781847202987

Kaseke, N., & Hosking, S. G. (2013). Sub-Saharan Africa electricity supply inadequacy: implications. *Eastern Africa Social Science Research Review, 29*(2), 113-132.

Krueger, R. A. (2014). *Focus groups: A practical guide for applied research*: Sage publications.

Liu, G., Huang, Y., Chen, Z., Liu, L., Wang, Q., & Li, N. (2020). 5G deployment: Standalone vs. non-standalone from the operator perspective. *IEEE Communications Magazine, 58*(11), 83-89. https://doi.org/10.1109/MCOM.2020.9269939

LoBiondo-Wood, G., & Haber, J. (2017). *Nursing research-e-book: methods and critical appraisal for evidence-based practice*: Elsevier Health Sciences.

López-Pérez, D., De Domenico, A., Piovesan, N., Xinli, G., Bao, H., Qitao, S., & Debbah, M. (2022). A Survey on 5G Radio Access Network Energy Efficiency: Massive MIMO, Lean Carrier Design, Sleep Modes, and Machine Learning. *IEEE communications surveys & tutorials, 24*(1), 653-697. https://doi.org/10.1109/COMST.2022.3143193

Maluleke, H., Bagula, A., Ajayi, O., & Chiaraviglio, L. (2022). An economic feasibility model for sustainable 5G networks in rural dwellings of south Africa. *Sustainability, 14*(19), 12153. https://doi.org/10.3390/su141912153

Mekuria, F., & Mfupe, L. (2019). *Spectrum sharing for unlicensed 5G networks*. Paper presented at the 2019 IEEE Wireless Communications and Networking Conference (WCNC). https://doi.org/10.1109/WCNC.2019.8885763

Mishra, A. R. (2018). *Fundamentals of network planning and optimisation 2G/3G/4G: evolution to 5G*: John Wiley & Sons. https://doi.org/10.1002/9781119331797

Moreno-Cardenas, E., Moreno, Y., & Barrial-Lujan, A. I. (2024). Strategic design of a business model for providing services over the 5G network in Peru. *Administrative Sciences, 14*(3), 55. https://doi.org/10.3390/admsci14030055

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International journal of qualitative methods, 1*(2), 13-22. https://doi.org/10.1177/160940690200100202

Naderifar, M., Goli, H., & Ghaljaie, F. (2017). Snowball sampling: A purposeful method of sampling in qualitative research. *Strides in development of medical education, 14*(3). https://doi.org/10.5812/sdme.67670

Okeleke, K., George, D., & Obiodu, E. (2019). *5G in Sub-Saharan africa: Laying the foundations*. Retrieved from https://data.gsmaintelligence.com/research/research/research-2019/5g-in-sub-saharan-africa-laying-the-foundations

Okeleke, K., & Joiner, J. (2023). *5G in Africa 2023 Market status, trends and outlook*. Retrieved from https://data.gsmaintelligence.com/research/research/research-2023/5g-in-africa-2023-market-status-trends-and-outlook

Okeleke, K., Joiner, J., & Kolta, E. (2022). *5G in Africa: realising the potential*. Retrieved from https://event-assets.gsma.com/pdf/5G-in-Africa.pdf

Oughton, E. J., & Lehr, W. (2022). Surveying 5G techno-economic research to inform the evaluation of 6G wireless technologies. *IEEE Access, 10*, 25237-25257. https://doi.org/10.1109/ACCESS.2022.3158068

Oughton, E. J., Lehr, W., Katsaros, K., Selinis, I., Bubley, D., & Kusuma, J. (2021). Revisiting wireless internet connectivity: 5G vs Wi-Fi 6. *Telecommunications Policy, 45*(5), 102127. https://doi.org/10.1016/j.telpol.2021.102127

Pandian, A. P. D., Lindgren, P., & Mihovska, A. D. (2023). Functioning Green Business Models For 6G Networking Technology By Epistemological Qualitative Research Method. *Journal of Survey in Fisheries Sciences, 10*(1S), 6342-6348.

Radovanović, D., Holst, C., Belur, S. B., Srivastava, R., Houngbonon, G. V., Le Quentrec, E., and Noll, J. (2020). Digital literacy key performance indicators for sustainable development. *Social inclusion, 8*(2), 151-167. https://doi.org/10.17645/si.v8i2.2587

Rao, S. K., & Prasad, R. (2016). Telecom Operators' Business Model Innovation in a 5G World. *Journal of Multi Business Model Innovation and Technology, 4*(3), 149-178. https://doi.org/10.13052/jmbmit2245-456X.431

Rao, S. K., & Prasad, R. (2018). Impact of 5G technologies on smart city implementation. *Wireless personal communications, 100*(1), 161-176. https://doi.org/10.1007/s11277-018-5618-4

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th Ed.): Pearson.

Schneir, J. R., Ajibulu, A., Konstantinou, K., Bradford, J., Zimmermann, G., Droste, H., & Canto, R. (2019). A business case for 5G mobile broadband in a dense urban area. *Telecommunications Policy, 43*(7), 101813. https://doi.org/10.1016/j.telpol.2019.101813

Shankar, V., & Narang, U. (2020). Emerging market innovations: Unique and differential drivers, practitioner implications, and research agenda. *Journal of the Academy of Marketing Science, 48*, 1030-1052. https://doi.org/10.1007/s11747-019-00685-3

Sirotkin, S. (2020). *5G Radio Access Network Architecture: The Dark Side of 5G*: John Wiley & Sons. https://doi.org/10.1002/9781119550921

Suryanegara, M. (2016). 5G as disruptive innovation: standard and regulatory challenges at a country level. *International Journal of Technology, 7*(4), 635-642. https://doi.org/10.14716/ijtech.v7i4.3232

Taheribakhsh, M., Jafari, A., Peiro, M. M., & Kazemifard, N. (2020). *5g implementation: Major issues and challenges*. Paper presented at the 2020 25th International Computer Conference, Computer Society of Iran (CSICC). https://doi.org/10.1109/CSICC49403.2020.9050110

World Bank Group. (2024). *Global Economic Prospects, June 2024*: World Bank Publications. https://doi.org/10.1596/978-1-4648-2058-8

Yrjölä, S., Ahokangas, P., & Matinmikko-Blue, M. (2018). *Novel context and platform driven business models via 5G networks*. Paper presented at the 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC). https://doi.org/10.1109/PIMRC.2018.8580819

A Lightweight Zero-Trust Architecture Implementation for Enhancing Cybersecurity in Small and Medium-Sized Enterprises

Truong Duy Dinh
Posts and Telecommunications Institute of Technology, Hanoi

Tran Duc Le
University of Wisconsin-Stout

Thi Thu Ha Nguyen
Posts and Telecommunications Institute of Technology, Hanoi

Hoang Giang Do
Posts and Telecommunications Institute of Technology, Hanoi

Abstract: Confronted by resource limitations and sophisticated cyber threats, Small and Medium Enterprises (SMEs) require tailored cybersecurity solutions. This research introduces and validates a Lightweight Zero-Trust Architecture (LZTA) specifically designed for SMEs. The proposed LZTA effectively integrates contextual access verification, multi-factor authentication, and role-based access control to ensure robust security without imposing excessive costs. Crucially, rigorous benchmarking demonstrated that the LZTA manages high-concurrency loads while significantly outperforming conventional and open-source Zero-Trust baselines in both response time and throughput. This work delivers a practical and high-performance blueprint for SMEs to adopt Zero-Trust principles, effectively balancing robust security with the operational constraints of smaller organisations.

Keywords: SMEs, Zero-Trust, Authorisation, Cybersecurity, Digital Ecosystem

Introduction

Small and Medium Enterprises (SMEs) are the backbone of the global economy, accounting for approximately 90% of businesses worldwide and over 50% of global employment (Worldbank, 2019). Despite their pivotal role, SMEs frequently operate with constrained financial and technical resources, leaving them particularly vulnerable to cyber threats. In 2024, cyber incidents such as ransomware attacks, IT outages, and data breaches were identified as the leading risks for SMEs globally, with 32% of respondents in a global survey citing cybersecurity as their top concern (Allianz, 2024b). The increasingly sophisticated and

http://doi.org/10.18080/jtde.v13n3.1284

evolving cyber threat landscape poses significant challenges for SMEs, which often operate with constrained budgets, limited IT expertise, and outdated security measures.

The most common types of cyberattacks affecting SMEs include malware (impacting 40% of SMEs in countries like Spain), ransomware (41% globally), and email fraud (36%) (Proofpoint, 2024). External threat actors – accounting for 62% of cybersecurity risks – pose a greater challenge than internal actors (31%) (Cisco, 2024a). Cyberattacks continue to pose severe risks to organisations, particularly SMEs, which often lack the resources to recover effectively. The average financial loss resulting from a data breach has risen sharply to $4.88 million globally, marking a 10% increase over the past year (IBM, 2024). Moreover, the consequences for SMEs are particularly dire – 70% of organisations experiencing a significant cyberattack report severe business disruptions, which can lead to long-term operational instability or closure within months (IBM, 2024).

Despite the growing threat, SMEs face substantial barriers in improving their cybersecurity defences. The three most significant challenges include low employee awareness (46%), a lack of qualified cybersecurity personnel (31%), and poor integration of security solutions (30%) (Cisco, 2024b; S-RM, 2023).

These statistics underscore the pressing need for more robust and systematic protection mechanisms that can be implemented within an SME's limited budget and expertise. Traditional perimeter-based cybersecurity models typically rely on the assumption that anything inside the organisational network perimeter can be trusted. In modern, distributed IT environments – marked by remote work arrangements, widespread use of cloud services, and increasingly sophisticated external threats – this perimeter-based approach has become inadequate. Once an attacker breaches the perimeter, lateral movement within the network frequently remains unchecked (Hasan, 2024; Kang *et al.*, 2023).

Zero Trust Architecture (ZTA), which operates on the principle of *'never trust, always verify',* has emerged as a paradigm shift in cybersecurity (Buck *et al.*, 2021; Rose *et al.*, 2020; Syed *et al.*, 2022). Unlike traditional perimetre-centric models, Zero Trust continuously authenticates and authorises each access attempt, regardless of network location. By enforcing continuous verification of users and devices, limiting access based on least privilege, and relying on contextual security policies, ZTA can address the unique vulnerabilities of SMEs (Kang *et al.*, 2023; Lund *et al.*, 2024).

Although Zero-Trust solutions have gained significant attention as an alternative, many existing implementations are resource-intensive and complex, requiring specialised skills and substantial investment – both of which pose formidable barriers for SMEs (Ghasemshirazi *et al.*, 2023). Additionally, most Zero-Trust frameworks cater to large

http://doi.org/10.18080/jtde.v13n3.1284

enterprises, leaving SMEs with limited guidance on how to adapt these robust strategies to their own resource constraints (Bashir, 2024; Hasan, 2024). As a result, SMEs continue to face rising cyber risks, including malware, ransomware, insider threats, and advanced persistent threats (APTs), but lack feasible roadmaps to adopt modern security strategies.

This research aims to design, implement, and evaluate a Lightweight Zero-Trust Architecture (LZTA) specifically tailored to the challenges and constraints of SMEs. It first seeks to develop a cost-effective and easily deployable Zero-Trust framework that accounts for SMEs' limited budgets and human resources. Next, it endeavours to demonstrate the feasibility and effectiveness of the proposed architecture by implementing it in a real-world or representative SME environment, where the focus lies on measuring improvements in security posture, particularly regarding threat mitigation and system resilience. Finally, the study aims to evaluate the architecture's performance under realistic conditions and use cases.

The remainder of this paper is organised as follows:

Following this introduction, Section 2 provides a **Literature Review** that explores the current cybersecurity landscape for SMEs, critically examines traditional security models, surveys existing Zero-Trust frameworks, and highlights the identified gaps that this research aims to address. Section 3 presents the detailed **Methodology**, outlining the design principles of the LZTA, specifying the technical environment and components used for its implementation, and describing the evaluation strategy used for testing its effectiveness. Section 4 then describes the **Proposed Lightweight Zero-Trust Architecture**, providing an in-depth look into its architecture. The subsequent section on **Prototyping and System Deployment** details the implementation steps taken, the specific technologies used. Section 6 outlines the **Testing and Validation** process, which included functional and performance evaluation of the architecture in a simulated SME environment. Section 7 – **Use Cases** – then addresses two common use cases in SMEs. Section 8 proceeds to the **Discussion.** The paper concludes with Section 9, the **Conclusions**, summarising the research contributions.

Literature Review

This section provides a comprehensive overview of the cybersecurity landscape in SMEs. We will analyse existing cybersecurity solutions, discuss the traditional versus zero-trust security models, and explain why Zero Trust could effectively address the cybersecurity gaps faced by SMEs.

http://doi.org/10.18080/jtde.v13n3.1284

SMEs are increasingly becoming targets for cyberattacks due to limited resources and expertise. Recent surveys indicate that 32% of SMEs worldwide identify cyber incidents as their top business risk in 2024, underscoring a rapidly evolving threat landscape that affects organisations of all sizes (Allianz, 2024a; NAVEX, 2024). This vulnerability is exacerbated by insufficient budgets and a lack of specialised IT personnel, with 31% of SMEs reporting difficulties in hiring qualified cybersecurity staff (Shojaifar & Järvinen, 2021). Additionally, 46% of SMEs attribute at least part of their susceptibility to low security awareness among employees, which enables threats such as phishing, social engineering, and insider attacks to take root more easily (Gani & Fernando, 2023). Breaches can result in substantial financial damage – often reaching hundreds of thousands or even millions of dollars in losses and may lead to long-term reputational harm and possible legal consequences (Manzoor *et al.*, 2024; Oluokun *et al.*, 2024). Alarmingly, some studies report that up to 60% of small businesses shut down within six months of a significant cyberattack (NAVEX, 2024). These statistics collectively highlight the necessity for tailored, robust, and efficient cybersecurity measures in the SME sector.

In response, SMEs have traditionally implemented a variety of point solutions to mitigate cyber risks. Antivirus and anti-malware software are widely adopted to detect known malicious signatures, although advanced persistent threats (APTs) commonly evade these reactive tools (Benjamin *et al.*, 2024). Firewalls remain a standard defence mechanism for filtering external traffic but often prove insufficient against insider threats or sophisticated attacks that bypass basic rules (Mmango & Gundu, 2024). Intrusion Detection and Prevention Systems (IDS/IPS) can proactively monitor network traffic for anomalies, yet these systems require constant tuning to minimise false positives, posing a challenge to organisations with limited staff (Nadella *et al.*, 2024). Encryption – both at rest and in transit – is crucial for data protection, but SMEs often cite complexity and cost as obstacles to widespread deployment (Habash, 2023). Likewise, backup solutions protect critical data against ransomware-induced lockouts, but many SMEs fail to test these backups regularly, leaving them unprepared for actual recovery scenarios (Samira *et al.*, 2024; Thomas & Galligher, 2018). The timely application of security patches is a fundamental best practice, yet resource constraints prevent many SMEs from maintaining rigorous patch management schedules (Dissanayake *et al.*, 2022). Furthermore, security awareness training, though essential, is frequently overlooked in budget planning despite social engineering attacks being a leading cause of breaches (Kocksch & Jensen, 2024; NAVEX, 2024). Multi-factor authentication (MFA) adds another layer of identity verification; however, limited IT resources can hinder seamless MFA deployment across all enterprise systems (Dave *et al.*, 2023).

http://doi.org/10.18080/jtde.v13n3.1284

While these measures represent important steps toward improving cybersecurity, they are grounded in what is commonly referred to as the traditional security model, which presumes a trusted 'internal' corporate network behind a guarded perimeter and a potentially hostile external environment (Instillery, 2023). This perimeter-based approach relies heavily on firewalls and gateways to keep attackers out, assuming that all internal traffic is relatively safe and trustworthy. Once an attacker breaches the perimeter – often by exploiting compromised credentials or social engineering tactics – they may move laterally within the network with minimal resistance (Hasan, 2024). These shortcomings are increasingly evident in today's distributed, cloud-centric IT environments, where remote work and bring-your-own-device (BYOD) policies blur the once-rigid boundaries of an organisation's infrastructure (Kang *et al.*, 2023).

To address these limitations, the Zero-Trust Security Model has gained prominence as a more proactive and adaptable approach. Zero Trust assumes that threats can emerge from within or outside the network, necessitating continuous verification of all access requests (Buck *et al.*, 2021). This approach employs micro-segmentation, wherein the network is partitioned into smaller, isolated zones to limit lateral movement in the event of a breach (Basta *et al.*, 2022; Xie *et al.*, 2021). It also mandates least privilege access, ensuring users only receive the minimal rights necessary for task completion, thereby reducing the overall attack surface (Bellamkonda, 2022; Metin *et al.*, 2024). Additionally, continuous monitoring and verification help detect and respond to anomalies in real time, while an identity-centric focus confirms user and device legitimacy prior to granting resource access (He *et al.*, 2022; Syed *et al.*, 2022). Proponents of Zero Trust argue it can better accommodate remote work, cloud services, and the inherent fluidity of modern enterprise architectures (Hasan, 2024; Lake, 2022; Syrotynskyi *et al.*, 2024). For SMEs, this approach promises stronger threat mitigation by confining attackers' mobility and neutralising insider threats, making it well-suited to an operational context where any significant breach can lead to outsized consequences (Luckett, 2024; Rahman *et al.*, 2024).

Despite its conceptual advantages, implementing Zero Trust at scale can be complex. Many existing frameworks – such as NIST SP 800-207 – offer comprehensive guidelines but often demand considerable technical expertise and funding, elements that may be scarce in SMEs (Rose *et al.*, 2020). Similarly, high-profile models like Google's BeyondCorp focus on global enterprise deployments, underscoring advanced infrastructure and extensive engineering capabilities not readily available to smaller organisations. Microsoft's Zero Trust strategy provides strong integration with cloud-based identity and access management services; however, licensing costs can be prohibitive for businesses operating on tight budgets. Consequently, a gap remains for lightweight Zero-Trust architectures that can adapt robust

http://doi.org/10.18080/jtde.v13n3.1284

security measures to the realities of SMEs, balancing cost-effectiveness, technical simplicity, and strong protective measures (Ramesh Chidirala, 2024).

Why Zero Trust Is Well-Suited for SMEs?

Zero Trust's adaptive features hold promise for smaller organisations. By implementing micro-segmentation (Khan, 2023), SMEs can isolate critical servers or data repositories, limiting the lateral movement of attackers who breach initial defences (Basta *et al.*, 2022; Xie *et al.*, 2021). Continuous verification helps identify suspicious user or device behaviours in near real time, preventing insider threats from persisting undetected (Saleem *et al.*, 2023). The model also readily integrates remote work scenarios, offering secure authentication and authorisation that do not hinge on traditional network perimeters (Wang *et al.*, 2022). Because Zero Trust is fundamentally policy-driven and can be managed centrally, SMEs may reduce overhead by automating security checks and scaling policies as needed (Gokhale & Kulkarni, 2023; Rose *et al.*, 2020). This flexibility makes Zero Trust frameworks more cost-effective in the long run, since updates and expansions focus on fine-tuning granular policies rather than overhauling entire infrastructures (Gokhale & Kulkarni, 2023; Hong *et al.*, 2023). Moreover, in light of rising compliance demands, Zero Trust's continuous monitoring and access control capabilities can improve the auditability and traceability of system changes, aiding SMEs in meeting regulatory requirements (Xu *et al.*, 2022; Zhang *et al.*, 2023). These attributes underscore Zero Trust's potential to address key gaps in SME cybersecurity without necessitating prohibitively large capital investments or highly specialised IT teams.

In conclusion, the literature reveals that SMEs confront a dynamic threat environment worsened by acute resource constraints and insufficient cybersecurity expertise. Traditional perimeter-based defences are increasingly inadequate in modern distributed and cloud-centric infrastructures. Zero Trust, with its continuous verification, least privilege, and micro-segmentation paradigm, promises a more holistic and proactive security stance for SMEs. However, existing Zero-Trust frameworks often cater to larger enterprises and remain too resource-intensive for smaller organisations. Consequently, there is a pressing need for lightweight, SME-focused Zero-Trust architectures that maintain robust security while accommodating practical limitations in budgets, staffing, and technical complexity. Addressing this gap could substantially advance the protection of a critical economic sector that continues to be an attractive and vulnerable target for cyber adversaries.

http://doi.org/10.18080/jtde.v13n3.1284

Methodology

This section details the research methodology used to develop and evaluate the lightweight Zero-Trust Architecture for SMEs. We employ a Design Science Research Methodology (DSRM), which provides a structured approach to creating and validating innovative artifacts, following Peffers *et al.* (2007) six-stage process. DSRM is particularly suited to this study's goal of constructing and validating a lightweight ZTA for SMEs. First, DSRM fosters both rigour and relevance by grounding artefact development in scholarly literature while addressing practical problems, such as constrained budgets and limited IT expertise common to SMEs. Second, DSRM's iterative cycles of design, demonstration, and evaluation align naturally with the agile and incremental nature of Zero-Trust security principles, where each layer of authentication and authorisation is tested for feasibility and refined if needed. Lastly, DSRM incorporates stakeholder feedback early and continuously, ensuring the resultant architecture remains responsive to SME needs and adaptable to real-world environments.

Applying the Design Science Research Methodology

DSRM consists of six iterative stages. The adapted model shown at Figure 1 includes the following stages:

Identify Problem and Motivate

The research begins by identifying the critical challenges SMEs face in cybersecurity. SMEs often operate under significant resource constraints, including limited budgets, lack of technical expertise, and inadequate IT infrastructures. These challenges, coupled with their increased vulnerability to sophisticated threats such as insider attacks, phishing, and ransomware, underscore the pressing need for robust but lightweight security solutions. Traditional perimeter-based models are inadequate for modern, distributed IT environments, and current Zero-Trust frameworks are often resource-intensive, making them unsuitable for SMEs. By applying inference, this stage uses insights from SME-specific challenges and Zero-Trust principles to establish the foundation for designing a tailored solution. These inferences guide the transition to defining actionable objectives for a lightweight ZTA.

Define Objectives of a Solution

This phase defines the goals of the lightweight Zero-Trust Architecture based on the identified challenges. The objectives focus on creating a scalable, cost-effective, and easy-to-deploy framework that aligns with Zero-Trust principles like least privilege access,

http://doi.org/10.18080/jtde.v13n3.1284

continuous verification, and contextual authentication. For SMEs, simplicity and operational feasibility are paramount, ensuring the solution minimises complexity and integrates seamlessly into existing systems. Here, theory plays a critical role by providing a structured framework and principles of micro-segmentation and defence in depth. This theoretical grounding clarifies why integrating Multi-Factor Authentication (MFA), contextual checks, and Role-Based Authorisation (RBAC) will likely enhance SME security. They justify the objectives and inform the architecture's design to ensure it meets SME needs effectively.

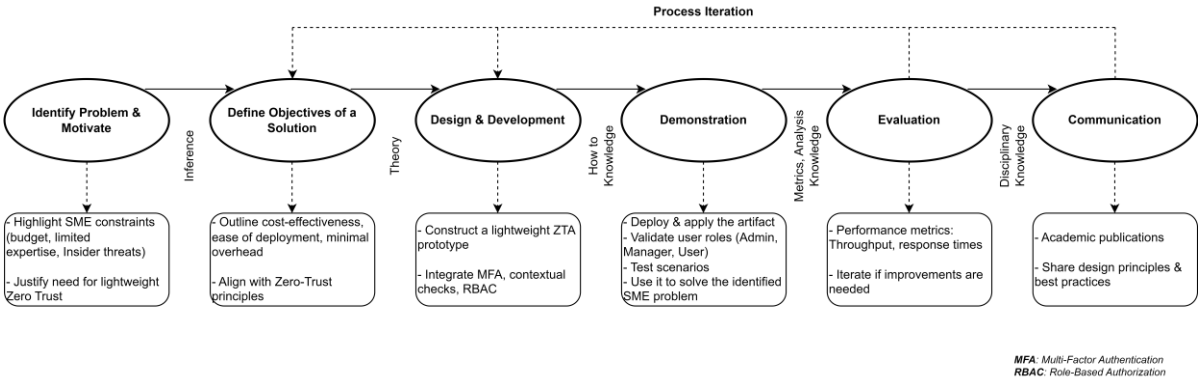


Figure 1: Research Model

Design and Development

The design and development phase centres on creating the lightweight Zero-Trust Architecture prototype. Key components include a Central Authentication Gateway for managing credentials and access requests, MFA for enhanced security, contextual access controls that verify IP, MAC, and time-based parameters, and RBAC to enforce least-privilege access. During this phase, how-to knowledge is pivotal, as it involves applying practical skills to build and configure the architecture. It moves the conceptual ZTA prototype into a working system. This includes developing the authentication gateway, integrating MFA with email OTPs, and defining role-based policies. By translating theoretical insights into tangible components, this phase produces a functional artefact ready for validation.

Demonstration

Once the artefact is developed, it is deployed in a simulated SME environment to validate its functionality. This stage includes real-world use cases such as managing different user roles (e.g., Admin, Manager, User) and testing scenarios like insider attacks and unauthorised access attempts. The artefact is assessed for its ability to meet SME-specific challenges, ensuring that it is both practical and effective. Metrics and analysis knowledge come into

http://doi.org/10.18080/jtde.v13n3.1284

play here, as the system's performance and security are measured using established benchmarks. This phase bridges the gap between theoretical design and practical application, demonstrating how the ZTA addresses the cybersecurity challenges identified earlier.

Evaluation

Evaluation is a critical phase that systematically assesses the artefact's effectiveness against predefined goals. This involves measuring performance metrics such as throughput, response times, and error rates, as well as security metrics like the system's ability to block unauthorised access and mitigate insider threats. Feedback from SME stakeholders is gathered to assess usability and implementation feasibility. Disciplinary knowledge is integral at this stage, as it provides the domain expertise needed to design evaluation criteria and contextualise results. Iterative refinements are made based on the findings, ensuring the architecture evolves to better meet the needs of SMEs while maintaining alignment with Zero-Trust principles.

Communication

The final phase focuses on disseminating the research findings to both academic and professional audiences. Results are shared through scholarly publications, industry forums, and practitioner-oriented workshops. These channels ensure the solution's broader adoption and contribute to the body of knowledge in cybersecurity for SMEs. By leveraging disciplinary knowledge, this stage positions the research within the broader context of Zero-Trust frameworks and SME cybersecurity, highlighting the novelty and practical value of the lightweight ZTA. The communication phase bridges the gap between research and practice, promoting the framework's adoption and impact.

Proposed Lightweight Zero-Trust Architecture

This section details the design and key components of the lightweight Zero-Trust architecture (LZTA) proposed to enhance security for SMEs, focusing on its authentication and access control framework.

Overarching Architecture

The proposed architecture, as illustrated in Figure 2, operates on the principle of 'never trust, always verify' and is designed to balance strong security measures with the resource and operational constraints of SMEs. To implement this principle effectively, we adopted a layered approach to security. This involves implementing multiple, overlapping security mechanisms that provide a robust defence strategy. Instead of relying on a single point of

http://doi.org/10.18080/jtde.v13n3.1284

security, the system is designed to control access at various levels, enhancing resilience to attack and creating multiple points of control. These layers include mechanisms for initial authentication, contextual validation, role-based access, dynamic token management and continuous auditing which provides the necessary depth, complexity and checks in access procedures.

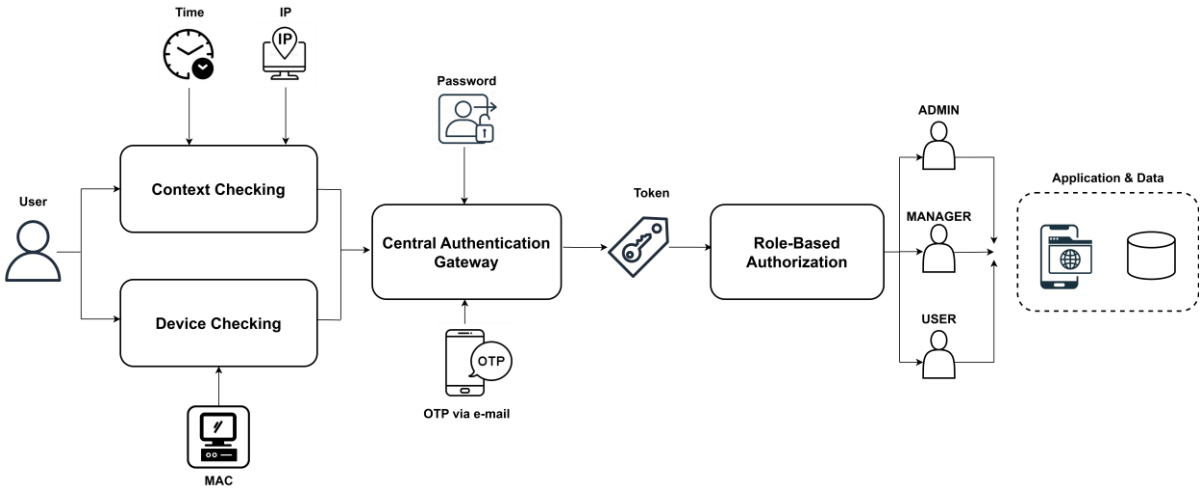


Figure 2: The proposed LZTA architecture

Layered Approach

The ZTA employs a layered security strategy, where each layer independently validates user and device authenticity, ensuring comprehensive protection. This approach significantly mitigates risks by implementing multiple checkpoints, preventing unauthorised access even if one layer is compromised. The architecture ensures that access is granted only when the user, device, and contextual parameters align with predefined security policies, adhering to the principles of defence in depth.

Contextual Access Verification

Multi-Dimensional Checks

This initial stage of access control verifies the context of the access request. The multi-dimensional checking mechanism ensures that user and device credentials are validated against several contextual parameters, rather than relying solely on a username and password. By integrating location data (e.g., IP ranges), device identification (MAC addresses), and working-hour policies, the system establishes a layered checkpoint approach before granting access to more sensitive resources.

A cornerstone of contextual verification is restricting resource access to designated working hours or Time-Based Control. See, for example, 8 AM to 5 PM, Monday through Friday shown at Figure 3. When a user attempts to log in, the system first examines the current

http://doi.org/10.18080/jtde.v13n3.1284

timestamp against an internally maintained schedule. If the request is made outside of approved hours, the system immediately rejects it, irrespective of the user's credentials or device compliance. This approach significantly reduces the threat window in which malicious actors can operate, thwarting overnight brute-force attempts or phishing campaigns timed for off-hours. Administrators can readily adjust the schedule to accommodate shifts, extended hours, or temporary exceptions, preserving both security and operational flexibility.

```
boolean isAllowedTime = vnTime.isAfter(LocalTime.of( hour 8, minute: 0)) && vnTime.isBefore(LocalTime.of( hour 17, minute: 0));
boolean isAllowedDay = dayOfWeek != DayOfWeek.SATURDAY && dayOfWeek != DayOfWeek.SUNDAY;
```

Figure 3: Time-based contextual access verification

In addition to verifying the time of access, the system checks the requesting IP address against a whitelist (or set of sanctioned ranges) (Figure 4). This IP-based filtering ensures that only devices originating from known networks – such as an internal corporate subnet or a trusted remote VPN – can pass the initial screening. If a user attempts to authenticate from an unfamiliar or blacklisted IP, the system denies the request outright, averting potential attacks from unknown internet locations. Moreover, by logging requests from disallowed IPs, administrators can investigate repeated unauthorised access attempts, gaining insights into possible cyber threats or compromised external nodes.

Even if the requesting IP address is not within the recognised range, the system applies an additional layer of security by examining the device's MAC address. When an off-range IP is detected, the system checks whether the associated MAC is on a predefined approval list (Figure 4). This approach grants limited flexibility for scenarios where remote or atypical IP addresses might be used (e.g., a remote employee occasionally connecting from a temporary location) but only if the physical device itself is known and trusted. Conversely, if the MAC address fails verification, the session is blocked. By enforcing two-tiered network checks – IP range followed by MAC validation – the architecture significantly reduces the likelihood of unauthorised devices masquerading under an allowed IP address, thus preventing numerous spoofing attacks.

http://doi.org/10.18080/jtde.v13n3.1284

```
# Whitelist of Approved IP Addresses
# Internal Corporate Subnet Range
192.168.0.0/24    # Office Subnet 1
192.168.1.0/24    # Office Subnet 2

# Trusted Remote VPN IPs
203.0.113.10      # VPN Gateway 1
203.0.113.11      # VPN Gateway 2

# Specific External Partners
198.51.100.5      # Partner A
198.51.100.6      # Partner B

# Predefined Approval List of MAC Addresses
# Corporate Devices
00:1A:2B:3C:4D:5E    # IT Department Laptop
00:1F:33:44:55:66    # HR Desktop Workstation

# Remote Employees
00:1B:77:88:99:AA    # John Doe Laptop
00:1D:EE:FF:GG:HH    # Jane Smith Mobile Device

# Temporary/Occasional Access Devices
00:1C:22:33:44:55    # Guest Conference Room Laptop
```

Figure 4: Device authentication based on IP and MAC addresses

Let U be the set of users attempting to access the system, where each user $u_i \in U$ submits an access request with parameters (t_i, IP_i, MAC_i), representing:

- t_i: The timestamp of the request.
- IP_i: The IP address of the requesting device.
- MAC_i: The unique MAC address of the requesting device.

A user is granted access only if all contextual conditions are met, which we define as:

$$P_{access}(u_i) = P\big(T_{valid}(t_i)\big) \times P\big(IP_{valid}(IP_i)\big) \times P\big(MAC_{valid}(MAC_i)\big) \quad (1)$$

where:

- $P\big(T_{valid}(t_i)\big)$ is the probability that the request occurs within allowed working hours.
- $P\big(IP_{valid}(IP_i)\big)$ is the probability that the IP address belongs to a trusted network.
- $P\big(MAC_{valid}(MAC_i)\big)$ is the probability that the request originates from an authorised device.

Since all three conditions must be met for access to be granted, the probability of an unauthorised user bypassing contextual verification is given by:

$$P_{bypass,CAV} = 1 - \big(P(T_{valid}) \times P(IP_{valid}) \times P(MAC_{valid})\big) \quad (2)$$

This holistic validation process not only minimises the chance of successful external attacks but also helps detect suspicious behaviour from internal or compromised accounts. As a result, if one dimension (e.g., an authorised IP) is satisfied but another (e.g., an unlisted MAC) is not, the request is denied, upholding the 'never trust, always verify' philosophy central to Zero Trust.

http://doi.org/10.18080/jtde.v13n3.1284

Central Authentication Gateway (CAG)

The Central Authentication Gateway serves as the next line of defence in the access control process, acting as the initial verification step for all users attempting to access the system. Its primary function is to authenticate user credentials and ensure that only authorised individuals gain entry. By acting as a centralised checkpoint, the gateway streamlines the authentication process while maintaining a high level of security. It enforces strict protocols to verify user identity before granting access to downstream systems or resources. By centralising this process, the system ensures consistency in authentication logic, enabling administrators to manage and update security policies from a single, unified interface rather than dispersing them across multiple services or modules.

When a user initiates a login request, the CAG first verifies the username and password combination against the stored credentials (e.g., in a secure directory or database). This password-based login serves as the most fundamental layer of authentication. While a simple password mechanism on its own might prove insufficient for robust security, it remains a recognisable and user-friendly starting point for many organisations, particularly those with limited IT resources. To enhance security, the system enforces password complexity requirements, such as minimum length, the inclusion of special characters, and regular password updates. Additionally, measures like account lockout after multiple failed attempts are implemented to prevent brute force attacks. While password-based login is a fundamental authentication method, it forms the first critical barrier against unauthorised access.

To bolster overall protection against password compromises, the CAG seamlessly integrates a multi-factor authentication (MFA) process. Immediately after the password is validated, the gateway prompts for a second factor, commonly in the form of a One-Time Password (OTP) delivered to the user's email. This additional requirement ensures that unauthorised individuals who happen to obtain a user's password cannot gain full access without also controlling the user's email channel. Such a combination of 'something you know' (the password) and "something you possess" (the email account to receive OTP) substantially elevates the difficulty for attackers.

- **OTP Generation**: In the event that a user's password check succeeds, the CAG calls an OTP generation module. This component creates a randomly produced alphanumeric code, valid for a brief timeframe. The short lifespan is deliberate: even if an attacker intercepts the OTP, it expires quickly, rendering it useless for long-term exploitation. By employing robust cryptographic algorithms to generate these codes, the system further decreases the likelihood of OTP collisions or predictability.

http://doi.org/10.18080/jtde.v13n3.1284

- **Email Delivery:** After the OTP is generated, the CAG securely dispatches the code to the user's registered email address. Upon receiving the OTP in their inbox, the user must provide it back to the gateway within the allotted time window. If the OTP is correct and submitted punctually, the user is granted preliminary access – subject to additional contextual or role-based checks that occur downstream in the authentication pipeline. This layered approach effectively prevents attackers armed solely with stolen credentials from entering the system, preserving both usability and security at a level suitable for SMEs.

Let $A(u_i)$ be the probability of a user u_i successfully authenticating through the CAG, which depends on:

- **Password authentication** probability $P\big(C_{valid}(C_i)\big)$, where C_i is the user's credentials.
- **Multi-factor authentication** probability $P\big(MFA_{valid}(MFA_i)\big)$, where MFA_i is the one-time passcode (OTP) verification.

Thus, the probability of successful authentication is given by:

$$A(u_i) = P\big(C_{valid}(C_i)\big) \times P\big(MFA_{valid}(MFA_i)\big) \quad (3)$$

To estimate brute-force attack success probability, we use:

$$P_{bypass,auth} = \frac{1}{N_{pw} \times N_{otp}} \quad (4)$$

where:

- N_{pw} is the total number of possible password combinations (e.g., 10^8 for an 8-character password).
- N_{otp} is the total number of OTP variations (e.g., 10^6 for a 6-digit OTP).

Dynamic Access Token Management

After a user passes all requisite security checks – such as password authentication, MFA, and contextual verifications – the system generates an access token that encapsulates the user's verified identity and role-based privileges. Often structured as a cryptographically signed token (Jones, 2015), this artefact contains metadata such as the user's unique ID, assigned role, and an expiration timestamp. By embedding these details directly in the token, the architecture minimises repeated lookups to the authentication database, enabling streamlined access checks during subsequent requests.

http://doi.org/10.18080/jtde.v13n3.1284

In practical terms, token generation typically occurs in the CAG. Upon successful authentication, the gateway issues the token and returns it to the client (e.g., a browser or mobile app). The token is then stored securely on the client side – often within an encrypted session storage or cookie – to prevent tampering. This design ensures that the system can unequivocally track the user's identity and policy entitlements without requiring the user to re-enter credentials at every step.

Once an access token is assigned, all subsequent requests from that user must include the token. This mechanism allows the system to verify, in real time, whether the user is still within their permissible scope of operation. As each request arrives, the Zero-Trust architecture inspects the token's validity, ensuring it has not expired, been tampered with, or revoked (e.g., due to role changes).

Let T be the token set, where each token t_i contains metadata (u_i, r_j, exp), with:

- u_i: User identity.
- r_j: Assigned role.
- exp: Token expiration time.

The probability that a token remains valid is:

$$P_{valid}(t_i) = P(authenticated) \times P(role_{valid}) \times P(exp_{valid}) \quad (5)$$

where $P(exp_{valid})$ ensures that the token has not expired; $P(role_{valid})$ is the probability that the stolen token still has a valid role; $P(authenticated)$ is the probability that the user was properly authenticated before receiving the token.

The probability of a stolen token being successfully used is:

$$P_{bypass,token} = P(steal) \times P(role_{valid}) \times P(exp_{valid}) \quad (6)$$

where $P(steal)$ is the probability that an attacker successfully steals a token. It is very small due to encryption and time-limited validity. Thus, this continuous authentication provides an additional safeguard by eliminating static sessions that remain valid indefinitely, thereby reducing exposure to session hijacking or replay attacks.

Role-Based Access Control (RBAC)

Within this lightweight Zero-Trust architecture, RBAC (Sandhu, 1998) provides a structured method for assigning and revoking privileges across the organisation. By mapping specific permissions to well-defined roles, the system ensures that each user has access strictly to the resources they need. In contrast to granting broad rights individually, RBAC fosters a 'least privilege' mindset (Lund *et al.*, 2024), lowering the risk of both intentional and accidental

http://doi.org/10.18080/jtde.v13n3.1284

misuse of data or system functions. Consequently, administrators can easily audit access patterns, update policies, and ensure organisational compliance without sifting through dozens of personalised permission sets.

The proposed RBAC system can support different roles, each tailored to the organisational hierarchy and operational needs of SMEs. In the scope of this research, we consider only three primary roles:

- **Admin:** This role grants full system control, including user management, policy configuration, and access to critical data and logs. Admin users oversee all aspects of the system.
- **Manager:** Managers have intermediate access, allowing them to view and manage resources within their department. Their access is limited to departmental data relevant to their leadership responsibilities.
- **User:** Standard users have the lowest access level, restricted to applications and resources necessary for their tasks. They cannot modify settings or access other users' data, minimising lateral movement in case of account compromise and adhering to Zero-Trust principles.

Let R be the set of roles, and each user u_i is assigned to exactly one role $r_j \in R$. The **access function** for a user is:

$$Access(u_i) = \begin{cases} 1, & \text{if } P_{role}(u_i, r_j) = 1 \text{ and } P_{perm}(r_j, p_k) = 1 \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

where:

- $P_{role}(u_i, r_j)$ indicates whether user u_i is assigned to role r_j.
- $P_{perm}(r_j, p_k)$ is the probability that role r_j has permission to access resource p_k.

An attacker attempting to bypass RBAC has a success probability:

$$P_{bypass,RBAC} = \sum_{r_i \notin R_{authorized}} P_{role}\,(u_i, r_i) \times P_{perm}(r_i, p_k) \quad (8)$$

In a well-structured RBAC system, unauthorised privilege escalation is rare, making $P_{bypass,RBAC} \approx 0$.

Figure 5 depicts the process by which a regular user logs in and acquires access to assigned resources.

http://doi.org/10.18080/jtde.v13n3.1284

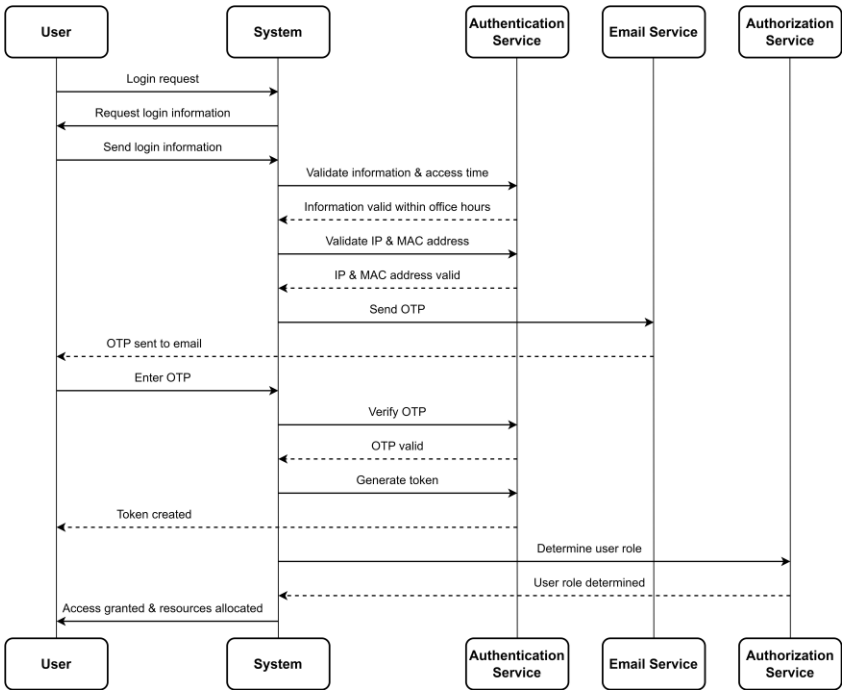


Figure 5: Sequence diagram illustrating user access to the service

Figure 6 extends the concept to an administrator login flow, highlighting additional privileges and system management functionalities.

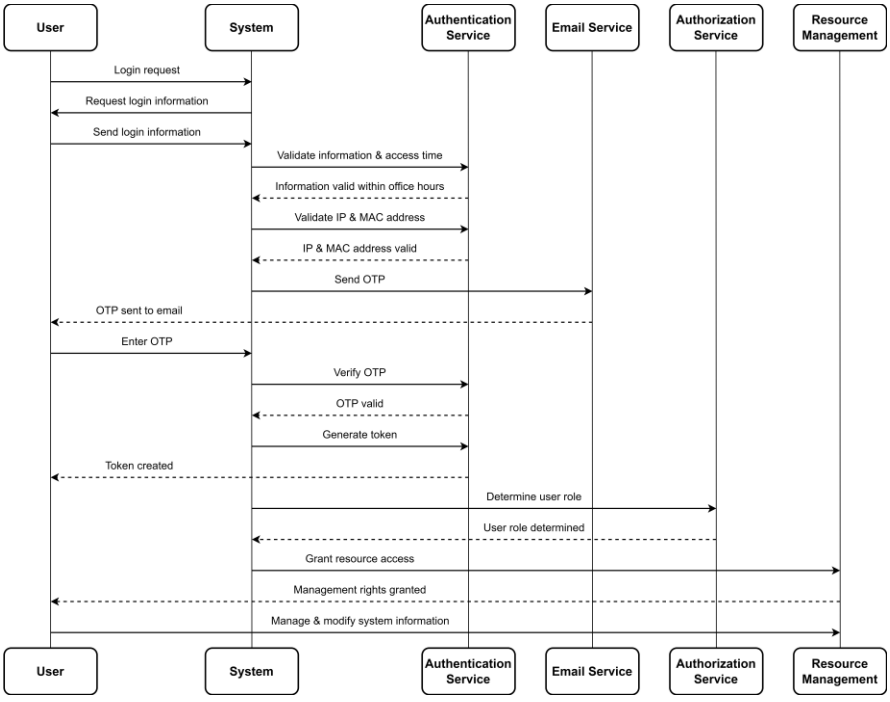


Figure 6: Sequence diagram illustrating administrator access to the service

http://doi.org/10.18080/jtde.v13n3.1284

Application and Data

Finally, once the user has passed all checks and is cleared by role-based rules, they can interact with the application and data resources they are authorised to use. The entire workflow ensures that an attacker who fails any of the prior security gates – context checking, device validation, password authentication, or OTP verification – cannot proceed to this protected layer.

This component is not a monolithic entity, but rather an abstraction representing all the diverse and specific resources that are typically found within an SME. These resources may include:

- **Applications:** These are the core software tools and services used by the SME employees to carry out their work tasks.
- **Servers**: Includes both physical and virtual server environments that support operations. These servers might house the applications, databases, and services crucial to the business.
- **Databases:** These are used to store sensitive customer, transaction, business, and employee data.
- **Data Storage:** This represents the files and other storage services within the SME's network, from simple shared folders to cloud storage.
- **Other resources**: This is a catch-all term to include other resources such as services and access to specific business processes, that are protected through our designed Zero Trust model.

Overall, this multiple-layers architecture exemplifies a lightweight yet robust Zero-Trust system. By placing equal emphasis on who is accessing (user identity, role) and how/when/where they are connecting (time, IP, device), the architecture delivers continuous verification and helps SMEs safeguard their key information assets with minimal overhead.

Prototyping and System Deployment

This section details the concrete steps taken to transform the conceptual Lightweight Zero-Trust Architecture into a functional prototype, bridging the gap between theory and practice. It includes the description of the development environment, specifics of component implementation, challenges faced, and proposed solutions, demonstrating how a lightweight yet robust Zero Trust architecture can be implemented for SMEs, making it suitable for academic publication.

http://doi.org/10.18080/jtde.v13n3.1284

A modular design was adopted to build the LZTA, breaking the system into a set of individuals, yet cohesive, modules that communicate with each other via secure interfaces. The backend is built as a REST API, which allows easy integration and a more scalable system. Figure 7 depicts the structure of this prototype. This diagram illustrates the separation of concerns, modularity, and interdependencies among key components, emphasising the systematic design of the backend.

Data Flow and Dependencies

The architecture demonstrates a top-down flow of data:

- **Controllers** depend on services for business logic, ensuring proper validation and enforcement of Zero-Trust principles, such as least privilege access.
- **Services** rely on repositories for secure database interactions, leveraging ORM (Object-Relational Mapping) (Keith *et al.*, 2010) for optimized data handling.
- **Repository** maps directly to the database, ensuring seamless data retrieval and storage while adhering to predefined access policies.

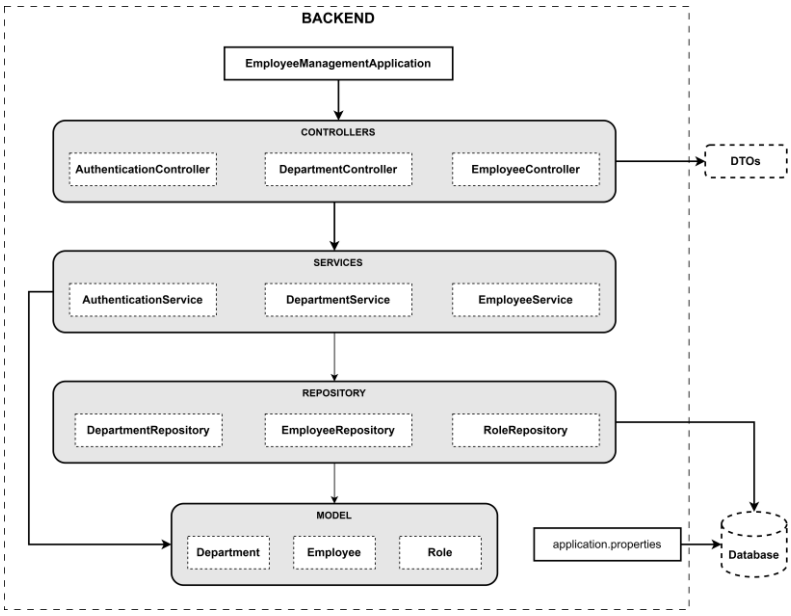


Figure 7: Back-end development of the LZTA prototype

Java was used for the core backend implementation, chosen for its cross-platform compatibility, robust security capabilities, and an extensive ecosystem that facilitates component integration and the development of flexible, portable applications. At the backend, the EmployeeManagementApplication.java serves as the entry point, orchestrating system-wide configuration and execution. The controller layer houses AuthenticationController, EmployeeController, and DepartmentController, which handle user requests related to authentication, employee, and department operations respectively.

http://doi.org/10.18080/jtde.v13n3.1284

These controllers delegate business logic to the service layer, where AuthenticationService, EmployeeService, and DepartmentService encapsulate critical logic for managing user roles, authentication workflows, departmental mapping, and data security.

The repository layer, represented by RoleRepository, EmployeeRepository, and DepartmentRepository, interfaces with the database, leveraging Spring Data JPA (Gierke *et al.*, 2012) for efficient data access and persistence. The model layer includes Employee.java, Department.java, and Role.java, which define the core data entities, ensuring consistency and integrity during database interactions. These entities are complemented by supporting Data Transfer Objects (DTOs) for seamless data exchange.

Additionally, the application.properties configuration file connects the application to the database, providing crucial settings like authentication credentials, connection URLs, and security parameters.

Contextual Access Verification Development

The Contextual Access Verification system forms a critical layer in the LZTA, ensuring that access requests are rigorously validated against specific contextual parameters. This layer operates through a custom-designed AccessFilter class, embedded within the Spring Security filter chain (Alex & Taylor, 2022), which continuously enforces time- and device-specific policies for access management. The AccessFilter leverages Java's LocalTime and DayOfWeek classes to dynamically assess the current time and verify it against predefined operational hours. This ensures that users can only access resources during approved time frames, adding a temporal layer to the security model.

In addition to temporal validation, the AccessFilter extends its contextual scope by verifying the IP address associated with each request. This IP validation step compares the incoming request's IP address against a whitelist maintained through the AllowedNetworkConfig class. This whitelist includes trusted IP ranges, such as internal corporate networks or authorised VPNs, ensuring that only approved networks can initiate access requests. Should an IP address fall outside the permitted range, the system escalates to a secondary verification step involving MAC address authentication. Through integration with the EmployeeRepository and the AllowedNetworkConfig class, the filter retrieves a list of pre-authorised MAC addresses and validates the device's unique identifier.

Figure 8 depicts the development of these functions using those mentioned above classes.

http://doi.org/10.18080/jtde.v13n3.1284

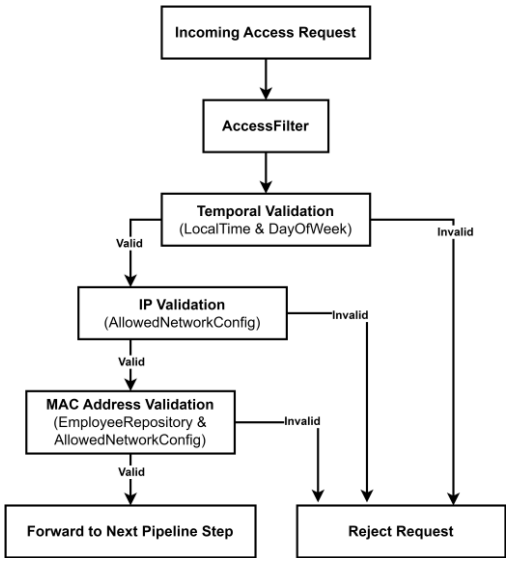


Figure 8: Contextual access verification development

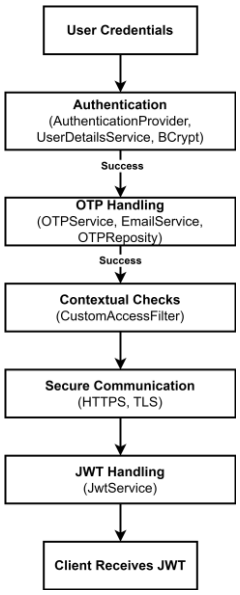


Figure 9: Central authentication gateway development

Central Authentication Gateway Development

The CAG operates as the first layer of defense, leveraging Spring Security's AuthenticationProvider and UserDetailsService interfaces to manage the authentication logic (Alex & Taylor, 2022; Dikanski *et al.*, 2012) (Figure 9). Upon receiving user credentials, the gateway initiates a multi-step validation process. The username is matched against the stored database records, while the password undergoes secure verification using the BCrypt hashing algorithm (Skanda *et al.*, 2022), a widely adopted cryptographic standard for password storage. The integration of BCrypt ensures that even if the password database is compromised, the hashed passwords remain computationally infeasible to reverse.

In scenarios where password validation succeeds, the gateway transitions to a multi-factor authentication mechanism. The OTP generation and validation process are managed through a dedicated OTPService, which creates a time-sensitive one-time password using a secure random number generator. To ensure seamless delivery, the system employs the JavaMailSender library, securely configured via SMTP protocols, for transmitting the OTP to the registered user email. The EmailService class encapsulates this functionality, including SMTP settings for secure communication, ensuring reliable and timely delivery of OTPs.

Upon receiving the OTP, users must submit it back to the gateway within the preconfigured expiration window. The gateway validates the OTP against the records in the OTPRepository, ensuring that only authenticated users can proceed. This step mitigates risks associated with stolen or compromised credentials, as possession of both the password and the OTP is required for authentication success.

http://doi.org/10.18080/jtde.v13n3.1284

The CAG is further enhanced with contextual access verification mechanisms, such as validating the IP and MAC addresses of incoming requests through a CustomAccessFilter.

The gateway's secure communication protocols ensure the confidentiality and integrity of user interactions. All credentials and sensitive data are transmitted over HTTPS, encrypted with TLS standards. This prevents data interception during transmission and aligns with industry best practices for secure communication.

Finally, upon successful authentication, the gateway generates a JSON Web Token using the JwtService class. The token encapsulates essential user metadata, such as roles and permissions, and is cryptographically signed using the HMAC SHA-256 algorithm to prevent tampering. This token is passed back to the client and is required for all subsequent requests, enabling a stateless and scalable session management model.

Dynamic Access Token Management Development

Dynamic access token management (Figure 10) in this system is implemented using a dedicated JwtService class, leveraging the Java JSON Web Token library to ensure secure and efficient token creation. During the authentication process, the token is generated immediately after successful user validation. This is achieved through a method in the JwtService class that constructs a JSON Web Token embedding key user details, such as the username and roles.

The token creation process involves multiple steps to guarantee security and functionality. First, user-specific details like the username and roles are included in the payload. To ensure the token's validity is time-bound, a timestamp is incorporated, with the typical expiration period set to 24 hours. This limited lifespan minimises the risk associated with potential token compromise.

To protect the integrity of the token, the system employs cryptographic signing using a secret key and the HMAC-SHA256 algorithm. This signing process, handled within the JwtService, ensures that any tampering with the token renders it invalid during verification. The generated token is then passed to the client via the AuthService, included in the authentication response.

Subsequent requests to the system include the token in the Authorisation header. These requests are intercepted by the JwtAuthenticationFilter, which is integrated into the Spring Security filter chain. The filter extracts the token from the header, validates its signature using the same cryptographic secret, and parses the token to extract user information. Once validated, the user's details, including roles, are populated in the SecurityContextHolder, enabling secure access to authorised resources.

http://doi.org/10.18080/jtde.v13n3.1284

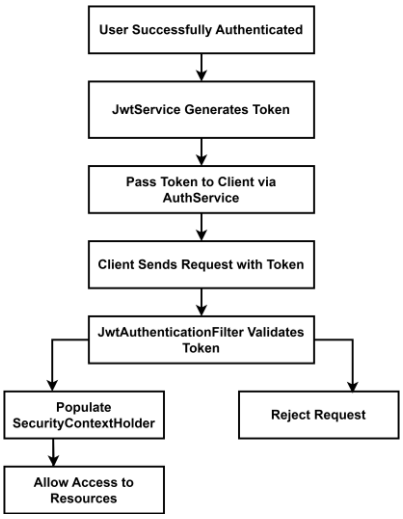


Figure 10: Dynamic access token development

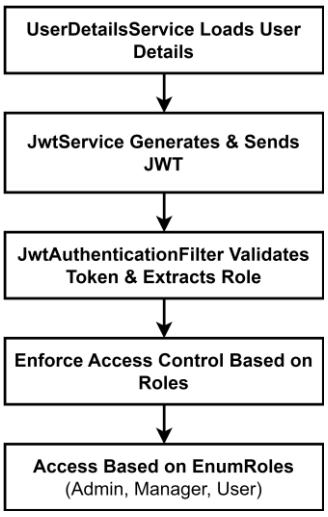


Figure 11: Role-based access control development

This approach ensures that the system maintains dynamic, stateless session management, fully aligned with the principles of Zero-Trust Architecture.

Role-Based Access Control Development

RBAC was implemented using Spring Security's robust access control mechanisms, combined with custom classes for flexibility and scalability (Figure 11). At the core of the RBAC system is the EnumRoles class, which provides a structured representation of the roles defined within the system: Admin, Manager, and User. Each role in this class is associated with a unique identifier and a descriptive name, ensuring clarity in assigning and managing permissions. The EnumRoles class facilitates centralised management of roles, simplifying their use across different system components.

Access control rules were enforced using Spring Security's **authorizeHttpRequests()** method, enabling fine-grained control over endpoint accessibility. Specific endpoints were mapped to corresponding roles, ensuring that only authorised users could execute particular actions.

To dynamically assign permissions during user authentication, the system integrates role information directly into the JSON Web Token. The JwtService class embeds the user's role as part of the token payload during token creation. When a user sends a request, the JwtAuthenticationFilter extracts this role information from the token and populates it into the SecurityContextHolder as explained above.

The role assignment process is supported by the UserDetailsService, which loads user-specific details, including roles, during authentication. These details are used not only for

http://doi.org/10.18080/jtde.v13n3.1284

token generation but also for enforcing access policies across the application. By combining Spring Security's built-in capabilities with custom role management through EnumRoles, the RBAC implementation offers a secure, flexible, and scalable solution suitable for the dynamic requirements of a ZTA.

Testing and Validation

This section details the testing procedures used to validate the functionality and security of the developed LZTA. This phase includes both functional testing of individual components and end-to-end security testing, following the principles of DSRM, to assess the prototype in a simulated real-world setting.

To contextualise the system's performance and validate its efficiency, a comparative benchmark analysis was also conducted. This evaluation compares the proposed LZTA against a conventional API gateway and an open-source Zero-Trust baseline to quantify its advantages in a resource-constrained SME environment.

Testing Environment

The testing was conducted on a setup representative of the typical resource constraints found in SMEs. The system was deployed on a single machine equipped with an AMD Ryzen 7 7735HS processor and 16 GB DDR5 RAM. The network connection utilised a stable broadband link, simulating a standard SME operational environment. This configuration ensured a realistic evaluation of the system's performance under hardware limitations commonly encountered in smaller organisations.

The backend system was tested in a runtime environment comprising Windows 11 as the operating system. The application was deployed on a Spring Boot server, leveraging the Java 17 runtime for executing backend logic. Persistent data storage was managed using a MySQL database, chosen for its compatibility with the Spring Data JPA framework.

Testing tools were carefully selected to address various aspects of system validation. Load testing was carried out using Apache JMeter (https://jmeter.apache.org/), installed on a separate client machine within the same network segment to minimise latency anomalies. JMeter test plans were designed with varying levels of concurrency (from 10 up to 100 or more threads), while ramp-up periods (0.5 – 1 second) simulated how rapidly concurrent users might appear in real scenarios. The network layout placed the JMeter client outside the container environment but within a controlled local LAN or VLAN, reducing interference from external internet traffic. Postman (https://www.postman.com/) was utilised for API testing, allowing precise examination of individual endpoints for functional correctness, response times, and adherence to access control policies. Additionally, debugging and

http://doi.org/10.18080/jtde.v13n3.1284

monitoring tools integrated into the Spring ecosystem facilitated real-time performance tracking and issue resolution.

Performance Testing Results

To validate the effectiveness of our proposed architecture, we conducted a comprehensive comparative performance analysis. This evaluation benchmarks our proposed LZTA against two baselines:

- A **Conventional API Gateway Model** without any integrated zero-trust security mechanisms, representing a typical SME setup without advanced security.
- An **OpenZiti-based Model** (https://openziti.io/), serving as a representative open-source ZTA baseline to measure the overhead of a generic Zero-Trust implementation.

The evaluation was performed on a virtual machine configured with 8 GB of RAM and 6 processor cores to simulate a resource-constrained environment typical of SMEs. We utilised Apache JMeter to simulate concurrent user loads and measure key performance indicators for critical API endpoints. The following tables summarise the performance results for four key APIs under simulated user loads.

Login API Performance

To evaluate the system's resilience and performance under high-traffic conditions at its primary entry point, the Login API (Table 1) was benchmarked with a simulated load of 100 concurrent users.

Table 1: Login API Performance Metrics

Metric	Proposed LZTA Model	Conventional Model	OpenZiti Baseline
Avg. Response Time	348 ms	8109 ms	9913 ms
Std. Deviation	92.49 ms	2782.41 ms	4094.72 ms
Throughput	68.3 req/s	7.1 req/s	5.7 req/s

Analysis: Our proposed LZTA model demonstrates overwhelmingly superior performance, maintaining low latency and high throughput under significant load. The *OpenZiti* baseline, while providing robust security, introduces substantial overhead, increasing the average response time by over 28-fold compared to our solution. This highlights the efficiency of our lightweight, integrated approach.

http://doi.org/10.18080/jtde.v13n3.1284

OTP Verification API Performance

The performance of the OTP Verification API (Table 2), a critical component for multi-factor authentication, was assessed under a moderate load of 30 concurrent users to measure its efficiency in real-time security operations.

Table 2: OTP Authentication API Performance Metrics

Metric	Proposed LZTA Model	Conventional Model	OpenZiti Baseline
Avg. Response Time	42 ms	416 ms	889 ms
Std. Deviation	27.47 ms	193.30 ms	208.54 ms
Throughput	30.5 req/s	21.5 req/s	14.6 req/s

Analysis: The LZTA model processed OTP verifications with exceptional speed and stability. Both the conventional and OpenZiti models exhibited significantly higher latency, confirming that the additional processing and network overlay layers in a generic ZTA solution can create performance bottlenecks in time-sensitive operations.

User Information Search API Performance

To assess the system's responsiveness for frequent data retrieval operations, the User Information Search API (Table 3) was subjected to a high-concurrency test of 100 users.

Table 3: Information Search API Performance Metrics

Metric	Proposed LZTA Model	Conventional Model	OpenZiti Baseline
Avg. Response Time	23 ms	2508 ms	3440 ms
Std. Deviation	2.75 ms	321.28 ms	1107.49 ms
Throughput	98.9 req/s	25.3 req/s	16.5 req/s

Analysis: For data retrieval operations, our model's performance was outstanding, with an average response time nearly 100 times faster than the baselines. The extremely low standard deviation (2.75 ms) underscores its remarkable stability, a critical factor for ensuring a consistent user experience.

User Detail Retrieval API Performance

Finally, the User Detail Retrieval API (Table 4) was evaluated with 100 concurrent users to confirm the system's ability to handle intensive, specific data-lookup tasks with high stability and low latency.

http://doi.org/10.18080/jtde.v13n3.1284

Table 4: User Information Detail API Performance Metrics

Metric	Proposed LZTA Model	Conventional Model	OpenZiti Baseline
Avg. Response Time	20 ms	1489 ms	2692 ms
Std. Deviation	1.75 ms	544.51 ms	959.84 ms
Throughput	98.9 req/s	28.5 req/s	18.6 req/s

Analysis: Similar to the search API, the LZTA model demonstrated superior efficiency and stability for detailed data retrieval, further validating its suitability for real-world applications where performance is key.

This comprehensive benchmark addresses key concerns of scalability and implementation overhead. The results clearly quantify the performance overhead associated with a generic, open-source ZTA solution like *OpenZiti*. The overlay network, certificate-based identity management, and policy enforcement engine, while comprehensive, introduce significant latency across all tested operations. Our LZTA model, by integrating essential zero-trust logic directly into the application gateway, minimises this overhead, achieving security enforcement without compromising performance.

Furthermore, the tests under a high load of 100 concurrent users demonstrate the superior scalability of our solution. While the baseline models showed signs of severe performance degradation and instability (evidenced by high average response times and large standard deviations), our LZTA model scaled gracefully, maintaining high throughput and a stable, responsive user experience. This comparative analysis robustly demonstrates that our proposed lightweight architecture provides a practical and effective balance of security and performance, making it an ideal solution for SMEs with limited infrastructural resources.

While this study successfully demonstrates the performance and feasibility of the proposed LZTA, it is important to acknowledge its limitations. The performance evaluation was conducted under laboratory conditions using simulated user loads on a single-machine setup. This approach, while effective for controlled benchmarking, constrains the generalisability of the findings to diverse, real-world SME environments which may feature more complex network topologies and unpredictable traffic patterns. Furthermore, the security validation focused primarily on performance metrics and the architecture's ability to enforce access policies, rather than comprehensive threat modeling or penetration testing, which would provide a more complete assessment of its security properties against sophisticated attacks.

Future research should aim to bridge these gaps. A crucial next step would be to conduct field trials or case studies involving actual SME deployments to validate the LZTA's practical

http://doi.org/10.18080/jtde.v13n3.1284

applicability and performance in a production environment. Such studies would provide invaluable insights into usability, user adoption challenges, and long-term stability. Additionally, future work could incorporate a rigorous security analysis, including formal threat modeling and penetration testing, to further validate the architecture's resilience.

Use Cases

Practical demonstrations of the proposed LZTA are best conveyed through representative scenarios that reflect common security and operational needs in SMEs. The following use cases serve to exemplify how the LZTA framework – particularly its core features of contextual verification, MFA, and RBAC – functions under everyday organisational conditions. While each scenario is assumed rather than derived from a live production environment, they are informed by typical SME practices and the known challenges of safeguarding remote access and managing privileged accounts. These two cases thus provide a logical, real-world grounding for how Zero-Trust principles address the dual concerns of external threats (e.g., off-hours login attempts) and internal controls (e.g., administrative role assignments).

Use Case 1: Off-Hours Remote Access by a Sales Employee

The primary motivation for this use case arises from the common practice of allowing sales teams to log into corporate systems beyond standard office hours. In a SME, it is not unusual for sales staff to prepare follow-up proposals or review leads late in the evening, particularly if they work with clients across different time zones. Such off-hours access, however, elevates the risk of unauthorised intrusion due to the lack of on-site oversight and the frequent use of external networks (e.g., home or public Wi-Fi). Consequently, a robust Zero-Trust framework that integrates time-based checks, device validation, and MFA can mitigate potential threats without impeding legitimate tasks.

From an architectural standpoint, two key actors shape this scenario: (1) the Sales Employee (operating under a User role) and (2) the LZTA modules, specifically the CAG, Contextual Access Filters (e.g., IP and MAC checks), and MFA Services. Before any off-hours login attempt, the user must hold valid credentials within the system (e.g., username and password), while their device should be pre-approved and recognised. Furthermore, company policy dictates permissible evening or weekend login windows, specifying stricter conditions – such as obligatory OTP verification – even if the user's MAC address is on record.

The login process begins when the Sales Employee connects from a non-corporate IP after standard working hours. The LZTA immediately checks the request timestamp against

http://doi.org/10.18080/jtde.v13n3.1284

configured schedules. If the detected time conflicts with normal business hours, the system performs a secondary device-level validation: verifying that the MAC address belongs to the salesperson's previously registered laptop or tablet. If these contextual verifications pass, the CAG prompts the user for their credentials. Once the password is confirmed, the system dispatches an OTP to the user's registered email address. The user must enter this OTP within a strict expiration window to prove possession of both a valid password and a legitimate email channel. Upon successful OTP submission, the system issues a short-lived token embedding the Sales role, thereby allowing access solely to sales-related dashboards or customer lead data.

Figure 12 illustrates the scenario in which the Sales employee was denied system access because the access attempt occurred at 11:38 PM, which is outside of working hours.

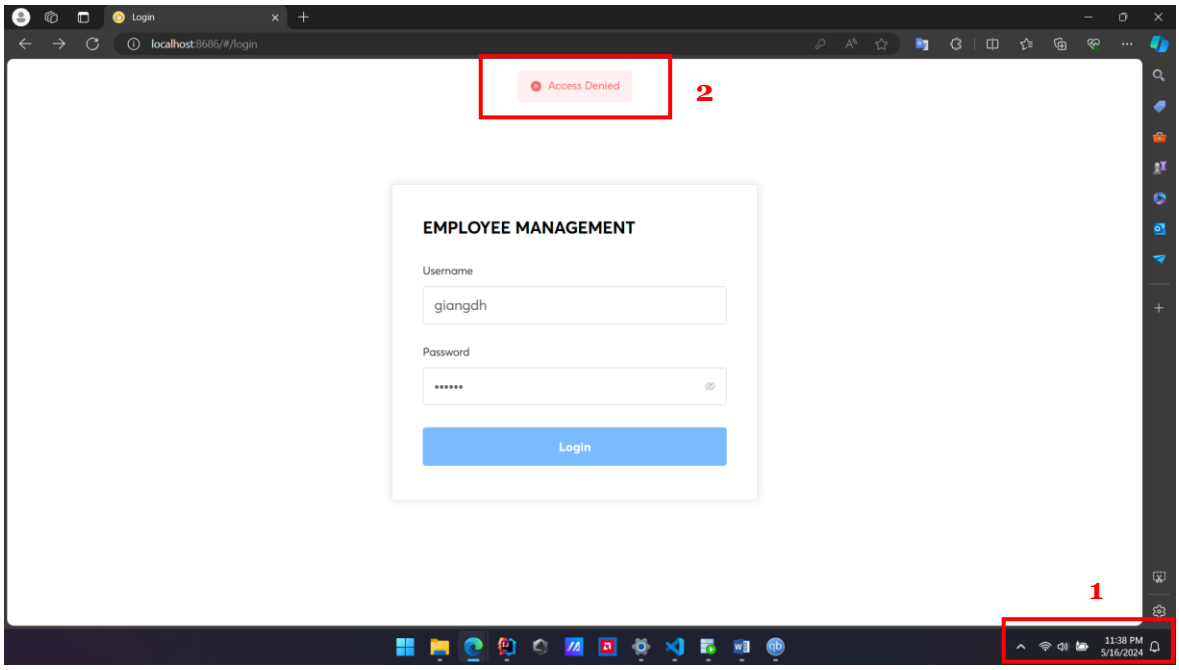


Figure 12: Denied access due to the working hours

Figure 13 depicts the scenario where the employee successfully passed the contextual verifications, and the password was confirmed. An OTP, valid within a strict expiration window, would then be required.

In practical terms, this off-hours use case highlights several Zero-Trust advantages. First, time-based enforcement and device recognition minimise external threats from unsanctioned remote networks. Second, multi-factor authentication ensures that stolen passwords alone cannot breach the system, especially when logins originate from unusual IPs or during atypical hours. Lastly, role-based privileges continue to apply post-login, preventing a Sales Employee from inadvertently accessing more sensitive data (e.g., HR

http://doi.org/10.18080/jtde.v13n3.1284

records or financial assets). By maintaining these layered checks, the LZTA fulfills SMEs' need for flexible scheduling and location-agnostic work, all while preserving a high standard of security and accountability.

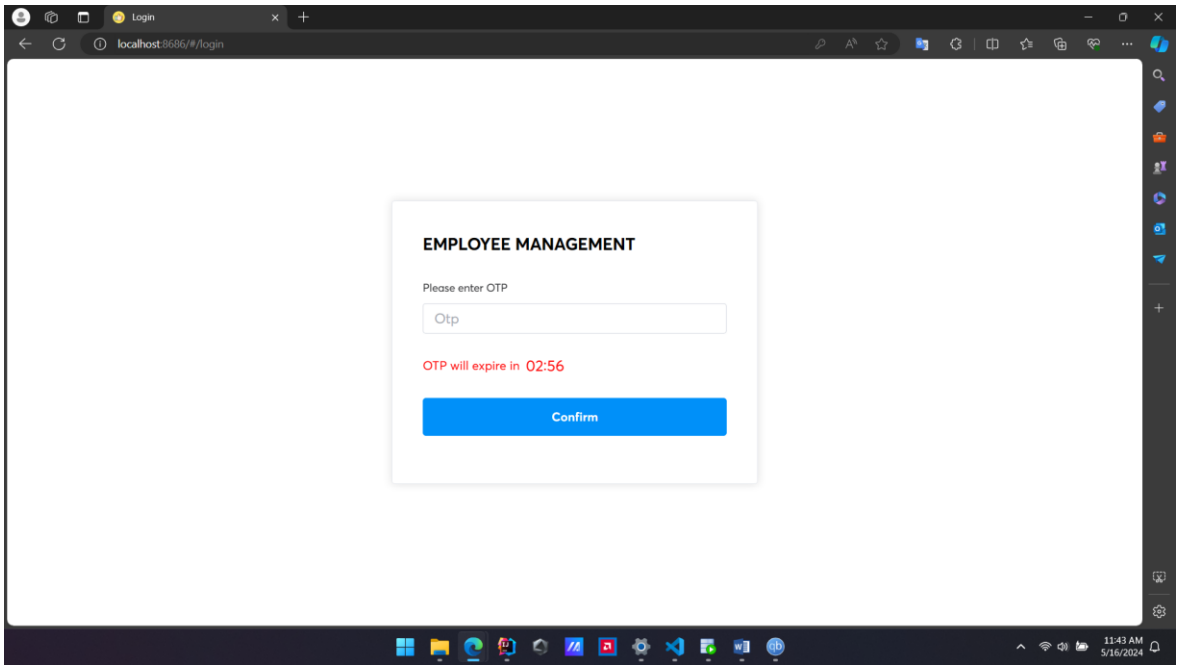


Figure 13: OTP verification

Use Case 2: Administrator Managing Employee Access

Another common requirement in SMEs is the centralised administration of user accounts, roles, and permissions. Typically, a designated administrator oversees the onboarding of new personnel, modifies existing privileges, and revokes access when employees leave or transfer departments. In such environments, administrators enjoy far-reaching control, rendering their accounts a prime target for malicious actors. Hence, any compromise of an admin account could grant adversaries broad system visibility and an opportunity to escalate attacks internally. A Zero-Trust architecture mitigates these risks by imposing robust, context-aware policies and continuously verifying both user identity and session integrity.

The key actor in this scenario is the Administrator – assigned the highest privilege level in the LZTA. Before any privileged action, such as creating or removing user accounts, the administrator must undergo the same initial checks as ordinary users, albeit with stricter contextual verification (e.g., permissible IP addresses limited to corporate subnets) and MFA. Upon entering valid credentials, the system dispatches a OTP to the admin's registered device or email, ensuring that credentials alone are insufficient for elevated tasks. Only when both password and OTP checks pass does the gateway issue a token reflecting the Admin role, granting the user high-level access within a narrowly defined administrative console.

http://doi.org/10.18080/jtde.v13n3.1284

Once authenticated, the administrator can navigate role definitions – such as User or Manager – and revise departmental assignments or privileges as needed. Each such change is logged at multiple layers: the role-based authorisation module confirms that the admin's token allows user management functions, while the auditing subsystem records the time of modification, the target user account, and the specific adjustments made. These logs provide vital forensic data in case of later disputes or security audits. By combining strict authentication requirements and fine-grained role checks, the architecture ensures that even privileged activities remain traceable and subject to Zero-Trust safeguards. This layered approach constrains the potential damage from compromised admin credentials and helps preserve security fidelity across the entire system. Figure 14 and Figure 15 display the dashboards for a regular user (longhl) and an Admin (giangdh), respectively. Only the Admin has the authority to perform various actions (as shown in the Action column) within the system and manage users.

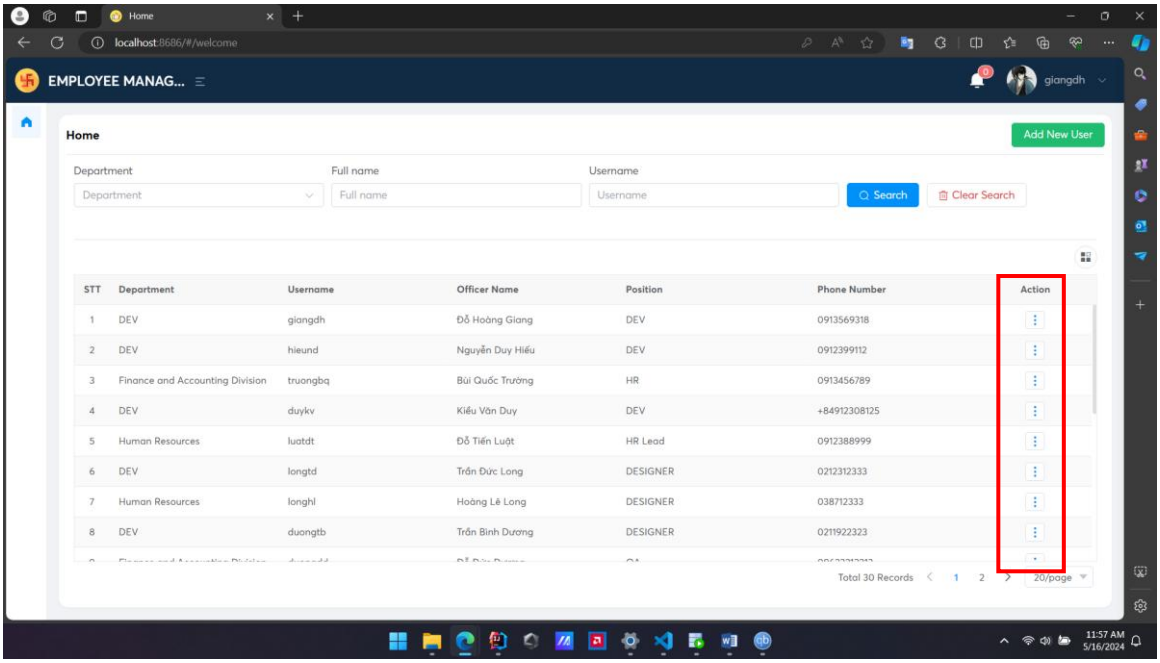


Figure 14: Normal user dashboard

In addition, to prevent misuse of unattended sessions, the LZTA enforces a short session timeout (e.g., 30 minutes of inactivity). As shown in Figure 16, if the Admin remains idle beyond this threshold, the system automatically invalidates the token and displays a 'Login session ended' prompt. This mechanism compels re-authentication, thus upholding Zero-Trust principles by denying indefinite access to privileged roles. Administrators, after logging back in, must again pass both password and MFA checks, ensuring that each privileged interaction is verifiably tied to a legitimate, current user session.

http://doi.org/10.18080/jtde.v13n3.1284

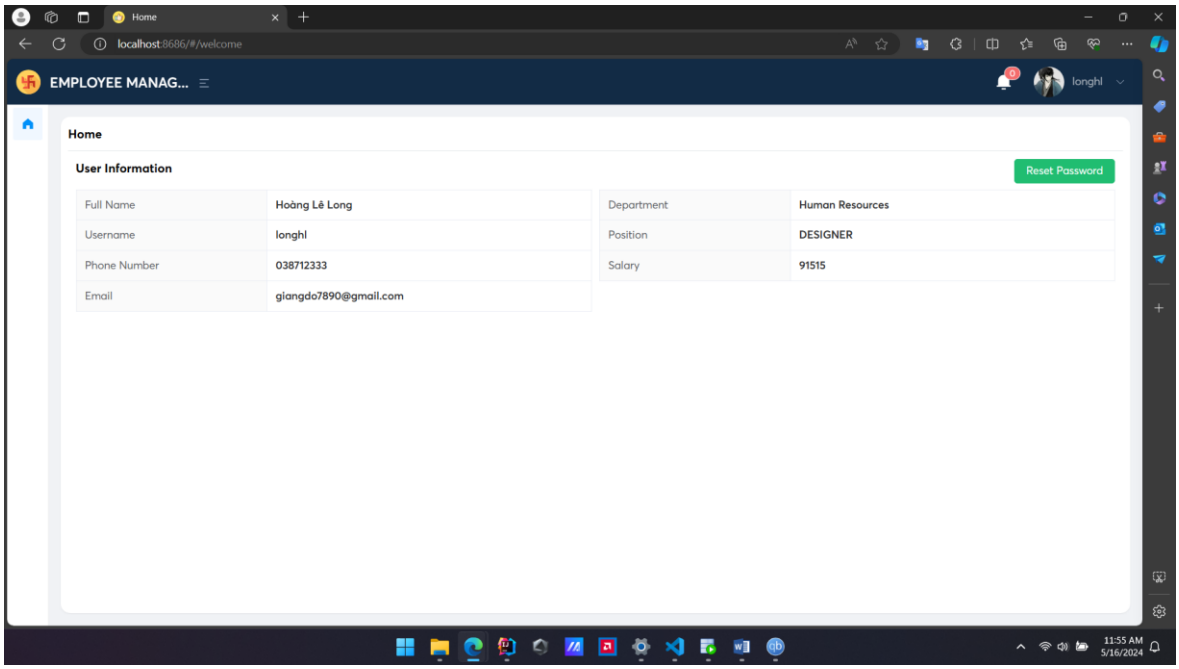


Figure 15: Admin has the authority to perform various actions

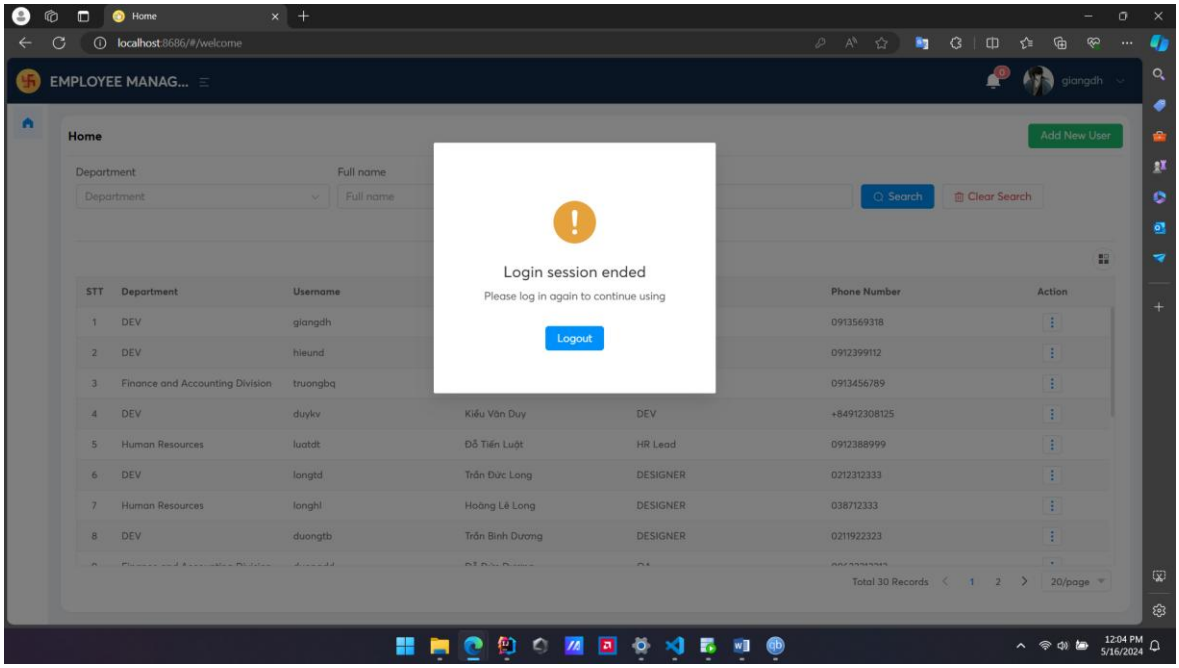


Figure 16: Short session timeout

Discussions

Technical Challenges

The implementation of the LZTA revealed several technical obstacles that shaped the system's evolution. Dependency conflicts during the integration of libraries for multi-factor

http://doi.org/10.18080/jtde.v13n3.1284

authentication and token management posed significant challenges. Resolving these required careful version alignment and iterative testing to ensure seamless functionality.

The incorporation of custom modules, such as Contextual Access Verification and RBAC, presented additional complexities. Ensuring smooth interactions between these modules and the central authentication gateway necessitated refining APIs and middleware configurations.

Lessons Learned

The development process underscored the importance of modular design. By compartmentalising functionalities into distinct components, such as the **JwtService** for token management and the **OTPService** for authentication, the system achieved greater flexibility and ease of maintenance. This approach enabled targeted debugging and iterative improvements without disrupting overall functionality.

Efficient contextual access controls proved vital for strengthening system security. The combination of IP and MAC address validation with time-based restrictions demonstrated the effectiveness of multi-dimensional access policies in mitigating unauthorised access. These insights affirm the viability of implementing Zero-Trust principles in resource-constrained SME environments, while emphasising the value of continuous refinement and scalability for long-term success.

Potential Feature Additions

Expanding the capabilities of the LZTA could significantly enhance its effectiveness and adaptability. AI-Driven Threat Detection (Kavitha & Thejas, 2024) represents a promising avenue, leveraging artificial intelligence to enable real-time monitoring and anomaly detection. Machine learning algorithms could analyse behavioural patterns and flag irregularities, offering proactive security measures.

Another enhancement involves Enhanced Contextual Access Controls through technologies like geofencing (Jayapradha & Singh, 2024) and advanced behavioural analytics (Al Mansur & Zaman, 2023). They could incorporate location-based restrictions and user activity profiling, further fortifying the system against unauthorised access.

User Adoption and Training

Adoption challenges may arise due to the perceived complexity of multi-factor authentication and role-based controls. Employees may resist changes that introduce additional steps into their workflows, requiring careful management of this transition.

http://doi.org/10.18080/jtde.v13n3.1284

Comprehensive training programs are essential to address these challenges. Workshops, interactive guides, and ongoing support can facilitate a smoother adoption process, ensuring users understand and effectively utilise the system. Tailored training for specific roles, such as administrators and end-users, further enhances engagement.

Conclusions

This research designed, implemented, and evaluated a Lightweight Zero-Trust Architecture tailored to the unique cybersecurity needs and resource constraints of SMEs. By integrating a Central Authentication Gateway that enforces contextual checks, multi-factor authentication, and role-based permissions, the proposed architecture provides a robust yet practical application of the '*never trust, always verify*' principle.

The LZTA's effectiveness was validated through both practical use cases and a comprehensive performance benchmark. The comparative analysis demonstrated the architecture's superior efficiency, showing that it maintains high throughput and low latency under a load of 100 concurrent users. Crucially, it outperformed both conventional API gateways and a generic open-source ZTA baseline by a significant margin, confirming that a lightweight, integrated approach can provide robust security without the substantial performance overhead typical of more complex solutions.

While the implementation faced typical technical challenges, this research successfully demonstrates that LZTA's simplicity and practicality do not come at the cost of performance. By balancing robust security with high efficiency, the proposed architecture provides a validated and accessible pathway for SMEs to adopt modern Zero-Trust principles. Future work will focus on enhancing the architecture with AI-driven threat detection and exploring enterprise-level scalability, further contributing to a secure and resilient digital ecosystem for SMEs.

References

Al Mansur, A., & Zaman, T. (2023). *User Behavior Analytics in Advanced Persistent Threats: A Comprehensive Review of Detection and Mitigation Strategies* 2023 7th International Symposium on Innovative Approaches in Smart Technologies (ISAS), IEEE, 1-6. https://doi.org/10.1109/ISAS60782.2023.10391553

Alex, B., & Taylor, L. (2022). *Spring Security*. Sping.io. Retrieved May 30, 2025 from https://docs.spring.io/spring-security/site/docs/3.2.0.RC1/reference/pdf/spring-security-reference.pdf

Allianz. (2024a). *Identifying the major business risks for 2024*. Retrieved May 30, 2025 from https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2024.pdf

Allianz. (2024b). *Leading risks for small enterprise companies worldwide from 2018 to 2024*. Retrieved May 30, 2025 from https://www.statista.com/statistics/1018196/leading-small-business-risks-globally/

Bashir, T. (2024). Zero Trust Architecture: Enhancing cybersecurity in enterprise networks. *Journal of Computer Science and Technology Studies*, *6*(4), 54-59. https://doi.org/10.32996/jcsts

Basta, N., Ikram, M., Kaafar, M. A., & Walker, A. (2022). *Towards a zero-trust micro-segmentation network security strategy: an evaluation framework* NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, IEEE, 1-7. https://doi.org/10.1109/NOMS54207.2022.9789888

Bellamkonda, S. (2022). Zero Trust Architecture Implementation: Strategies, Challenges, and Best Practices. *International Journal of Communication Networks and Information Security*, *14*, 587-591.

Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. *Global Journal of Engineering and Technology Advances*, *19*(2), 134-153. https://doi.org/10.30574/gjeta.2024.19.2.0084

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, *110*, 102436. https://doi.org/10.1016/j.cose.2021.102436

Cisco. (2024a). *Biggest cybersecurity risks for organizations worldwide as of February 2024, by type*. Retrieved May 30, 2025 from https://www-statista-com.ezproxy.lib.uwstout.edu/statistics/1474901/companies-biggest-cyber-threats-by-type/

Cisco. (2024b). *Most challenging areas for companies worldwide to protect against cyberattacks as of February 2024*. Retrieved May 30, 2025 from https://www-statista-com.ezproxy.lib.uwstout.edu/statistics/1475088/companies-cybersecurity-challenge-areas/

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023). *The new frontier of cybersecurity: emerging threats and innovations* 2023 29th International Conference on Telecommunications (ICT), IEEE, 1-6. https://doi.org/10.1109/ICT60153.2023.10374044

Dikanski, A., Steinegger, R., & Abeck, S. (2012). Identification and implementation of authentication and authorization patterns in the spring security framework. The Sixth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2012), 14-30.

Dissanayake, N., Jayatilaka, A., Zahedi, M., & Babar, M. A. (2022). Software security patch management-A systematic literature review of challenges, approaches, tools and practices. *Information and Software Technology*, *144*, 106771. https://doi.org/10.1016/j.infsof.2021.106771

Gani, A. B. D., & Fernando, Y. (2023). Digital empathy and supply chain cybersecurity challenges: concept, framework and solutions for small-medium enterprises.

International Journal of Management Concepts and Philosophy, *16*(1), 1-10. https://doi.org/10.1504/IJMCP.2023.128777

Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero Trust: Applications, Challenges, and Opportunities. *arXiv preprint arXiv:2309.03582*.

Gierke, O., Darimont, T., & Strobl, C. (2012). *Spring Data JPA-Reference Documentation*. Retrieved May 30, 2025 from https://docs.spring.vmware.com/spring-data-jpa-distribution/docs/3.1.13/reference/html/index.html

Gokhale, A., & Kulkarni, S. (2023). Enhanced Zero Trust Implementation--a novel approach for effective network policy management and compliance tracking. *Authorea Preprints*. https://doi.org/10.22541/au.168517996.68474374/v1

Habash, R. M. (2023). Zero Trust Security Model for Enterprise Networks. *Iraqi Journal of Information and Communication Technology*, *6*(2), 68-77. https://doi.org/10.31987/ijict.6.2.223

Hasan, M. (2024). Enhancing Enterprise Security with Zero Trust Architecture. *arXiv preprint arXiv:2410.18291*.

He, Y., Huang, D., Chen, L., Ni, Y., & Ma, X. (2022). A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, *2022*(1), 1-13. https://doi.org/10.1155/2022/6476274

Hong, S., Xu, L., Huang, J., Li, H., Hu, H., & Gu, G. (2023). SysFlow: Toward a programmable zero trust framework for system security. *IEEE Transactions on Information Forensics and Security*, *18*, 2794-2809. https://doi.org/10.1109/TIFS.2023.3264152

IBM. (2024). *Cost of a Data Breach Report 2024*. Retrieved May 30, 2025 from https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

Instillery, T. (2023). *Zero Trust vs Traditional Security Models: How Do They Compare?* Retrieved May 30, 2025 from https://tinyurl.com/InstilleryZeroTrust

Jayapradha, J., & Singh, J. (2024). A Geo-Fencing Approach for a Location-Based Alert System. In *Applications of New Technology in Operations and Supply Chain Management* (pp. 1-14). IGI Global. https://doi.org/10.4018/979-8-3693-1578-1.ch001

Jones, M. (2015). JSON web token (JWT). *Internet Engineering Task Force (IETF) RFC*, *7519*.

Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and application of zero trust security: A brief survey. *Entropy*, *25*(12), 1595. https://doi.org/10.3390/e25121595

Kavitha, D., & Thejas, S. (2024). AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation. *IEEE access*, *12*, 173127 - 173136. https://doi.org/10.1109/ACCESS.2024.3493957

Keith, M., Schnicariol, M., Keith, M., & Schnicariol, M. (2010). Object-relational mapping. *Pro JPA 2: Mastering the Java™ Persistence API*, 69-106.

Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105-116. https://doi.org/10.30574/wjarr.2023.19.3.1785

Kocksch, L., & Jensen, T. E. (2024). The Mundane Art of Cybersecurity: Living with Insecure IT in Danish Small-and Medium-Sized Enterprises. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW2), 1-17. https://doi.org/10.1145/3686893

Lake, K. (2022). *The Benefits of Zero Trust Security to Small and Medium Enterprises*. Jumpcloud. Retrieved May 30, 2025 from https://jumpcloud.com/blog/zero-trust-benefits-smes

Luckett, J. (2024). *A Zero Trust Roadmap for Consumers and Small Businesses* Marymount University]. https://www.proquest.com/docview/3051318191

Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero Trust Cybersecurity: Procedures and Considerations in Context. *Encyclopedia*, *4*(4), 1520-1533. https://doi.org/10.3390/encyclopedia4040099

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *Plos one*, *19*(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

Metin, B., Özhan, F. G., & Wynn, M. (2024). Digitalisation and Cybersecurity: Towards an Operational Framework. *Electronics*, *13*(21), 4226. https://doi.org/10.3390/electronics13214226

Mmango, N., & Gundu, T. (2024). Cultivating Collective Armor: Towards a Collaborative Cybersecurity Resilience Framework for SMEs. *European Conference on Innovation and Entrepreneurship*, 523-531.

Nadella, G. S., Gonaygunta, H., Kumar, D., & Pawar, P. P. (2024). Exploring the impact of AI-driven solutions on cybersecurity adoption in small and medium enterprises. *World Journal of Advanced Research and Reviews*, *22*(1), 1190-1197. https://doi.org/10.30574/wjarr.2024.22.1.1185

NAVEX. (2024). *The State of Cybersecurity for Small and Medium Businesses*. Retrieved May 30, 2025 from https://www.navex.com/en-us/blog/article/the-state-of-cybersecurity-for-small-and-medium-businesses/

Oluokun, A., Idemudia, C., & Iyelolu, T. (2024). Enhancing digital access and inclusion for SMEs in the financial services industry through cybersecurity GRC: A pathway to safer digital ecosystems. *Computer Science & IT Research Journal*, *5*(7), 1576-1604. https://doi.org/10.51594/csitrj.v5i7.1277

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Proofpoint. (2024). *Most significant cybersecurity threats in organizations worldwide according to Chief Information Security Officers (CISO) as of February 2024*. Retrieved May 30, 2025 from https://www.statista.com/statistics/1350460/cybersecurity-threats-at-companies-worldwide-cisos/

Rahman, A., Indrajit, E., Unggul, A., & Dazki, E. (2024). Implementation of Zero Trust Security in MSME Enterprise Architecture: Challenges and Solutions. *Sinkron: jurnal dan penelitian teknik informatika*, *8*(3), 2077-2087. https://doi.org/10.33395/sinkron.v8i3.13949

Ramesh Chidirala, D. P., Henrique Trevisan, and Yeswanth Narra. (2024). *Implementing Zero Trust Security: A Practical Approach for SMBs*. AWS. Retrieved May 30, 2025 from https://aws.amazon.com/blogs/smb/implementing-zero-trust-security-a-practical-approach-for-smbs/

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. In *NIST Special Publication 800-207*: National Institute of Standards and Technology.

S-RM. (2023). *What were the biggest cyber security challenges for organizations in the United States and the United Kingdom in 2023?* Retrieved May 30, 2025 from https://www-statista-com.ezproxy.lib.uwstout.edu/statistics/1430256/top-cyber-security-challenges-for-organizations-in-the-us-and-uk/

Saleem, M., Warsi, M., & Islam, S. (2023). Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. *Journal of Information Security and Applications*, *72*, 103389. https://doi.org/10.1016/j.jisa.2022.103389

Samira, Z., Wondaferew, Y., Osundare, O. S., Ekpobimi, H. O., & Kandekere, R. C. (2024). Comprehensive data security and compliance framework for SMEs. *Magna Scientia Advanced Research and Reviews*, *12*(1), 043-055. https://doi.org/10.30574/msarr.2024.12.1.0146

Sandhu, R. S. (1998). Role-based access control. In *Advances in computers* (Vol. 46, pp. 237-286). Elsevier. https://doi.org/10.1016/S0065-2458(08)60206-5

Shojaifar, A., & Järvinen, H. (2021). *Classifying SMEs for approaching cybersecurity competence and awareness* Proceedings of the 16th International Conference on Availability, Reliability and Security, ACM, 1-7. https://doi.org/10.1145/3465481.3469200

Skanda, C., Srivatsa, B., & Premananda, B. (2022). *Secure Hashing using BCrypt for Cryptographic Applications* 2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon), IEEE, 1-5. https://doi.org/10.1109/NKCon56289.2022.10126956

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE access*, *10*, 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679

Syrotynskyi, R., Tyshyk, I., Kochan, O., Sokolov, V., & Skladannyi, P. (2024). Methodology of network infrastructure analysis as part of migration to zero-trust architecture. *Cyber Security and Data Protection 2024*(3800), 97-105.

Thomas, J., & Galligher, G. (2018). Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science*, *11*(1), 14. https://doi.org/10.5539/cis.v11n1p14

Wang, X., Mansour, S., & El-Said, M. (2022). *Introducing Zero Trust in a Cybersecurity Course* Proceedings of the 23rd Annual Conference on Information Technology Education, ACM, 118-120. https://doi.org/10.1145/3537674.3555779

Worldbank. (2019). *Improving SMEs' access to finance and finding innovative solutions to unlock sources of capital*. Retrieved May 30, 2025 from https://www.worldbank.org/en/topic/smefinance

Xie, L., Hang, F., Guo, W., Lv, Y., & Chen, H. (2021). A micro-segmentation protection scheme based on zero trust architecture. ISCTT 2021; 6th International Conference on Information Science, Computer Technology and Transportation, VDE, 1-4.

Xu, W., Xie, Y., Lv, M., Sun, H., Li, A., & Zhao, H. (2022). *SDP Security Control Technology Based on Zero Trust* 2022 IEEE 4th International Conference on Civil Aviation Safety and Information Technology (ICCASIT), IEEE, 611-616. https://doi.org/10.1109/ICCASIT55263.2022.9986934

Zhang, K., Xu, S., & Shin, B. (2023). *Towards Adaptive Zero Trust Model for Secure AI* 2023 IEEE Conference on Communications and Network Security (CNS), IEEE, 1-2. https://doi.org/10.1109/CNS59707.2023.10288810

An Energy-Efficient Based Secure IOT Data Transfer with Hashed Data Access Policy Using ACROT-DHSKECC and LSCRC32

Tamarapalli Anjikumar
Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India

A.S.N. Chakravarthy
Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Kakinada, Andhra Pradesh, India

Abstract: The rapid expansion of Internet of Things (IoT) applications in healthcare has amplified the need for secure, efficient, and scalable data transmission frameworks. This study proposes an energy-aware and secure IoT-based data transmission architecture tailored for remote healthcare monitoring systems. Unlike conventional encryption-centric models, the proposed framework integrates lightweight double encryption (ACROT-DHSKECC) and hashed access control (LSCRC32) with optimised network path selection using clustering and Grasshopper Optimisation Algorithm (GOA). This integration reduces latency, enhances node-level energy efficiency, and secures data transmission over distributed networks. The system's design aligns with next-generation telecom infrastructure, making it well suited for deployment in 5G-enabled smart healthcare environments. Simulation results demonstrate reduced hash generation time, lower memory usage, and enhanced encryption performance, affirming its viability for secure data delivery in modern digital health ecosystems.

Keywords: Secure Data Transmission, IoT Healthcare, Energy-Efficient Communication, 5G Healthcare, Grasshopper Optimisation Algorithm (GOA).

Introduction

In the improvement of health, Healthcare (HC) plays a crucial role through prevention, diagnosis, treatment, and cure of disease, illness, injuries, and other physical as well as mental impairments in people (Javaid & Haleem, 2021). HC systems provide extra resources to keep patients in a safe atmosphere (Haghi *et al.*, 2021). A resource like the health records of the patients in the HC system consists of useful and confidential information regarding the patient's health (Adere, 2022). This clinical data of the patient includes the history of the

http://doi.org/10.18080/jtde.v13n3.1301

patient regarding the information of diagnosis, progression, and treatment taken for the disease (Ghazal *et al.*, 2022). In the HC system, data management monitors and ensures health data access for diagnosis and decision-making across the organisation in a coordinated manner (Alshamrani, 2022). By integrating Internet of Things (IoT) technology, the real-time data management in the HC system is performed.

HC services' quality and reliability are augmented by the integration of IoT technology with the traditional HC system (Comput *et al.*, 2021). Currently, an IoT system provides additional support for HC experts in terms of remote health monitoring (Chauhan *et al.*, 2020). The sensors connected to the patient's body automatically collect and transmit the required data over the Internet by utilising IoT technology and give access to the doctor from any place for identifying the disease (Humayun & Jhanjhi, 2021; Ghazal *et al.*, 2021). The IoT consists of a wireless connectivity network with medical devices that allow the patient's HC data to be shared via the Internet for further monitoring and decision-making (Karunarathne *et al.*, 2021). Yet, the IoT data's security, interoperability, and ethical concerns may be challenging in this system, which reduces the patient's privacy and safety because of sharing sensitive information (Ratta *et al.*, 2021). Therefore, by employing several encryption methodologies, the data security is augmented, and the network's interoperability is enhanced by some optimisation models (Bhuiyan *et al.*, 2021; Pradhan *et al.*, 2021).

Random Hashing Mechanism (RHM), Deep Neural Network (DNN), Access policy creation, Deep Belief Network (DBN), Elliptic Curve Cryptography (ECC), Routing protocols, Deep Sparse Auto Encoder (DSAE), Wildcard-fuzzy search, K-Nearest Neighbour (KNN), Butter Ant Optimisation (BAO), Digital Signature Algorithm (DSA), and Blockchain (BC) technology are some of the prevailing techniques utilised for secure health data transfer (DT) through the Internet (Dwivedi *et al.*, 2022; Rejeb *et al.*, 2023). Nonetheless, these methodologies do not ensure the security and privacy of the data owners and users based on their roles in the HC system. Thus, an energy-efficient secured IoT DT model is proposed with a hashed data access policy by using ACROT-DHSKECC and LSCRC32.

Although the proposed framework emphasises recent advancements in secure data transmission for IoT healthcare, it is fundamentally built upon well-established cryptographic principles. The encryption mechanism integrates ECC and provides high security with minimal computational overhead, ideal for constrained IoT environments (Koblitz, 1987; Miller, 1985). Furthermore, the model employs the classical Diffie–Hellman key exchange protocol to enable secure key agreement between communicating entities (Diffie & Hellman, 1976). In terms of access control, the proposed LSCRC32 hashing algorithm enhances the traditional CRC32 method by accelerating hash computation without compromising collision resistance (Peterson & Brown, 1961). These foundational contributions form the security

http://doi.org/10.18080/jtde.v13n3.1301

backbone of the proposed framework, ensuring that both legacy and modern cryptographic perspectives are adequately addressed.

The integration of IoT into healthcare systems has redefined modern clinical practices by enabling continuous, real-time patient monitoring, remote diagnostics, and timely intervention. This evolution, driven by the convergence of embedded devices and telecommunication infrastructure, supports emerging smart healthcare models within the broader digital economy. As data travels from wearable sensors to cloud platforms and healthcare professionals, maintaining the privacy, integrity, and reliability of that data becomes both a technological and regulatory imperative. However, while current research has focused primarily on cryptographic techniques, less attention has been paid to how these security measures impact the communication efficiency, energy consumption, and scalability of the underlying telecommunication networks. This paper bridges this gap by introducing a secure IoT data transmission model that is not only robust from a security standpoint but is also optimised for performance in real-world telecom settings – particularly those involving bandwidth-limited environments, edge devices, and 5G infrastructures.

Problem statement

Major limitations of the existing works:

- None of the prevailing techniques concentrates on enhancing the confidentiality along with privacy of data owners and users based on their roles.
- Load balancing was utilised to minimise energy consumption along with extending the network lifetime, but did not concentrate on the energy and distance of the nodes.
- A hybrid cryptographic technique was utilised for electronic health records. However, the key management for data security was not sufficient.
- Sometimes, the encrypted data was easily retrieved using the keyword, and it reduced the reliability of the system.
- The attributes-centric access control for electronic medical records has failed to create a complex and time-efficient access policy.

Main objectives

The major contributions of the proposed methodology to overcome the challenges in the prevailing works are:

- In this proposed model, a double encryption method with a hashed access policy ensures confidentiality and privacy for data owners and users based on their roles.

http://doi.org/10.18080/jtde.v13n3.1301

- K-Means-based clustering and Grasshopper Optimisation Algorithm (GOA)-based optimal path (OP) selection models are employed in the proposed system to reduce energy consumption along with extending the network lifetime by concentrating on the energy and distance of the nodes.
- Here, DHSKECC is utilised for efficient key management to improve the security level of the data.
- A double encryption method with data hiding by using ACROT-DHSKECC-based data encryption is proposed in this framework to avoid easy retrieval of the data by using keywords.
- The optimal attributes are selected by using the Artificial Algae Algorithm (AAA) and are used to create a hashed access policy by using LSCRC32, which will create a complex and minimum time consuming-based access policy.

The remaining parts of the paper are arranged as follows. The related works are analysed in a Literature Survey, the proposed methodology is elucidated in a section entitled "Proposed Methodology for Secure IoT Data Transmission", and the proposed framework's performance is discussed under Results and Discussion. A final Conclusion includes future recommendations.

Literature Survey

Ullah *et al.* (2021) presented an energy-efficient as well as reliable routing protocol for augmenting a wireless body area network's stability and reliability. For enhancing the network's stability, the developed model consisted of adaptive static clustering routing techniques. This model had a minimum end-to-end delay. However, this work did not concentrate on the energy and distance of the nodes.

Oliveira *et al.* (2023) presented an attribute-centric access control for electronic medical records. By using contextual attributes, this model developed the access control policy for ensuring that the data sharing was done with appropriate HC professionals in the acute care period. As per analysis results, this model effectively created a complex policy. Nevertheless, this model failed to create a complex policy with minimal time consumption.

Deepalakshmi (2021) presented a hybrid cryptographic access control for secure electronic health record retrieval from a cloud server. Here, an improved Key Generation Scheme of the Rivest, Shamir, Adleman (RSA) algorithm was used for encrypting the health data, and the Blowfish algorithm for encrypting the keys. As per the experimental results, this model

http://doi.org/10.18080/jtde.v13n3.1301

provided better security and also effectively retrieved the data from the cloud. Yet, the key management for data security was not sufficient.

Kumar *et al.* (2023) deployed a BC-orchestrated DSAE with Bidirectional Long Short-Term Memory (BiLSTM) for secure DT in IoT HC systems. For reducing security issues, the developed model was integrated with the off-chain storage interplanetary file system. As per the outcome, it surpassed the prevailing models in BC and non-BC settings. However, the resource consumption was high for secure DT.

Li *et al.* (2021) presented a ciphertext-policy weighted attribute-centric encryption technique in IoT-based HC systems. Here, by using 0-1 coding technology, an effective access control policy was created. Likewise, for ensuring data security, both online and offline encryption and outsourced decryption technologies were utilised. The developed model's efficacy in data security in the HC system was depicted by its outcome. Nonetheless, this model had high encryption and key generation times.

Kondaka *et al.* (2021) portrayed an iCloud Assisted Intensive Deep Learning (iCAIDL) model for an intensive HC monitoring system. Here, for detecting the situation of patients and alerting HC professionals, a machine learning approach was also utilised over the cloud IoT paradigm. The model's robustness in terms of better computational efficiency was exhibited in its outcome. Yet, due to the utilisation of remote servers, the security concern of this model was high.

Kathamuthu *et al.* (2022) advanced a deep Q-learning-centric neural network with a privacy preservation for data security in the HC IoT. The developed model protected the health data with less encryption along with decryption time by integrating neural networks. This model minimised network traffic along with communication errors. Yet, a large amount of data was required for learning purposes.

Masud *et al.* (2021) demonstrated an anonymity-preserving user authentication for IoT-centric HC systems. The developed scheme established secure access for the authorised user and prohibited the unauthorised user from getting access to the IoT-based health data. This model had fewer computation and communication costs. However, this model had the possibility for a privilege-insider attack on the HC data.

Chinaei *et al.* (2021) presented a BC logging contract-based optimal witnessing of IoT HC data. Here, the verification error was minimised by optimally selecting the witness, subject to the cost constraints. The analysis proved that this model had fewer errors and cost compared with other traditional models. Still, the overheads of this model were high for longer periods with variable witnesses.

http://doi.org/10.18080/jtde.v13n3.1301

Refaee *et al.* (2022) presented a secure and scalable HC DT in IoT by using BAO. For the HC data's dimensionality reduction, the principal component analysis method was wielded. Likewise, for extracting the features from the data, a modified local binary pattern model was used. Lastly, the fuzzy dynamic protocol enhanced the DT's overall security. As per the results, this model's superiority was high in secure DT. Yet, due to the error in the data labelling process, this model was less reliable.

Valivarthi & Kurniadi (2024) proposed a hybrid consensus mechanism combining Delegated Proof of Stake and Whale Optimisation for energy-efficient and secure IoT data sharing in fog computing. This consensus strategy is reflected in our proposed work through the adoption of lightweight cryptographic exchange using ACROT-DHSKECC to optimise energy consumption. As a result, the system achieves improved security and reduced resource overhead in IoT-based fog environments.

Secure user authentication using BLAKE2 hashing and Diffie-Hellman key exchange was proposed by Natarajan et al. (2024) for mobile cloud computing. Our proposed system adopts their approach by employing hashed data access policies and DHSKECC-based encryption to ensure secure key exchange within IoT environments. This technique enhances data confidentiality and access control while maintaining low computational overhead, making it suitable for resource-constrained IoT systems.

Our proposed model adopts the optimisation strategies and secure Directed Acyclic Graph (DAG) protocol framework introduced by Valivarthi et al. (2023) for fog-based IoT data sharing. By integrating LSCRC32 hashing and access-controlled encryption via ACROT, the system enhances secure and efficient data handling in constrained IoT environments. This approach ensures scalable and energy-efficient data transfer while maintaining robust access control.

Kadiyala & Kaur (2021) presented a decentralised data sharing system using co-evolutionary optimisation and hybrid cryptography for IoT environments. Our proposed framework incorporates this approach by employing isogeny-resilient hybrid encryption (DHSKECC) and hashed access policies for adaptive security. This ensures robust protection against evolving threats while maintaining lightweight performance.

A privacy-preserving cloud computing approach using enhanced homomorphic encryption guided by Multilayer Perceptron (MLP)-LSTM models was proposed by Srinivasan *et al.* (2025). Our framework builds on this strategy by integrating LSCRC32-based hashing and secure key exchange to safeguard data privacy in IoT data transfers. This integration ensures secure sharing with low latency and computational efficiency, making it well-suited for real-time IoT applications.

http://doi.org/10.18080/jtde.v13n3.1301

Proposed Methodology for Secure IoT Data Transmission by Using ACROT-DHSKECC and LSCRC32

Here, by using ACROT-DHSKECC and LSCRC32, an energy-efficient secure IoT DT model is proposed. Initially, in the hospital cloud server, the IoT sensor data of the patients is stored. A hashed access policy is created for security based on the attributes of the IoT data, patient, and doctor. In Figure 1, the proposed framework's structure is presented.

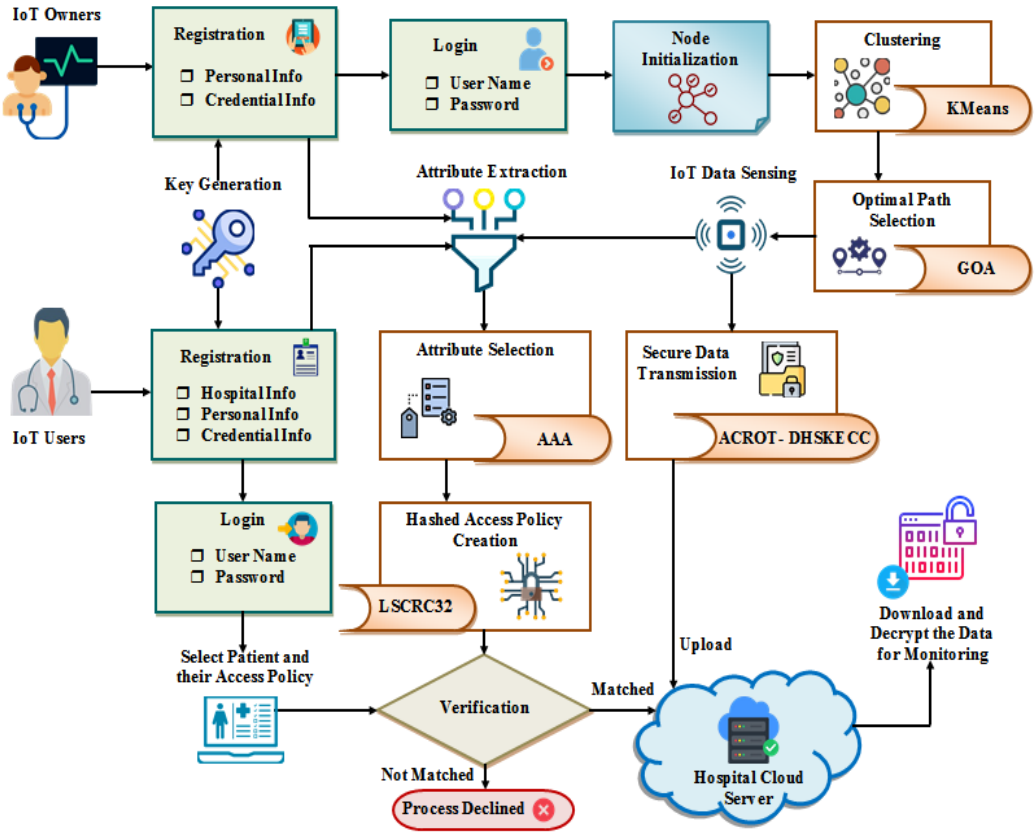


Figure 1. Structure of the proposed framework

Registration

Here, the p number of patients (P) (IoT owners) is registered with their personal information like name, age, sex, contact number, and address, and credential information like username and password. Next, P is equated as:

$$P = \{P_1, P_2, \ldots\ldots, P_p\} \tag{1}$$

Likewise, the d number of doctors (D) (IoT users) is also registered into the network with their hospital information like hospital ID, department, hospital name, and register number, personal information like name, age, sex, contact number, address, employee ID, and role, and credential information like username and password. The registered D is represented as:

http://doi.org/10.18080/jtde.v13n3.1301

$$D = \{D_1, D_2, \ldots\ldots, D_d\} \tag{2}$$

Public as well as private keys are generated and shared with the patient and doctor in registration. Then, by using their username and password, the patient logs in to the network.

Node initialisation

The patients who are logged in to the network are considered as nodes (P). Hence, the p number of nodes is initialised here.

Clustering

Then, to reduce the energy utilisation of the network, the nodes (P) are clustered by employing the K-Means clustering algorithm. K-Means could handle large numbers of data and can be easily scaled and adapted to different applications. At first, the cluster centroids (Ξ) for the R' number of clusters are initialised from (P). After initialisation, to measure the dissimilarity between them, the Euclidean distance is calculated between P and Ξ. Therefore, the Euclidean distance is calculated as:

$$\aleph(P, \Xi) = \sqrt{\sum (P - \Xi)^2} \tag{3}$$

Here, $\aleph(P, \Xi)$ signifies the Euclidean distance between P and Ξ. Further, by using $\aleph(P, \Xi)$, each (P) is assigned to the nearest centroid and is expressed as follows:

$$c_l = \underset{R'}{\operatorname{argmin}} \|\aleph(P, \Xi)\| \tag{4}$$

Here, c_l signifies the nearest centroid of the cluster. The centroid of each cluster is updated once all points have been assigned to a cluster and is given as follows:

$$\Xi^* = \frac{1}{\tau} \sum P \tag{5}$$

Here, τ depicts the total number of nodes in the $(R')^{\text{th}}$ cluster and Ξ^* signifies the updated centroid of the $(R')^{\text{th}}$ cluster. Till the maximum iterations ($\Xi^{*\max}$) is reached, the above step is continued. Thus, from (P), the data are clustered and are represented as follows:

$$H_{\text{clus}} = \{H_{\text{clus}}^1, H_{\text{clus}}^2, \ldots\ldots H_{\text{clus}}^{\text{nl}}\} \tag{6}$$

Here, H_{clus} signifies the clustered data of (P) and nl signifies the total number of clustered data in H_{clus}. Therefore, the OP for the DT is further selected based on H_{clus}.

Optimal path selection

Next, by using GOA, the OP for the DT is selected from H_{clus}. The Grasshopper Optimisation Algorithm (GOA) is highly effective in solving global unconstrained, along with constrained,

http://doi.org/10.18080/jtde.v13n3.1301

optimisation issues. The population (λ) of the grasshopper (i.e., paths within H_{clus}) is initialised as:

$$\lambda = \{\lambda_1, \lambda_2, \ldots\ldots, \lambda_r\} \tag{7}$$

where $r$signifies the number of grasshoppers. The fitness (φ) of the grasshopper is the minimum (min) distance (ϑ) to the food source, and it is depicted as:

$$\varphi = \min\{\vartheta\} \tag{8}$$

Primarily, the i^{th} grasshopper's position in the population based on φ is evaluated as:

$$\lambda_i = U_i + \ell_i + V_i \tag{9}$$

where λ_i signifies the i^{th} grasshopper's position, U_i signifies the interaction of the i^{th} grasshopper between the food source and other grasshoppers' swarms, ℓ_i depicts the gravity force on the i^{th} grasshopper, and V_i denotes the wind advection of the i^{th} grasshopper. Next, the position of the grasshopper is updated centred on U_i, ℓ_i, V_i of the grasshopper in the foraging and swarm behaviours. Thus, U_i, ℓ_i, and V_i are represented as follows:

$$U_i = \sum_{j=1}^{r} \wp\left(d_{\text{ij}}\right)\bar{d}_{\text{ij}}\text{, where } i \neq j\text{,} \tag{10}$$

$$d_{\text{ij}} = \left|\lambda_j - \lambda_i\right| \tag{11}$$

$$\bar{d}_{\text{ij}} = \frac{\left|\lambda_j - \lambda_i\right|}{d_{\text{ij}}} \tag{12}$$

Here, j signifies another grasshopper in the population, d_{ij} depicts the Euclidean distance betwixt the i^{th} and j^{th} grasshopper, λ_j denotes the j^{th} grasshopper's position, $\bar{d}_{\text{ij}}$ signifies the distance unit vector, and ($\wp$) depicts the strength of '2' social forces like repulsion ($\wp_1$) and attraction ($\wp_2$) betwixt grasshoppers. Then, $\wp$ is expressed as:

$$\wp = \text{ue}^{-\left(\frac{W'}{v}\right)} - e^{-W'} \tag{13}$$

Here, u and v characterise the intensity and length scale of $\wp$, respectively, e portrays the exponential function, and W' signifies a random number. Here, the repulsion and attraction forces are determined based on the expression:

$$\wp = \begin{cases} \wp_1, & \text{if } 0 \geq d_{ij} > 2.079 \\ \text{Neither } \wp_1 \text{ nor } \wp_2, & \text{if } d_{ij} = 2.079 \\ \wp_2, & \text{if } d_{ij} < 2.079 \end{cases} \tag{14}$$

Then, the gravity force is determined as:

$$\ell_i = -\upsilon \hbar_{\upsilon} \tag{15}$$

http://doi.org/10.18080/jtde.v13n3.1301

where υ signifies the gravitational constant, along with $\hat{\kappa}_{\upsilon}$signifying the unit vector towards the earth's centre. Next, the V_i of the grasshopper is estimated as:

$$V_i = s\hat{T}_s \tag{16}$$

Here, s signifies the drift constant and $\hat{T}_s$ signifies the wind direction's unit vector. Then, the i^{th} grasshopper's position is estimated as:

$$\lambda_i = \sum_{j=1}^{r} \wp\left(\left|\lambda_j - \lambda_i\right|\right)\left(\frac{\left|\lambda_j - \lambda_i\right|}{d_{\text{ij}}}\right) - \upsilon\hat{\kappa}_{\upsilon} + s\hat{T}_s \tag{17}$$

Yet, some grasshopper swarms quickly reach their comfort zone, so the grasshopper fails to converge to the location of the global solution. Thus, the dimension of the search space (t) is represented as:

$$\lambda_i^t = \hat{S}\left(\sum_{j=1}^{r} \hat{S}\frac{\text{ub}^t - \text{lb}^t}{2}\wp\left(\left|\lambda_j^t - \lambda_i^t\right|\right)\left(\frac{\left|\lambda_j^t - \lambda_i^t\right|}{d_{\text{ij}}}\right)\right) + \tilde{\kappa}_{\text{best}}^t \tag{18}$$

Here, $\hat{S}$ denotes the decreasing coefficient, ub^t and lb^t represent the upper and lower bound of t, respectively, and $\tilde{\kappa}_{\text{best}}^t$ simulates the tendency of the grasshopper to move towards the global best solution $\left(\lambda_{\text{best}}^t\right)$. Here, the gravity force of the grasshopper is not considered, and the wind advection is always pointed towards λ_{best}^t. The decreasing coefficient is responsible for reducing the grasshopper's movement around the target and search convergence around the target. Thus, $\hat{S}$ is depicted as:

$$\hat{S} = \hat{S}_{\max} - \text{it}\frac{\hat{S}_{\max} - \hat{S}_{\min}}{\text{it}_{\max}} \tag{19}$$

where $\hat{S}_{\max}$ and $\hat{S}_{\min}$ imply the maximum and minimum values of $\hat{S}$, respectively, and it and $\text{it}_{\max}$ represent the current and maximum iterations, respectively. Then, we update the grasshopper's position centred on the current position, global best position, and the position of all other grasshoppers in the swarm. The optimal position of the grasshopper is obtained at the end of $\text{it}_{\max}$, and it indicates the OP (ε) from $\Im$. Then, through the OP (ε), the IoT data are sensed.

IoT data sensing

Next, by using sensors, the IoT data of P are collected and are transferred through the selected ε to make it available for the doctor to monitor. The sensed IoT data (Γ) are represented as:

$$\Gamma = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_c\} \tag{20}$$

where c signifies the number of sensed IoT data.

http://doi.org/10.18080/jtde.v13n3.1301

Secure data transmission

To ensure confidentiality and secure sharing of IoT-generated healthcare data, the proposed framework employs a dual-layer encryption strategy integrating ACROT (ASCII Conjunction Rotate technique) and DHSKECC (Diffie–Hellman Secret Key over Elliptic Curve Cryptography). This section outlines the key concepts of these components and their role in securing the data flow, while omitting low-level mathematical derivations in favour of qualitative descriptions suitable for a system-oriented audience.

ACROT – Lightweight Data Obfuscation Layer

The ACROT algorithm serves as a lightweight ciphering technique designed to efficiently obscure plaintext using a combination of ROT13 character shifts and ASCII-level substitutions. To increase complexity beyond the limitations of traditional ROT schemes, ACROT introduces unique conjunction characters (e.g., <<) within the data stream and transforms these into obfuscated ASCII values. This process yields a preliminary ciphertext that is sufficiently randomised to resist trivial pattern analysis, while remaining computationally feasible for constrained IoT devices.

DHSKECC – Secure Key Agreement and Asymmetric Encryption

To securely transmit the ACROT-obfuscated data, the system applies a hybrid encryption mechanism that combines ECC with the Diffie–Hellman (DH) key exchange protocol. ECC provides the advantages of strong encryption with short key lengths, making it well-suited for IoT networks with limited bandwidth and processing power. The integration of DH enables both parties (patient and doctor) to compute a shared secret key over an insecure channel without transmitting the key itself, thus reinforcing the confidentiality of the exchanged data.

Key generation, public/private key exchange, and secret computation follow standard ECC and DH procedures, which are well-established in the cryptographic literature. Interested readers may refer to foundational references for mathematical details.

Encryption and Decryption Flow

At the sender (Patient side)

The sensed data are first obfuscated using ACROT. The obfuscated data are then encrypted using the doctor's ECC public key and the shared DH-based secret key.

At the receiver (Doctor side)

Upon receiving the ciphertext, the doctor decrypts it using their private ECC key and the shared secret. The original data are reconstructed by reversing the ACROT process.

http://doi.org/10.18080/jtde.v13n3.1301

This dual-layer encryption mechanism enhances both security and efficiency, balancing robustness against cryptanalytic attacks with suitability for low-power healthcare IoT devices.

Although the proposed framework introduces ACROT (ASCII Conjunction with ROT13) as part of its encryption pipeline, it is important to emphasise that ACROT is not intended to function as a standalone encryption algorithm. Rather, it serves as a lightweight data obfuscation layer designed to introduce minimal transformation to plaintext data before robust encryption. The ACROT process performs basic character substitution using ROT13 logic and ASCII-based transformations to obscure patterns in the raw data, particularly suited for repetitive IoT sensor outputs. However, the core cryptographic strength of the system lies entirely in the DHSKECC module, which securely combines ECC with Diffie–Hellman key exchange to achieve confidentiality and secure key agreement. This layered structure allows ACROT to operate as a pre-processing step that may assist in data compression or format masking without compromising overall security. We explicitly acknowledge that ACROT, by itself, does not meet standard cryptographic criteria for confidentiality, integrity, or resistance to known attacks, and its use is purely for lightweight pre-processing in resource-constrained IoT devices. All cryptographic assurances – such as secure key distribution, confidentiality, and access control – are achieved through ECC-based encryption and hashed policies generated via LSCRC32. The proposed system does not rely on ACROT for security-critical functions, and this clarification ensures transparency in both design and implementation.

Hash-Based Access Control

In addition to encryption, access control is implemented using a hashed policy generated by the Large-Speed CRC32 (LSCRC32) algorithm, which improves upon traditional CRC32 by processing 16 bits per iteration instead of 8. This method ensures rapid hashcode generation with strong collision resistance, making it ideal for resource-constrained environments.

However, real-world IoT deployments encounter various constraints, particularly device heterogeneity. This refers to the variation in hardware capabilities, communication protocols, operating systems, data formats, energy resources, and security features among IoT devices. In healthcare IoT (IoT-HC) ecosystems, this includes a wide array of wearable sensors, implantable devices, mobile phones, smart hospital equipment, and cloud-based data centres. This heterogeneity introduces several challenges in IoT system design. Interoperability becomes difficult due to different manufacturers using proprietary standards (which hinders seamless communication), data aggregation, real-time monitoring, and centralised decision-making. Security inconsistencies also arise, as some devices support advanced encryption mechanisms like ECC, while others with limited processing or memory capabilities may only support basic encryption or none at all, creating vulnerabilities in the system. Additionally, discrepancies in data formats, such as JSON, XML, or binary streams, necessitate real-time

http://doi.org/10.18080/jtde.v13n3.1301

translation or standardisation, which complicates integration and analysis. Devices also vary in computational capacity; lightweight wearables may not have sufficient resources to perform operations like on-device encryption or access control policy evaluation, which then need to be offloaded to fog or cloud servers.

In the context of the proposed framework, which integrates double encryption using ACROT-DHSKECC and hashed access control using LSCRC32, these issues become critical. Low-power devices might face difficulties in executing ASCII transformations or Diffie-Hellman key exchanges in real time, and memory-constrained devices may struggle with the LSCRC32-based access control verification. These limitations indicate a reliance on edge or cloud servers for processing. To address these issues, several mitigation strategies can be employed. Middleware platforms like IoTivity, EdgeX Foundry, or Node-RED can help manage interoperability. Adaptive security mechanisms that adjust encryption complexity based on device capacity can maintain a balance between performance and protection. Standardisation efforts, such as adopting IEEE 11073 for medical device communication and employing ontologies for data harmonisation, can improve semantic compatibility. Edge computing can be used to handle intensive operations, reducing the burden on constrained devices. Additionally, cross-layer optimisation, which combines energy-aware routing protocols like GOA with clustering techniques that consider device heterogeneity, can help distribute workloads effectively. Overall, device heterogeneity is a fundamental constraint in real-world IoT systems, and addressing it through modular, lightweight, and adaptive solutions is essential for achieving scalable, secure, and efficient deployments in healthcare and other domains.

Attribute extraction

Next, the attributes are extracted from $\Gamma, P,$ and D for creating the access policy. From Γ, the attributes like file name, absolute path, file type, file size, parent folder, free space, total space, usable space, hash code, creation time, accessed time, modified time, hidden, executable, readable, writable, and key are extracted. Then, from P, attributes like patient id, patient name, age, sex, contact number, place, public key, and private key are extracted. Similarly, from D, the hospital id, doctor id, hospital name, doctor name, branch, hospital register number, age, sex, contact number, place, doctor's specialisation, Universally Unique Identifier (UUID), public key, and private key attributes are extracted. The total extracted attributes are denoted as S.

http://doi.org/10.18080/jtde.v13n3.1301

Attribute selection

Further, by using AAA, the optimal attributes are selected from S. The Artificial Algae Algorithm (AAA) can attain the optimal solution's convergence and discovery via its adaptation and evolution processes. The population of the algal colony (S) is initialled as:

$$S = \{S_1, S_2, \ldots, S_h\} \tag{21}$$

where h characterises the number of algal colonies in the population. Next, the algal colony's initial position is depicted as:

$$S_{a,b}^{E} = S_a^{\min} + (S_a^{\max} - S_a^{\min}) \times \alpha_1 \tag{22}$$

Here, $S_{a,b}^{E}$ signifies the position of the a^{th} algal colony in the b^{th} position of the search dimension (E), $S_a^{\max}$ and $S_a^{\min}$ signify the maximum and minimum searching range in E, respectively, and α_1 represents a random number. The fitness (χ) of the algal colony is the high hashcode complexity (hc), and it is illustrated as:

$$\chi = \max\{\text{hc}\} \tag{23}$$

Based on χ, the algal colony's position is updated under the evolutionary phase. Here, the algal colony with the highest χ (χ_{high}) grows more and reproduces itself in the environment, while the algal colony with the lowest χ (χ_{low}) fights for survival. The algal colony's growth is illustrated by the Monod function (Z), and the size of the a^{th} algal colony (L_a) determined by Z is expressed as:

$$L_a^{w+1} = Z \cdot L_a^{w}, \text{where } a = \{1,2,\ldots,h\} \tag{24}$$

Here, w and $w+1$ denote the current and next iteration, respectively. The Monod function is depicted as:

$$Z = \frac{2\chi}{L_a + 2\chi} \tag{25}$$

Then, the energy level of each algal colony is estimated as:

$$\omega = \frac{L_a^2 - L_{\min}^2}{L_{\max}^2 - L_{\min}^2} \tag{26}$$

The algal colony's algal cell is illustrated as:

$$\chi_{\text{high}} = \max L_a^{w} \tag{27}$$

$$\chi_{\text{low}} = \min L_a^{w} \tag{28}$$

Here, the single algal cell of χ_{high} replicates the algal cell of χ_{low} in w, and it is denoted as:

$$\chi_{\text{low}}^{w} = \chi_{\text{high}}^{w} \tag{29}$$

http://doi.org/10.18080/jtde.v13n3.1301

Then, the insufficiently grown algal colony tries to resemble itself as χ_{high} in the adaptation process based on the starvation level (ϕ) in the environment, and it is described as:

$$\phi^{w} = \max\phi_{a}^{w} \tag{30}$$

where ϕ_{a}^{w} signifies the a^{th} algal colony's starvation level in the w^{th} iteration and ϕ^{w} depicts the algal colony with the highest starvation level. The starvation level increases when the algal cell has insufficient light. Thus, χ_{low} having the highest starvation level is adapted to χ_{high} and is expressed as follows:

$$\phi^{w+1} = \phi^{w} + \left(\phi_{\text{big}}^{w} - \phi^{w}\right) \times r_{\text{an}} \tag{31}$$

Here, ϕ_{big}^{w} signifies the biggest algal colony and r_{an} represents the random value. Afterwards, in the algal cell's helical movement, the gravity restricting the movement is represented as 0, and the viscous drag of the algal cell is displayed as shear force, which is directly proportional to the algal cell size. The friction surface (k) of the colony also depends on its size. The friction surface and the distance to the light source determine the helical movement's step size in '3' dimensions and are illustrated as:

$$L_{a_1}^{w+1} = L_{a_1}^{w} + \left(L_{a_1}^{M} - L_{a_1}^{w}\right)(\Delta - k_a)\xi' \tag{32}$$

$$L_{a_2}^{w+1} = L_{a_2}^{w} + \left(L_{a_2}^{M} - L_{a_2}^{w}\right)(\Delta - k_a)\cos\alpha' \tag{33}$$

$$L_{a_3}^{w+1} = L_{a_3}^{w} + \left(L_{a_3}^{M} - L_{a_3}^{w}\right)(\Delta - k_a)\sin\beta' \tag{34}$$

Here, $a_1, a_2,$ and a_3 depict the three different algal cells selected from the a^{th} algal colony, Δ is the shear force of the algal cell, α' and β' are the random angles, ξ' represents a random number, and M depicts the index value from the tournament selection process that works as a light source for the algal cells. Here, the friction surface is described as:

$$k = 2\pi\left(\sqrt[3]{\frac{3L_a}{4\pi}}\right)^{2} \tag{35}$$

Lastly, we check whether the χ_{low} effectively adapted to χ_{high} with minimum ω or not. The above process continues until the maximum iteration (w_{max}) is reached. Thus, the optimal attributes $\left(\hbar_{\text{opt}}\right)$ are selected at the end of w_{max}.

Hashed access policy creation

Then, by using Large Speed Cyclic Redundancy Check 32 (LSCRC32), the hashed access policy is created based on $\hbar_{\text{opt}}$. The conventional CRC32 has a relatively simple mathematical foundation, which makes it easy to implement. CRC32 is specifically designed to detect changes in data, making it highly effective for data verification. In CRC32, each byte is

http://doi.org/10.18080/jtde.v13n3.1301

processed one by one while generating the hash value. So, in order to improve the speed in the computations, we are using LSCRC32 where we are processing two bytes at a time instead of one byte. At first, based on $\hbar_{\text{opt}}$, an initialisation vector (ξ) is selected as the initial hash value(δ_0) in the LSCRC32 algorithm. Thus, ξ is a 32-bit value, and it is depicted as:

$$\delta_0 = \xi \tag{36}$$

Next, two bytes of δ_0 are processed at a time instead of one byte and is denoted as ρ_m. Next, ρ_m and the first two bytes of the data ρ_{m-1} are processed using the XOR operation:

$$\Sigma_m = \rho_m \oplus \rho_{m-1} \tag{37}$$

Here, Σ_m signifies the current hash value. After that, Σ_m is left shifted by one bit and is given as follows:

$$\delta_m = \Sigma_m << 1 \tag{38}$$

Here, δ_m characterises the shifted hash value. Next, δ_m is XORed with a generator polynomial using the following condition based on the Most Significant Bit (MSB) value:

$$\mathfrak{F} = \begin{cases} \delta_m \oplus g_p, & \text{if MSB} = 1 \\ \delta_m \otimes g_p, & \text{if MSB} \neq 1 \end{cases} \tag{39}$$

Here, g_p signifies the generator polynomial, $\delta_m \otimes g_p$ signifies that the XOR operation cannot be applied with δ_m and g_p, and $\mathfrak{F}$ represents the updated hash value. Thus, the final hash value is obtained based on the $\mathfrak{F}$ and is expressed as:

$$\mathfrak{H} = \mathfrak{F} \oplus \xi \tag{40}$$

where $\mathfrak{H}$ characterises the final hash value. Therefore, the hashed access policy is created and is denoted as δ_{m+1}.

The pseudocode for LSCRC32 is presented here.

http://doi.org/10.18080/jtde.v13n3.1301

Pseudocode for LSCRC32 algorithm

Input: Optimal attributes, $(\hbar_{\text{opt}})$
Output: Hashed access policy, δ_{m+1}

Begin
Initialise vector (ξ)
Select initial hash value (δ_0)
For each $\hbar_{\text{opt}}$ **do**
Process (ρ_m)
Compute $\Sigma_m = \rho_m \oplus \rho_{m-1}$
Apply $\delta_m = \Sigma_m << 1$ *# Left Shift*
Update hash value
If (MSB $= 1$) **{**
$\mathfrak{F} = \delta_m \oplus g_p$
} else (MSB $\neq 1$) **{**
$\mathfrak{F} = \delta_m \otimes g_p$
} end if
Compute final hash value, $\mathfrak{I} = \mathfrak{F} \oplus \xi$
End For
Return hashed access policy, δ_{m+1}
End

Next, for further verification process, the generated hashed access policy is stored in the system.

Monitoring process

The registered D login to the network for the monitoring process by using a username and password. After login, the doctors select the patient and get their hashed access policy$\left(\Theta(\delta_{m+1})\right)$. Then, $\Theta(\delta_{m+1})$ and δ_{m+1} are checked for the verification process (Ψ), and it is depicted as:

$$\Psi = \begin{cases} \Theta(\delta_{m+1}) = \delta_{m+1}, & \text{allow} \\ \Theta(\delta_{m+1}) \neq \delta_{m+1}, & \text{declined} \end{cases} \tag{41}$$

The doctor downloads and decrypts the data from the hospital server when the hashed access policy matches by using private and public keys generated during registration for monitoring; otherwise, the process is declined. Thus, the IoT data collected from the IoT users are securely transmitted and stored in the hospital cloud server. The proposed framework's performance is discussed further.

http://doi.org/10.18080/jtde.v13n3.1301

Complex secure system architecture for healthcare IoT

The proposed system introduces a complex secure architecture specifically tailored to the demands of modern healthcare IoT environments. This complexity arises not from unnecessary computational overhead but from the layered and integrated design that addresses multiple operational and security requirements simultaneously. At its core, the system employs dual-layer encryption: the lightweight ASCII Conjunction Rotate (ACROT) for fast obfuscation and the robust Diffie–Hellman over Elliptic Curve Cryptography (DHSKECC) for secure asymmetric key exchange. To enforce fine-grained access control, the model generates hashed access policies using LSCRC32. This enhanced cyclic redundancy check algorithm supports faster and more secure hash generation than traditional CRC methods. Beyond encryption and access control, the system uses K-Means clustering and the Grasshopper Optimisation Algorithm (GOA) to manage energy consumption and optimise path selection for data transmission — key to maintaining performance in bandwidth-constrained and heterogeneous IoT environments. The combination of these elements results in a multi-layered, modular system that ensures confidentiality, access control, low-latency transmission, and energy efficiency. Such an approach meets the stringent demands of real-world healthcare deployments, particularly within 5G-enabled networks, mobile edge computing (MEC), and smart hospital ecosystems. Unlike simplistic encryption-only solutions, the proposed architecture offers a comprehensive security framework that is both functionally rich and performance-aware, capable of adapting to complex healthcare operational settings.

Results and Discussion

Here, the proposed model's performance is analysed to prove this model's efficacy in securely transmitting HC data via the Internet. The proposed model is implemented in the working platform of JAVA by using publicly available data sources.

Experimental setup

To ensure the reproducibility and validity of the reported experimental results, the system configuration and software environment used for implementing and evaluating the proposed framework are detailed in this section. All experiments were conducted on a desktop computer equipped with an Intel Core i7-11700 processor (2.50 GHz, 8 cores), 16 GB RAM, and a 512 GB solid-state drive (SSD), running Windows 11 Pro 64-bit. The implementation of the proposed ACROT-DHSKECC and LSCRC32 algorithms was carried out in Java (JDK version 1.8) using the Eclipse IDE (2023-03 release). No external cryptographic libraries or third-

http://doi.org/10.18080/jtde.v13n3.1301

party simulation frameworks were used; all functionalities were developed using standard Java packages.

Performance evaluation metrics such as key generation time, encryption/decryption time, memory usage, and hashcode generation time were recorded across five benchmark healthcare datasets. Each experiment was repeated ten times, and the average values were reported to minimise the effects of transient computational overheads. The performance parameters (e.g., execution time in milliseconds, memory usage) are inherently dependent on the hardware and software environment in which the experiments were executed. The above configuration is provided to enable accurate replication of results and to support reproducibility across independent validation studies.

Dataset description

For implementing the proposed framework, five publicly available healthcare datasets were utilised: the Polycystic Ovary Syndrome (PCOS) dataset, heart disease dataset, diabetes dataset, breast cancer dataset, and obesity dataset. All datasets were sourced from open-access repositories such as Kaggle and the UCI Machine Learning Repository. Only attributes measurable through IoT-based sensors were selected for analysis. Table 1 summarises the key IoT-relevant features used from each dataset.

Table 1. Dataset description

Datasets	Source	Total number of attributes	Utilised IoT-based attributes
PCOS dataset	Kaggle (PCOS Dataset, n.d.)	44	Pulse rate, relative risk, haemoglobin.
Heart disease dataset	UCI ML Repository (Heart Disease Dataset, n.d.)	14	Resting blood pressure, cholesterol level, fasting blood sugar level, resting electrocardiographic measurement, thalach.
Diabetes dataset	UCI ML Repository (Pima Indians Diabetes Database, n.d.)	9	Glucose, blood pressure, skin thickness, insulin, body mass index, diabetes pedigree function.
Breast cancer dataset	UCI ML Repository (Breast Cancer Wisconsin (Diagnostic) Data Set, n.d.)	32	radius_mean, texture_mean, perimeter_mean, area_mean, smoothness_mean.
Obesity dataset	Kaggle (Obesity Levels Dataset, n.d.)	17	Frequently consumed high-calorie food, frequency of consumption of vegetables, number of main meals, and consumption of water daily.

In this framework, only data collected through IoT-compatible physiological or behavioural sensors were considered for further analysis to maintain consistency with the system's sensing capabilities.

http://doi.org/10.18080/jtde.v13n3.1301

Performance analysis

Here, the proposed methodologies' performances are weighed against the existing models in order to prove the proposed models' robustness.

Performance evaluation of proposed ACROT-DHSKECC

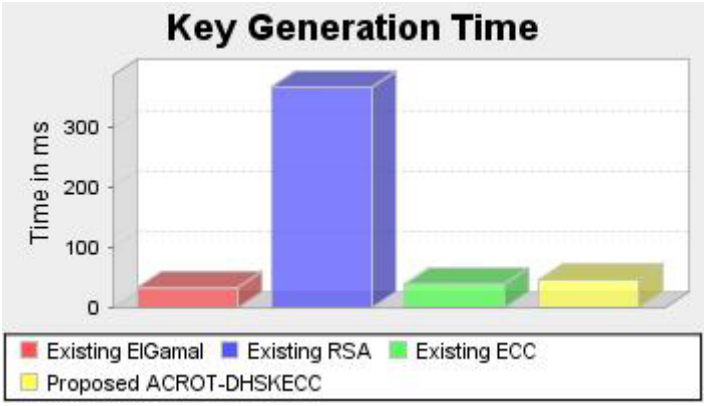


Figure 2. Performance analysis of the proposed ACROT-DHSKECC in terms of key generation time

In Figure 2, regarding key generation time, the proposed ACROT-DHSKECC's performance is analogised to prevailing ECC, RSA, and ElGamal. The proposed ACROT-DHSKECC had a key generation time of 45 ms, which was higher than the existing ECC due to the secret key generation employing DH in the ACROT-DHSKECC. Yet, when analogised to the existing RSA and Elgamal, the proposed approach took less key generation time. Although the ACROT-DHSKECC approach shows an increase in key generation time compared to standard ECC, this is a deliberate design choice to enhance key agreement security by incorporating Diffie-Hellman. Rather than emphasising performance efficiency in terms of speed, the method aims to offer a more secure and robust key exchange while maintaining acceptable latency. Thus, the proposed approach should be viewed as a security-optimised encryption strategy rather than a purely time-optimised one.

Figures 3(a) and 3(b) show the proposed ACROT-DHSKECC's performance for various datasets centred on encryption and decryption time. Regarding encryption and decryption time, the ACROT-DHSKECC for the breast cancer dataset was 142 ms and 124 ms, respectively, which were higher than the existing ECC. Similarly, for all other datasets, the existing ECC took less time for the encryption and decryption process than the proposed approach and existing approaches, such as RSA and ElGamal. However, the proposed ACROT-DHSKECC attained less encryption and decryption time compared to RSA and ElGamal. Thus, the proposed model effectively secures DT within IoT networks while optimising time usage.

http://doi.org/10.18080/jtde.v13n3.1301

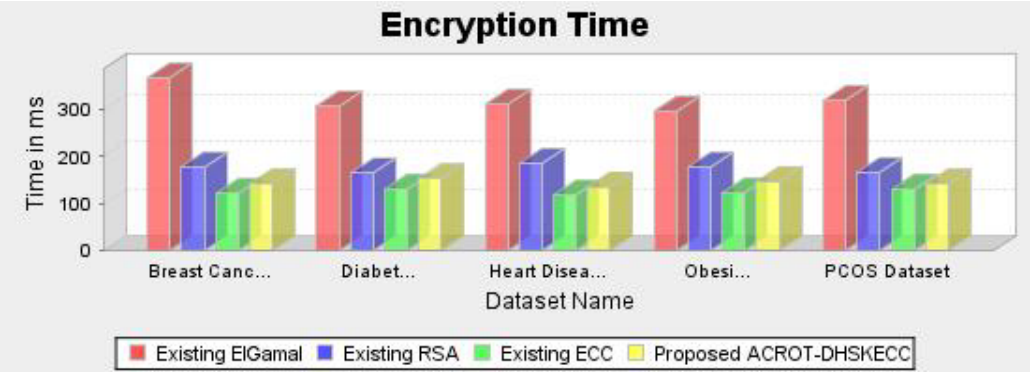


Figure 3(a). Encryption time analysis

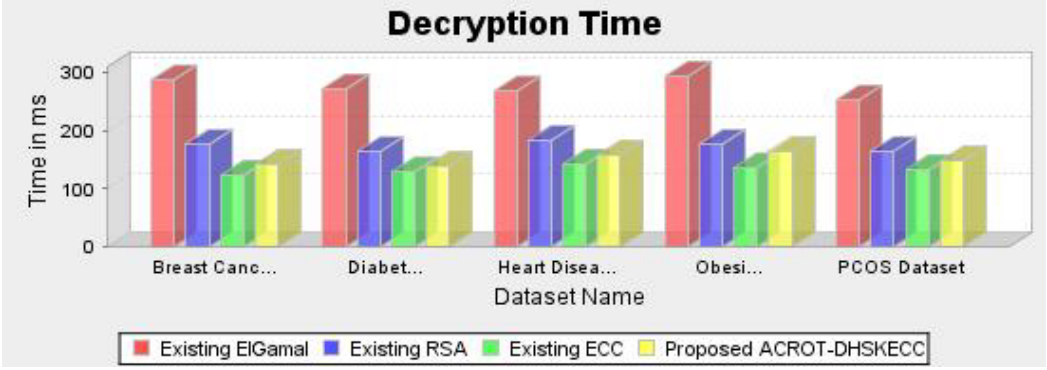


Figure 3(b). Decryption time analysis

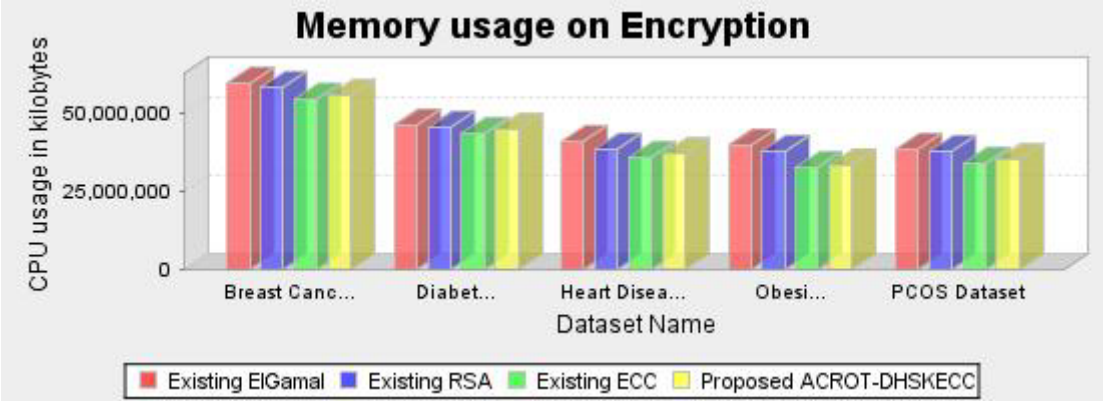


Figure 4(a). Memory usage on encryption analysis

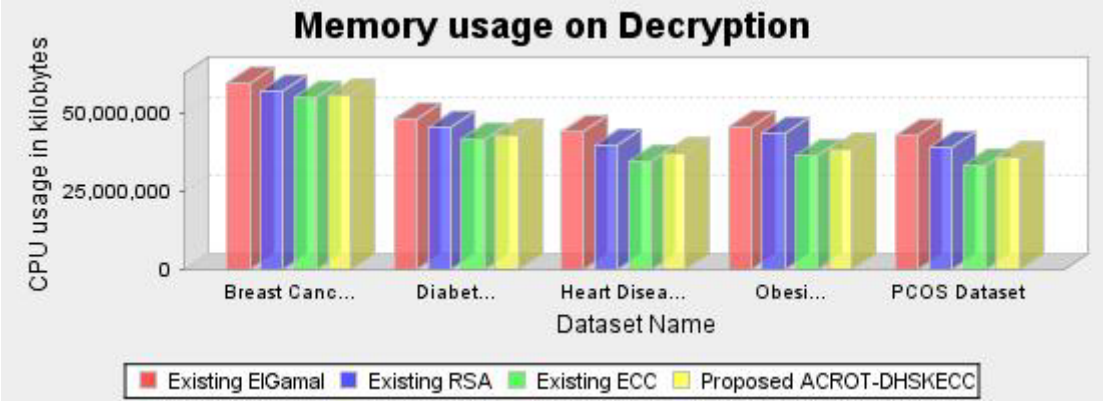


Figure 4(b). Memory usage on decryption analysis

The performance of the proposed ACROT-DHSKECC method across various datasets regarding memory usage on encryption and decryption is depicted in Figure 4(a) and Figure

http://doi.org/10.18080/jtde.v13n3.1301

4(b). The proposed ACROT-DHSKECC demonstrated a memory usage of 55 218 756 kb during encryption and 55 874 458 kb during decryption, which were higher than the existing ECC for the breast cancer dataset. Additionally, for all other datasets, the existing ECC demonstrated low memory usage on encryption along with decryption, when compared to the proposed approach. However, the proposed ACROT-DHSKECC attained less memory usage on encryption and decryption when analogised to RSA and ElGamal. Thus, the proposed model effectively secures DT within IoT networks while optimising memory usage.

While the proposed ACROT-DHSKECC method demonstrates higher memory usage compared to the baseline ECC — particularly around 55 MB for the breast cancer dataset during encryption and decryption — this overhead stems from the integration of double encryption and Diffie-Hellman-based key generation. These added layers of security significantly strengthen confidentiality and key management, which are critical in healthcare applications. Although the memory consumption is greater than ECC, it remains lower than RSA and ElGamal methods. Therefore, the memory–security trade-off is justifiable. For future improvements, memory-efficient cryptographic refinements or lightweight key exchange protocols may be explored to reduce this overhead further without sacrificing security.

Performance analysis of proposed LSCRC32

The performance of the proposed LSCRC32 as well as the existing CRC32, Secure Hashing Algorithm512 (SHA512), and Message-Digest5 algorithm (MD5) is analysed and compared here.

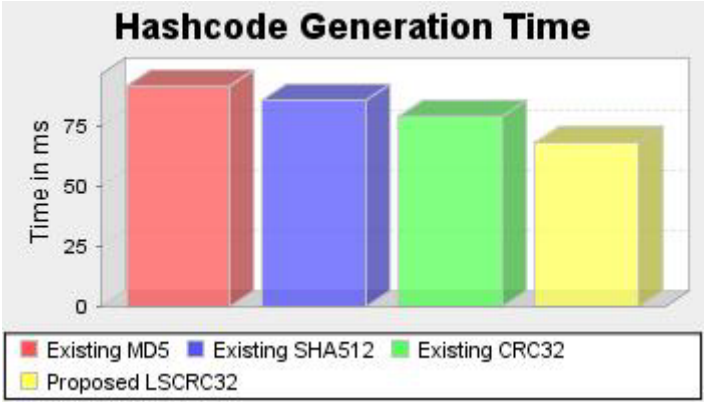


Figure 5. Hashcode generation time analysis

The analysis of the hashcode generation time of the proposed LSCRC32 and the existing approaches is depicted in Figure 5. Here, the proposed LSCRC32 took a lesser hashcode generation time of 68 ms than the existing CRC32. Also, the other existing models like MD5 and SHA512 took more time to generate the hashcode than the LSCRC32. The enhanced performance of LSCRC32 is because of processing 16 bits instead of 8 bits at a time, thereby effectively reducing the time. Thus, for hashed access policy creation, the proposed model efficiently generates the hash code.

http://doi.org/10.18080/jtde.v13n3.1301

Comprehensive analysis

Here, the proposed research's performance is assessed with conventional works.

The comparative analysis of the proposed model with the related works is depicted in Table 2. In the existing works, for an energy-efficient secure IoT HC DT process, methods like ECC-based energy-efficient routing protocol, BC-based fog consensus protocol, BC-assisted secure data management framework, Probabilistic super learning with random hashing, and ElGamal Blind Signature techniques are developed. The existing methods had 41% improvement, 300 ms, 21 s, and 0.27 s of execution time, while, for the two reported, the existing methods had 100 ms and 52% improvement of response time in the health DT process. By contrast, the proposed model had only 70 ms of response time and 250 ms of execution time. As a result of creating double encryption and a hashed access policy, the proposed model's dynamic performance was achieved by using ACROT-DHSKECC and LSCRC32. Hence, the proposed model's superiority is proved by the analysis.

Table 2. Comparative analysis of the proposed research and the traditional works

Authors	Methods	Objective	Response Time	Execution Time
Proposed	ACROT-DHSKECC and LSCRC32	Secure IoT DT	70 ms	250 ms
Natarajan, Lokesh, Flammini, & Premkumar (2023)	ECC-based energy-efficient routing protocol	Security and energy enhancement in HC 5.0	-	41% improvement over baseline
Almaiah *et al.* (2022)	BC-based fog consensus protocol	Data preservation in digital HC	100 ms	300 ms
Abbas *et al.* (2021)	BC-assisted secure data management framework	Secured data management for health information analysis	52% improvement over baseline	-
Khadidos *et al.* (2022)	Probabilistic super learning with random hashing	HC data security	-	21 s
Sun, Liu, & Yu (2021)	ElGamal Blind Signature	Privacy-preserving for intelligent diagnosis in IoT HC	-	0.27 s

Note: Percentages indicate reported performance improvement relative to baseline methods in respective studies. All absolute time values are expressed in SI units (milliseconds or seconds).

Telecommunications and Digital Economy relevance

The proposed model directly supports the digital transformation of healthcare services by enhancing secure data flow over telecom infrastructures. Specifically, the use of lightweight encryption (ACROT-DHSKECC) and adaptive hashed access control (LSCRC32) minimises

http://doi.org/10.18080/jtde.v13n3.1301

bandwidth and energy consumption, making the framework suitable for deployment over 5G, LPWAN, and mobile edge computing (MEC) networks.

From a telecommunications perspective, the integration of clustering and optimised path routing ensures balanced traffic distribution and extended network lifetimes, which are critical in wireless sensor networks (WSNs) deployed in remote health monitoring systems. Moreover, this system reduces transmission latency and improves throughput by avoiding centralised computation bottlenecks, aligning with key performance indicators (KPIs) for telecom-grade healthcare platforms.

In the context of the digital economy, this model empowers healthcare providers to deliver high-quality, secure telehealth services, even in bandwidth-constrained rural areas. It promotes equitable access to healthcare services by ensuring secure and low-latency communication between patients and doctors, contributing to the sustainability of eHealth ecosystems.

Functional requirement-based comparison

While traditional performance metrics such as execution time and memory usage are vital, the real-world applicability of cryptographic systems — especially in healthcare IoT — must also be judged on functional criteria, such as confidentiality, access control, scalability, and adaptability to network constraints. To this end, we present a qualitative comparison of our proposed ACROT-DHSKECC framework against widely used cryptographic techniques, including ECC, RSA, and ElGamal. Table 3 compares the proposed ACROT-DHSKECC framework with conventional cryptographic methods (ECC, RSA, ElGamal) based on critical functional requirements for IoT healthcare. The proposed model excels in security, efficiency, and adaptability for 5G-enabled, resource-constrained environments.

Table 3. Functional Requirement-Based Comparison of Cryptographic Techniques

Requirement	**ECC**	**RSA**	**ElGamal**	**Proposed ACROT-DHSKECC**
Data confidentiality	Supported	Supported	Supported	Strongly supported (via dual-layer encryption)
Role-based access control (RBAC)	Not supported	Not supported	Not supported	Fully supported (through hashed LSCRC32 access policy)
Hashed access policy with low complexity	Not supported	Not supported	Not supported	Fully supported (with improved LSCRC32 2-byte processing)

http://doi.org/10.18080/jtde.v13n3.1301

Requirement	ECC	RSA	ElGamal	Proposed ACROT-DHSKECC
Low-latency usability in constrained IoT	Partially supported	Not supported	Partially supported	Fully supported (via energy-aware clustering and optimised routing)
Secure key agreement	Not supported	Not supported	Supported	Fully supported (Elliptic Curve + Diffie–Hellman integration)
Lightweight operation for resource-limited devices	Supported	Not supported	Not supported	Fully supported (designed for edge/fog adaptability)
Compatibility with 5G and edge computing	Partially supported	Not supported	Not supported	Fully supported (modular and network-optimised design)

Figure 6 illustrates the sequential process of ensuring secure patient data transmission in IoT healthcare. It begins with dual-layer encryption, followed by hashed access policy creation and role-based verification, enabling low-latency and secure communication. The approach is optimised for real-time, resource-constrained IoT healthcare environments.

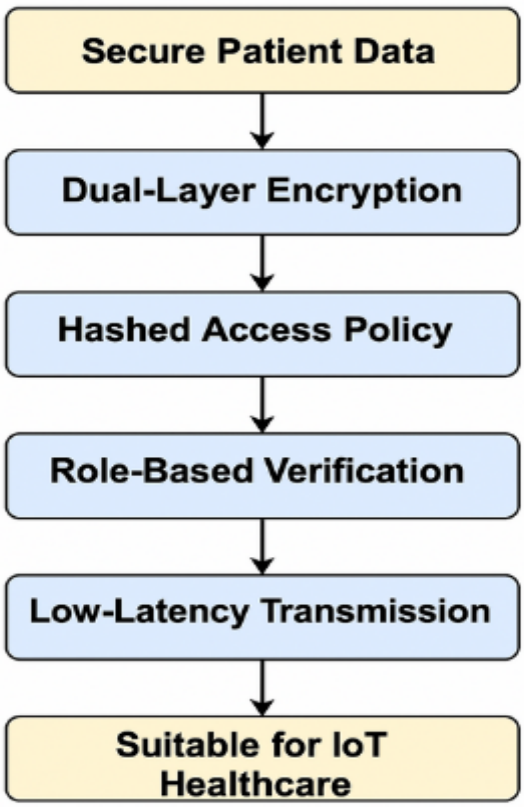


Figure 6. Healthcare IoT security requirements addressed by the proposed method

http://doi.org/10.18080/jtde.v13n3.1301

The proposed ACROT-DHSKECC method goes beyond simply encrypting data. It introduces a dual-layer encryption approach that combines ASCII-based lightweight transformations with ECC secured by a Diffie–Hellman key exchange. This ensures stronger confidentiality and secure key negotiation between parties. Moreover, our use of the LSCRC32 hashing method facilitates a role-based, hashed access policy that operates with minimal computational overhead. This access control layer is absent in conventional ECC or RSA implementations. Importantly, the proposed system integrates energy-efficient clustering (K-Means) and optimal path selection (GOA) to reduce transmission latency and extend the lifetime of IoT nodes — capabilities critical for real-world deployment in 5G, fog-based, or rural healthcare infrastructures. Therefore, even though ECC may outperform in isolated speed benchmarks, ACROT-DHSKECC offers a more comprehensive and functional solution tailored for secure, scalable, and responsive healthcare IoT ecosystems.

Conclusion

This study proposed a secure and energy-efficient IoT-based data transmission framework tailored for healthcare applications, integrating a dual-layer encryption mechanism (ACROT-DHSKECC) and a hashed access policy using LSCRC32. The framework enhances data confidentiality and integrity during transmission across decentralised healthcare networks. Patient data is encrypted and transmitted through an optimised path derived via clustering and the Grasshopper Optimisation Algorithm, significantly reducing energy consumption at the network level.

Experimental results demonstrated the efficiency of the proposed system, with encryption and decryption times of 142 ms and 124 ms, respectively, for the breast cancer dataset, and a hashcode generation time of 68 ms using LSCRC32. These results confirm the model's suitability for secure data transfer in resource-constrained, IoT-enabled healthcare environments, particularly those operating over 5G or mobile cloud infrastructures.

Future recommendations

While the current model effectively clusters nodes and optimises data routing for energy savings, it does not incorporate trust evaluation of participating nodes. This limitation could expose the network to internal threats, such as malicious or compromised nodes. Future research will focus on integrating trust-aware routing and anomaly detection mechanisms to further strengthen the resilience and reliability of the proposed framework in real-world healthcare IoT deployments.

http://doi.org/10.18080/jtde.v13n3.1301

References

Abbas, A., Alroobaea, R., Krichen, M., Rubaiee, S., Vimal, S., & Almansour, F. M. (2021). Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things. *Personal and Ubiquitous Computing, 28*(1), 1–15. https://doi.org/10.1007/s00779-021-01583-8

Adere, E. M. (2022). Blockchain in healthcare and IoT: A systematic literature review. *Array, 14*, 100139. https://doi.org/10.1016/j.array.2022.100139

Almaiah, M. A., Hajjej, F., Ali, A., Pasha, M. F., & Almomani, O. (2022). A novel hybrid trustworthy decentralized authentication and data preservation model for digital healthcare IoT based CPS. *Sensors, 22*, 1–25. https://doi.org/10.3390/s22010125

Alshamrani, M. (2022). IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. *Journal of King Saud University - Computer and Information Sciences, 34*(8), 4687–4701. https://doi.org/10.1016/j.jksuci.2021.06.005

Bhuiyan, M. N., Rahman, M. M., Billah M. M., & Saha, S. (2021). Internet of Things (IoT): A Review of Its Enabling Technologies in Healthcare Applications, Standards Protocols, Security, and Market Opportunities. *IEEE Internet of Things Journal, 8*(13), 10474–10498. https://doi.org/10.1109/JIOT.2021.3062630

Breast Cancer Wisconsin (Diagnostic) Data Set. (n.d.). UCI Machine Learning Repository. https://archive.ics.uci.edu/ml/datasets/Breast+Cancer+Wisconsin+(Diagnostic)

Chauhan, R., Kaur, H., & Chang, V. (2020). An optimized integrated framework of big data analytics managing security and privacy in healthcare data. *Wireless Personal Communications, 117*, 87–108. https://doi.org/10.1007/s11277-020-07040-8

Chinaei, M. H., Gharakheili, H. H., & Sivaraman, V. (2021). Optimal witnessing of healthcare IoT data using blockchain logging contract. *IEEE Internet of Things Journal, 8*(12), 1–14. https://doi.org/10.1109/JIOT.2021.3051433

Comput, J. P. D., Nhu, G., Ho, N., Viet, L., Elhoseny, M., Shankar, K., Gupta, B. B., & El-latif, A. A. A. (2021). Secure blockchain-enabled cyber–physical systems in healthcare using deep belief network with ResNet model. *Journal of Parallel and Distributed Computing, 153*, 150–160. https://doi.org/10.1016/j.jpdc.2021.03.011

Deepalakshmi, P. C. P. (2021). HCAC EHR: Hybrid cryptographic access control for secure EHR retrieval in healthcare cloud. *Journal of Ambient Intelligence and Humanized Computing, 13*(2), 1–19. https://doi.org/10.1007/s12652-021-02942-2

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Dwivedi, R., Mehrotra, D., & Chandra, S. (2022). Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *Journal of Oral Biology and Craniofacial Research, 12*(2), 302–318. https://doi.org/10.1016/j.jobcr.2021.11.010

Ghazal, T. M., Hasan, M. K., Alshurideh, M. T., Alzoubi, H. M., Ahmad, M., Akbar, S. S., Kurdi, B. A., & Akour, I. A. (2021). IoT for smart cities: Machine learning approaches in smart

healthcare – A review. *Future Internet, 13*(8), 1–19. https://doi.org/10.3390/fi13080191

Ghazal, T. M., Saeed, R. A., Hasan, M. K., Pandey, B., Gohel, H., & Eshmawi, A. A. (2022). A review on security threats, vulnerabilities, and countermeasures of 5G-enabled Internet-of-Medical-Things. *IET Communications, 16*(5), 421–432. https://doi.org/10.1049/cmu2.12301

Haghi, M., Madanipour, M., Nikravan, M., Asghari, P., & Mahdipour, E. (2021). A systematic review of IoT in healthcare: Applications, techniques, and trends. *Journal of Network and Computer Applications, 192*, 103164. https://doi.org/10.1016/j.jnca.2021.103164

Heart Disease Dataset. (n.d.). UCI Machine Learning Repository. https://archive.ics.uci.edu/ml/datasets/Heart+Disease

Humayun, M., & Jhanjhi, N. Z. (2021). Secure healthcare data aggregation and transmission in IoT: A survey. *IEEE Access, 9*, 16849–16865. https://doi.org/10.1109/ACCESS.2021.3052850

Javaid, M., & Haleem, I. (2021). Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 pandemic. *Journal of Oral Biology and Craniofacial Research, 11*(2), 209–214. https://doi.org/10.1016/j.jobcr.2021.01.015

Kadiyala, B., & Kaur, H. (2021). Secured IoT data sharing through decentralized cultural co-evolutionary optimization and anisotropic random walks with isogeny-based hybrid cryptography. *Journal of Science and Technology, 6*(6), 231–245. https://doi.org/10.46243/jst.2021.v06.i06.pp231-245

Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. *IEEE Internet Computing, 25*(4), 37–48. https://doi.org/10.1109/MIC.2021.3051675

Kathamuthu, N. D., Chinnamuthu, A., Iruthayanathan, N., Ramachandran, M., & Gandomi, A. H. (2022). Deep Q-learning-based neural network with privacy preservation method for secure data transmission in IoT healthcare application. *Electronics, 11*, 1–14. https://doi.org/10.3390/electronics11050745

Khadidos, A. O., Shitharth, S., Khadidos, A. O., Sangeetha, K., & Alyoubi, K. H. (2022). Healthcare data security using IoT sensors based on random hashing mechanism. *Journal of Sensors, 2022*, 1–17. https://doi.org/10.1155/2022/8457116

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203–209. https://doi.org/10.2307/2007884

Kondaka, L. S., Thenmozhi, M., Vijayakumar, K., & Kohli, R. (2021). An intensive healthcare monitoring paradigm by using IoT-based machine learning strategies. *Multimedia Tools and Applications, 81*(26), 1–15. https://doi.org/10.1007/s11042-021-11439-7

Kumar, P., Kumar, R., Gupta, G. P., Tripathi, R., Jolfaei, A., & Islam, A. K. M. N. (2023). A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system. *Journal of Parallel and Distributed Computing, 172*, 69–83. https://doi.org/10.1016/j.jpdc.2022.10.002

Li, H., Yu, K., Liu, B., Feng, C., Qin, Z., Srivastava, G., & Member, S. (2021). An efficient ciphertext-policy weighted attribute-based encryption for the Internet of Things. *IEEE*

Journal of Biomedical and Health Informatics, 26(5), 1–12. https://doi.org/10.1109/JBHI.2021.3075995

Masud, M., Gaba, G. S., & Choudhary, K. (2021). Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. *IEEE Internet of Things Journal, 9*(4), 1–8. https://doi.org/10.1109/JIOT.2021.3080461

Miller, V. S. (1985). Use of elliptic curves in cryptography. In A. M. Odlyzko (Ed.), *Advances in Cryptology – CRYPTO '85 Proceedings* (pp. 417–426). Springer. https://doi.org/10.1007/3-540-39799-X_31

Natarajan, D. R., Peddi, S., Valivarthi, D. T., Narla, S., Kethu, S. S., & Kurniadi, D. (2024). Secure user authentication and data sharing for mobile cloud computing using BLAKE2 and Diffie-Hellman key exchange. In *2024 International Conference on Emerging Research in Computational Science (ICERCS)* (pp. 1–8). IEEE. https://doi.org/10.1109/ICERCS63125.2024.10895363

Natarajan, R., Lokesh, G. H., Flammini, F., & Premkumar, A. (2023). A novel framework on security and energy enhancement based on Internet of Medical Things for healthcare 5.0. *Infrastructures, 8*, 1–18. https://doi.org/10.3390/infrastructures8010018

Obesity Levels Dataset. (n.d.). Kaggle. https://www.kaggle.com/datasets/mansoordaku/obesity-levels

Oliveira, M. T. de, Verginadis, Y., Reis, L. H. A., Psarra, E., Patiniotakis, I., & Olabarriaga, S. D. (2023). AC-ABAC: Attribute-based access control for electronic medical records during acute care. *Expert Systems With Applications, 213*, 119271. https://doi.org/10.1016/j.eswa.2022.119271

PCOS Dataset. (n.d.). Kaggle. https://www.kaggle.com/datasets/jainilcoder/pcos-dataset

Peterson, W. W., & Brown, D. T. (1961). Cyclic codes for error detection. *Proceedings of the IRE, 49*(1), 228–235. https://doi.org/10.1109/JRPROC.1961.287814

Pima Indians Diabetes Database. (n.d.). UCI Machine Learning Repository. https://archive.ics.uci.edu/ml/datasets/diabetes

Pradhan, B., Bhattacharyya, S., & Pal, K. (2021). IoT-based applications in healthcare devices. *Journal of Healthcare Engineering, 2021*, 1–18. https://doi.org/10.1155/2021/6632599

Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and Internet of Things in healthcare and medical sector: Applications, challenges, and future perspectives. *Journal of Food Quality, 2021*, 1–20. https://doi.org/10.1155/2021/7608296

Refaee, E., Parveen, S., Mohamed, K., Begum, J., Parveen, F., Raja, M. C., Gupta, S. K., & Krishnan, S. (2022). Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications. *Journal of Food Quality, 2022*, 1–12. https://doi.org/10.1155/2022/5665408

Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., Alghamdi, S., Alhasawi, Y., & Iranmanesh, M. (2023). The Internet of Things (IoT) in healthcare: Taking stock and moving forward. *Internet of Things, 22*, 100721. https://doi.org/10.1016/j.iot.2023.100721

Srinivasan, K., Chauhan, G. S., Jadon, R., Budda, R., Gollapalli, V. S. T., & Prema, R. (2025). Secure and privacy-preserving cloud computing through MLP-LSTM based enhanced homomorphic encryption technique. *International Journal of Humanities Social Science and Management (IJHSSM), 5*(2), 285–290. https://www.ijhssm.org

Sun, Y., Liu, J., & Yu, K. (2021). PMRSS: Privacy-preserving medical record searching scheme for intelligent diagnosis in IoT. *IEEE Transactions on Industrial Informatics, 18*(3), 1–10. https://doi.org/10.1109/TII.2021.3070544

Ullah, F., Khan, M. Z., Faisal, M., Rehman, U., Abbas, S., Mubarek, F. S. (2021). An Energy Efficient and Reliable Routing Scheme to enhance the stability period in Wireless Body Area Networks. *Computer Communications, 165*, 20–32. https://doi.org/10.1016/j.comcom.2020.10.017

Valivarthi, D. T., & Kurniadi, D. (2024). A hybrid consensus method for energy-efficient and secure IoT data sharing in fog computing, integrating delegated proof of stake and whale optimization techniques. *Journal of IoT in Social, Mobile, Analytics, and Cloud, 6*(4), 308–326. https://doi.org/10.36548/jismac.2024.4.002

Valivarthi, D. T., Peddi, S., Narla, S., Kethu, S. S., & Natarajan, D. R. (2023). Fog computing-based optimized and secured IoT data sharing using CMA-ES and firefly algorithm with DAG protocols and federated Byzantine agreement. *International Journal of Engineering & Science Research, 13*(1), 117–132. https://www.ijesr.org

History of Telecommunications

Biography

Automation of Directory Assistance

Simon Moorhead
Telecommunications Manager

Abstract: The *Journal* revisits two historic papers from 1981 and 1982 that describe a successful trial in Sydney of a computer-based system to automate the Directory Assistance paper records in Australia. The trial led to the implementation of a national Directory Assistance system that provided productivity improvements but fell short of the performance achieved by similar systems in the USA.

Keywords: History of Australian Telecommunications, Automation, Directory Assistance, *Telecommunication Journal of Australia*.

Introduction

The reprinting of these historic papers (Dougall, 1981; Baxter & Lyon, 1982) was influenced by recent discussions regarding artificial intelligence (AI) and the potential disruption to employment practices and skill sets. It is widely assumed that clerical and administrative roles are the most exposed to AI modernisation.

Back in the early 1980s, Telecom Australia (now part of Telstra) undertook a trial of a directory assistance system (DAS) from Computer Consoles Incorporated (CCI) supplied by STC; this is the subject of the first paper (Dougall, 1981). At that time, Telecom was utilising a 50-year-old manual retrieval system which needed to be modernised to handle greater volumes and achieve better response times. CCI was based in the United States and the system had been in operation in US telephone companies since early 1977.

The objective of the trial (Dougall, 1981)was to enable the study of the application of computer directory assistance systems in Telecom and, specifically:

- to assist in the planning and implementation of a national computer DAS network;
- to assist in the preparation of a specification and tender schedule for a national computer DAS network; and

https://doi.org/10.18080/jtde.v13n3.1330

- to form a basis for negotiations with staff associations on the national introduction of computer systems in the Directory Assistance Service.

The trial was a success and demonstrated the operational viability of computer-based DAS systems. Significant productivity gains were expected (given the trial achieved 40% gains), as well as improvement in customer service through faster response and improvement in the quality and time to update information. A curious observation was that customers had greater acceptance of a directory result or a "non-listing" if they knew a computer system was being used.

What the paper does not mention is the future performance of the directory assistance service looked bleak and automation was critical (Campbell, 2017). The 22 million calls to the service in 1976 had increased to 78 million in 1981. Operating costs were $4.3 million in 1971, $17.7 million in 1976, and $38 million in 1981, and were projected to reach $63 million in 1985. Further information on the background of the Directory Assistance Service can be found in Campbell (2025), which is also in this issue.

Following the successful trial, a contract for a full DAS system was awarded to IBM Australia. This is the subject of the second paper (Baxter & Lyon, 1982).

The national system selected by Telecom was a standard IBM DAS packaged system incorporating standard hardware, system and application software. However. development of a substantial software package was carried out by Telecom to enable the conversion of the data, from the existing white pages directory compilation systems.

The system was divided into two distinct networks, namely the Data Base Update Network and the Retrieval Network. The Master Update Centre was located in Clayton (Victoria) at the Telecom Data Processing Centre and was the heart of the IBM DAS/C system. The Retrieval Centre and Manual Assistance Centre were located in each mainland capital city (with Tasmania sharing Victoria's).

The master data base and the inquiry data base were divided or "partitioned" into 53 separate "books" or "files". The partitions reflected the configuration of the State-based published directories at the time.

A significant amount of data manipulation and correction was required to automate the residential, business and Government white pages data. Once corrected, these databases were updated on a daily basis and distributed on tape by couriers to the Retrieval Centres.

In implementing the DAS system, Telecom moved from the traditional manual system, which was over 50 years old, to a computer-based system to help satisfy the ever-increasing demand for Directory Assistance.

http://doi.org/10.18080/jtde.v13n3.1330

In 1988 (Campbell, 2017; 2025), Booz Allen & Hamilton conducted a benchmarking study comparing the performance of Telecom's DAS/C directory assistance service with similar services operating in four of the Regional Bell Operating Companies (RBOCs) in the USA. Telecom delivered a clearly inferior service at a significantly higher cost, with the RBOCs reporting minimal incidences of Repetitive Strain Injury. The poorer performance in Telecom was attributed to the high labour intensity of the service, monopoly wages and conditions, union obstruction to productivity improvements, and union demands that operator numbers be increased to handle the ever-growing calls (rather than improve productivity) (Campbell, 2017). For further details on what Telecom could have done, see Campbell (2025).

This behaviour was in direct contrast to the "enthusiastic contribution of operating staff" at the start of the trial. Are we about to see similar impediments with the introduction of AI?

References

Baxter, I., & Lyon, H. (1982). The National Computerised Directory Assistance Service — DAS/C. *Telecommunication Journal of Australia, 32*(2), 95–100.

Campbell, I. (2017). Fact or Fraud? the epidemic which struck Telecom Australia from 1983 to 1986. *Journal of Telecommunications and the Digital Economy, 5*(2), 75–97. https://doi.org/10.18080/jtde.v5n2.107

Campbell, I. (2025). Comments on the Two Historical Reprints in Automation of Directory Assistance. *Journal of Telecommunications and the Digital Economy*, *13*(3), 191–195. https://doi.org/10.18080/jtde.v13n3.1340

Dougall, C. J. (1981). Trial of a Computer Directory Assistance System — Sydney. *Telecommunication Journal of Australia, 31*(1), 79–84.

The Historic Papers

Dougall (1981)

Trial of a Computer Directory Assistance System — Sydney

CHARLES J. DOUGALL, B. Com., ARMIT, MIE (Aust)

A trial was conducted in Sydney in 1979 of a computer information retrieval system which replaced paper records at directory assistance positions with visual display units. This paper describes the background to the trial and presents results which demonstrate the operational viability of computer directory assistance systems in Telecom Australia's Directory Assistance Service.

A trial in Telecom Australia's Directory Assistance Service (DAS) of computer directory information retrieval was conducted at the Sydney 013 Centre (GPO) over a period of 6 months from 7 February to 7 August 1979. In the trial, directory paper records on ten operator positions and one supervisor position were replaced by Visual Display Units (VDUs) which the operator used to access an information retrieval computer system located at East Sydney Telephone exchange.

The information retrieval system used as the vehicle for the trial was the Computer Consoles Incorporated (CCI) DAS/C system supplied through STC Australia Pty. Ltd. CCI are based in the United States and the DAS/C system has been in operation in US telephone companies since early 1977.

The implementation of the trial and data collection for trial evaluation purposes were conducted by Telecom's NSW Administration with overall project management being conducted by the Headquarters DAS Project Team. CCI and STC installed and maintained the DAS/C system. The network configuration established for the trial is shown in **Fig 1.**

TRIAL OBJECTIVES

The trial was not intended to prove the technical functioning of the CCI system as the system was acquired as a standard hardware/software package which was well proven in operation in the United States.

The objective of the trial was to enable the study of the application of computer DAS systems in Telecom Australia and specifically

- to assist in the planning and implementation of a national computer DAS network
- to assist in the preparation of a specification and tender schedule for a national computer DAS network and
- to form a basis for negotiations with staff associations on the national introduction of computer systems in the Directory Assistance Service.

OPERATING PERFORMANCE

The trial showed that computer information retrieval is an operationally viable alternative to the paper records system currently used in the Directory Assistance Service. Operator productivity gains in excess of 40% were achieved during the trial. The ten DAS/C positions were divided into two groups of five positions. One group, designated the "Control Group" comprised 12 operators who occupied five positions over all shifts for the full six month trial period; these operators only operated DAS/C positions and did not work on paper records positions. Furthermore, these 12 operators were selected to be representative of the cross-section of operating ability in the Sydney DAS centre. This was done to enable meaningful extrapolation of control group performance results to apply to the entire centre and other centres in Australia. The remaining five positions were occupied by the remaining operators in the Sydney DAS Centre on a rostered basis of 3 days training and two days of answering live traffic. In addition these remaining operators occupied available vacant DAS/C positions at any other time outside of the rostered sessions. This enabled all operators in the Sydney DAS/C Centre to have some experience in the operation of DAS/C.

Improvement in operator productivity was measured through improvement in Average Work Time (AWT) which is defined as the average, for all calls answered by the operator, of the time interval between the connect and disconnect of customers' calls. It therefore measures the average time that operators spend on customers' enquiries, including conversation and information retrieval time. An interface between the CCI system and the GPO call queue system was established to enable the compilation of this statistic on the CCI system.

Graphs of AWTs over the six month trial period for DAS/C and paper records positions are shown in **Fig 2.**

http://doi.org/10.18080/jtde.v13n3.1330

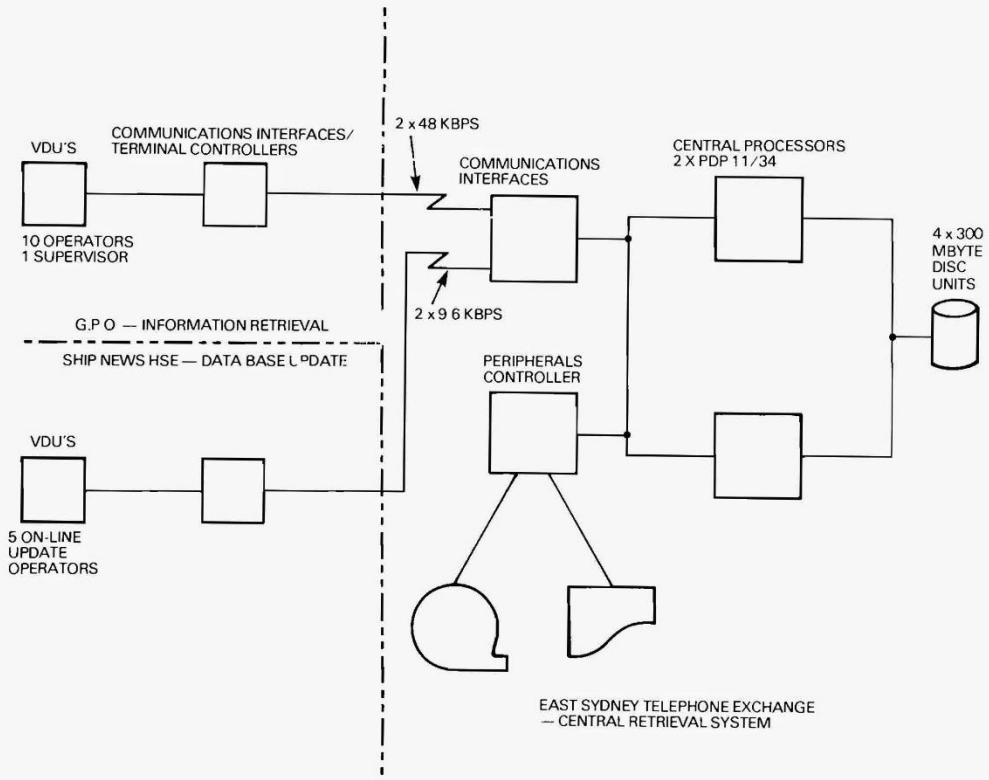


Fig. 1 — Network Configuration

CHARLES J. DOUGALL joined the APO in 1968 as a cadet engineer. In 1970 he was appointed engineer in the Victorian Planning Branch, and was transferred to Victorian Construction Branch in 1972 where he worked on installation of metropolitan exchanges including the first public ARE 11 installation at Elsternwick.

In 1976 he was appointed Senior Engineer in the Planning Division Headquarters and in 1978 was promoted to his current position in Telephone Switching Planning Branch as project manager for the Directory Assistance project.

http://doi.org/10.18080/jtde.v13n3.1330

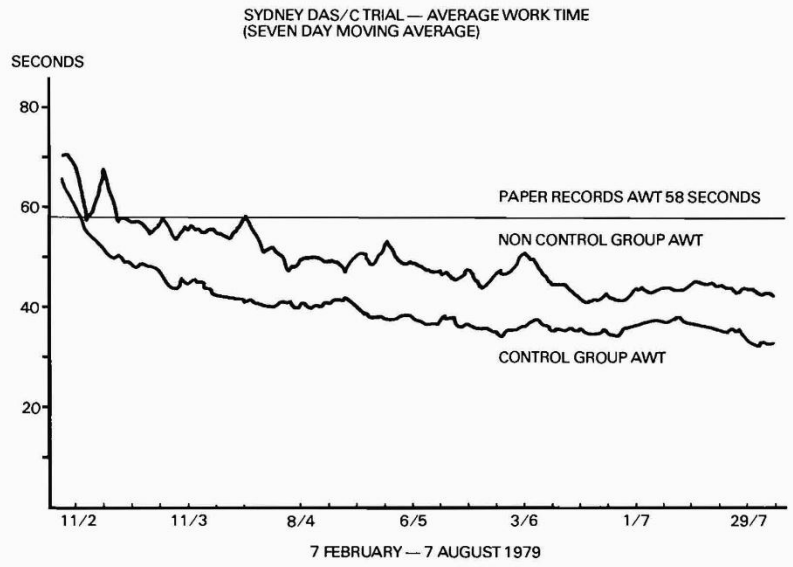


Fig. 2 — Average Work Time — Seven Day Moving Average.

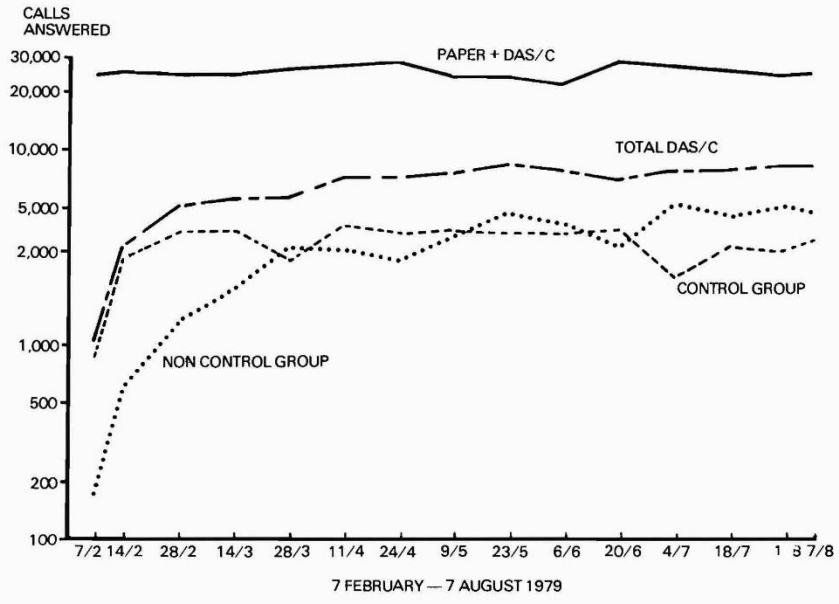


Fig. 3 — Call Volumes

http://doi.org/10.18080/jtde.v13n3.1330

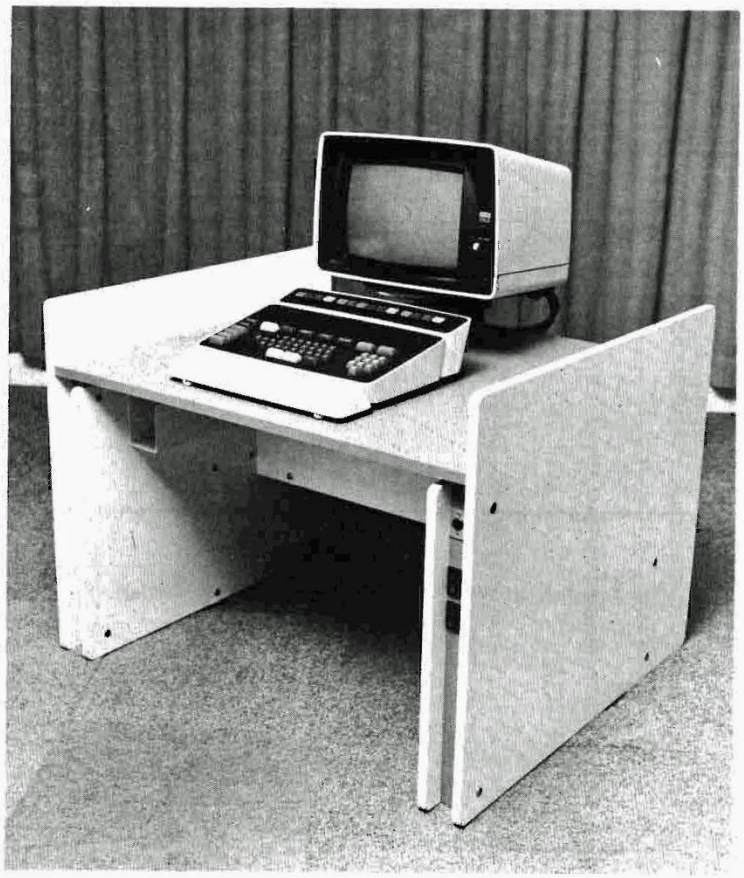


Fig. 4 — Adjustable VDU Workstation

CALL VOLUMES

The call volumes handled by the Sydney DAS centre over the trial period for DAS/C and paper records positions are shown in **Fig 3.** The increasing call volume with time, handled by DAS/C positions, is a reflection of the AWT reduction with time. It should be noted that every opportunity was taken by non-control-group staff to operate DAS/C positions. Thus the occupancy of DAS/C positions was high even at times of relatively low traffic when occupancy of paper-records positions was low. Thus conclusions of the effectiveness of DAS/C positions versus paper-records positions based on a straight comparison of paper-records calls and DAS/C calls could be misleading. The AWT comparison should be used to compare call processing effectiveness of DAS/C and paper-records positions.

NUMBER RETRIEVAL SUCCESS RATE

There was little difference between DAS/C and paper-records in the success rate of numbers found.

However, operators were able to more confidently convey to customers that a listing did not exist to match the information supplied when using DAS/C positions as opposed to paper-records positions. Furthermore, customers, knowing that a computer system was being used by the operator, were more willing to accept a no listing result than they were with operators using paper records.

An analysis of outcomes of calls handled by DAS/C positions appears in Table 1.

Table 1 : Analysis of Outcomes of Calls Handled

Outcome	% of Calls Handled
Listing Found	76
No Listing — Full Info. by caller	9
— Insufficient Info. by caller	5
Call Redirected to 0175, 0170	4
Call Redirected to other levels	3
Call Drop-Outs	3

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 13 Number 3

http://doi.org/10.18080/jtde.v13n3.1330

OPERATIONAL REVIEW OF DAS/C SYSTEM

The CCI DAS/C system is designed with internal redundancy to provide a high level of up-time performance and a fast enquiry response time at the operator's terminal.

Total service loss due to equipment failure was not experienced during the trial although some equipment failure did occur which caused service degradation, i.e. increased system response time. The extent of partial service loss was interpreted to have resulted in an overall equipment percentage up-time over the trial of 99.87%. System response time, measured as the interval between depression of the last key by the operator and appearance of the last character on the terminal screen, averaged at about 0.9 seconds.

STAFF INVOLVEMENT

Operator staff and their staff association (ATPOA) were involved in the project a long time prior to the contract being let for the trial. An agreement was negotiated in early 1978 with ATPOA on the operation of the trial and in August 1978 seminars on the trial were held for all directory assistance operators in Sydney.

A staff consultative group was formed in September 1978 to consult on matters relating to the introduction and evaluation of the trial. This group held fortnightly meetings prior to and during the trial and provided valuable input to management in the preparation and evaluation of the trial. The meetings were a necessary aid to project development and a useful forum for testing of new ideas and obtaining feedback on problems at the work face, operator attitudes and system performance.

ERGONOMIC AND ACCOMMODATION ASPECTS

In the course of the trial, detailed studies were conducted into the design of workstations and lighting for visual display units (VDUs) with the aid of consultants from the Department of Productivity and Sydney University.

The workstation studies led to the development of an adjustable workstation **(Fig 4)** which enables adjustment by the operator of

- VDU screen angle
- VDU viewing distance
- VDU screen height
- Keyboard height and position independently from VDU screen position.

The workstation will undergo a further operational trial at the Sydney GPO prior to a decision on application in the future national computer DAS network.

An economical and effective lighting scheme was developed in the trial to overcome problems of screen reflections and high ambient light levels. The existing surface-mounted fluorescent fittings were modified to provide controlled lighting suitable for the task. A surround was installed over the fitting with a diffuser which emitted light at a cut off angle such that glare effects in the line of vision of the operator were reduced and reflections from the VDU screens minimised. The resulting lower level of illumination of the ceiling and work area was overcome by the use of floor mounted upright fittings which increased the ceiling illumination. These fittings are shown in **Fig 5.**

The principles of this lighting scheme do not require high ceilings and can be readily and economically applied in most buildings.

Fig. 5 — Lighting Scheme.

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 13 Number 3 September 2025

http://doi.org/10.18080/jtde.v13n3.1330

DATA BASE PREPARATION AND UPDATE

The data base was prepared mainly through automatic conversion from two computer directory compilation master files — one supplied by Telecom Australia's Information Systems Department for the Private Names section of the Sydney White Pages and the other by William Brooks Pty Ltd for the remainder. Programs for the conversion were written by STC who were also responsible for preparation of the data base.

Government entries were input manually and some business listings required manipulation to overcome problems encountered in automatic conversion.

In the early stages of the trial the data base was updated daily entirely by on-line manual methods, using 5 update terminals located at Shipnews House, North Sydney. Towards the end of the trial a batch update system was developed to handle the processing of new and deleted listings in the Telecom produced Private Names file with all other listings being updated manually on-line. STC developed software to read the Telecom produced magnetic tape file and convert the create and delete messages to CCI update compatible formats.

The updating of the data base functioned effectively; however there was a high reliance on direct manual update which is not recommended for future systems as this is costly and inevitably leads to data base errors and non-synchronisation of the data base with the published directory.

THE OUTCOME OF THE TRIAL

The trial was undoubtedly successful in demonstrating the operational viability of computer DAS systems. Significant productivity gains can be expected with a national DAS system as well as improvement in customer service through faster response and improvement in the quality of information. In addition, data base updating facilities will enable reduction in delays in updating directory assistance data thereby also contributing to improvement in customer service.

At the time of writing, installation work was well advanced on the conversion of all "013" paper-records positions at Sydney GPO to the CCI DAS/C system. This expansion of the limited 10 position trial is being undertaken to establish, under full scale operating conditions, organisational arrangements and operating procedures to be applied when the national computer DAS system is installed.

In late January 1981 Telecom Australia obtained Ministerial approval to let a contract with IBM Australia Ltd for a national DAS computer network. This will be installed progressively over the financial years 1981/82 to 1983/84.

Many people within and outside of Telecom Australia contributed to the successful installation and operation of the trial. The contribution made by the operating staff, through their enthusiastic support and participation in the consultative group, was particularly important.

In Brief

REVISED STANDARD FOR METRIC CABLES — AS 3116

The Standards Association of Australia has published a revision of its standard AS 3116 for Elastomer insulated cables.

The new specification revises the 1974 edition and covers elastomer insulated cables and flexible cables for operation at working voltages up to and including 0.6/1kV. It also provides requirements for conductors, insulation, length of lay of course, fillers, binders, tapes, coverings and sheaths, markings, construction and dimensions, and tests.

Principal changes from the earlier standard relate to deletion of R-60 elastomer insulation, and to the size of galvanised steel round armour wire. The deletion has been made because there is now very little demand for this material, and the metric Wiring Rules, AS 3000, no longer provide a rating for this insulation compound.

In the 1974 standard, 0.8mm diameter wire was specified, but this has now been replaced by two sizes 0.9mm and 1.25mm — because it is no longer readily available. The change in armour dimensions has brought the need for a recalculation of the dimensions of finished cables.

Appendices cover calculation of the dimensions of protective coverings and cables, rounding of numbers, colours of manufacturers' identification threads, and information required with enquiry and order.

Copies of AS 3116 may be obtained from any SAA office at a cost of $11.40, plus a charge of $1.50 to cover postage and handling.

For further information please contact:
Jack Moncrieff
Telephone (02) 929 6022

http://doi.org/10.18080/jtde.v13n3.1330

Baxter & Lyon (1982)

The National Computerised Directory Assistance Service — DAS/C

I. BAXTER, H. LYON

National DAS/C consists of a standard IBM data retrieval system, a data base update network which has been designed specifically for Australian conditions and a series of automatic call distributors, which link the retrieval system to the telephone network.

This paper describes, in general terms, the features of the overall system together with some of the operating procedures.

INTRODUCTION

The National DAS/C system selected for use in Telecom Australia is a standard IBM DAS packaged system incorporating standard hardware and, system and application software. However, development of a substancial software package was carried out by Telecom to enable the conversion of the data, from the existing white pages directory compilation systems, for the creation of the DAS data base and for the system which will feed this data base on a daily schedule.

Associated with the overall DAS/C project is the installation of network automatic call distributors (NACDs) in each State. The ACD chosen for this programme is based on the LME ASDP 162. Some adaptation has been necessary to obtain the desired interworking with Telecom services including the DAS/C system.

SYSTEM DESCRIPTION

The system can be divided into two distinct networks with four prime components:

The Data Base Update Network

- Master Update Centre (MUC)
- Data Send Centre (DSC) and Directory Inquiry Centre (DIC)

The Retrieval Network (Fig. 1).

- Retrieval Centre (RC)
- Manual Assistance Centre (MAC)

The DAS/C system functions interactively with DA operators to help provide an improved service, increased operator job satisfaction and reduce operating costs. The DAS/C system has been designed to significantly reduce operator effort and hence work time while promoting consistent, accurate response to customer inquiries. This is achieved by combining the judgement and decision making abilities of the human operator with the computer's ability to rapidly handle and search large volumes of data.

Significant features of the IBM DAS/C are:

- sophisticated file access techniques, uniquely developed for residence, business, and government requests, help provide increased accuracy and speed of search, and significantly reduce the number of "not founds";
- custom designed keyboard/display inquiry terminals allow free-form entry of inquiry arguments and easy request modification, thus increasing operator productivity;
- unique operator keying strategy and specially designated keys for common words and localities, reduces the number of keystrokes required to obtain a requested listing;
- keying strategy is easy to learn and adapts to each individual DA operator's approach, making new operators effective sooner;
- operator and system statistics are collected and produced which allow constant monitoring of the technical performance of the system as well as assisting in DA ongoing training management;
- online national directory files eliminate the costs associated with paper records.

DATA BASE UPDATE NETWORK

Master Update Centre

The MUC located in Clayton (Victoria) Data Processing Centre is the heart of the IBM DAS/C system.

The hardware components constituting the MUC include:

- IBM 4341 processor;
- display console;
- storage control unit;
- direct access storage subsystem;
- tape control unit;
- magnetic tape unit.

The national master data base will be created by using locally developed programmes to convert the white pages directory compilation files. There are four separate compilation systems involved in this conversion and error rejects will be corrected by Directories Branches and re-inserted to provide the final data base of all Australian telephone customers.

Procedures will be developed to facilitate DA operators reporting data base inconsistencies, identified during "live" working of the system.

http://doi.org/10.18080/jtde.v13n3.1330

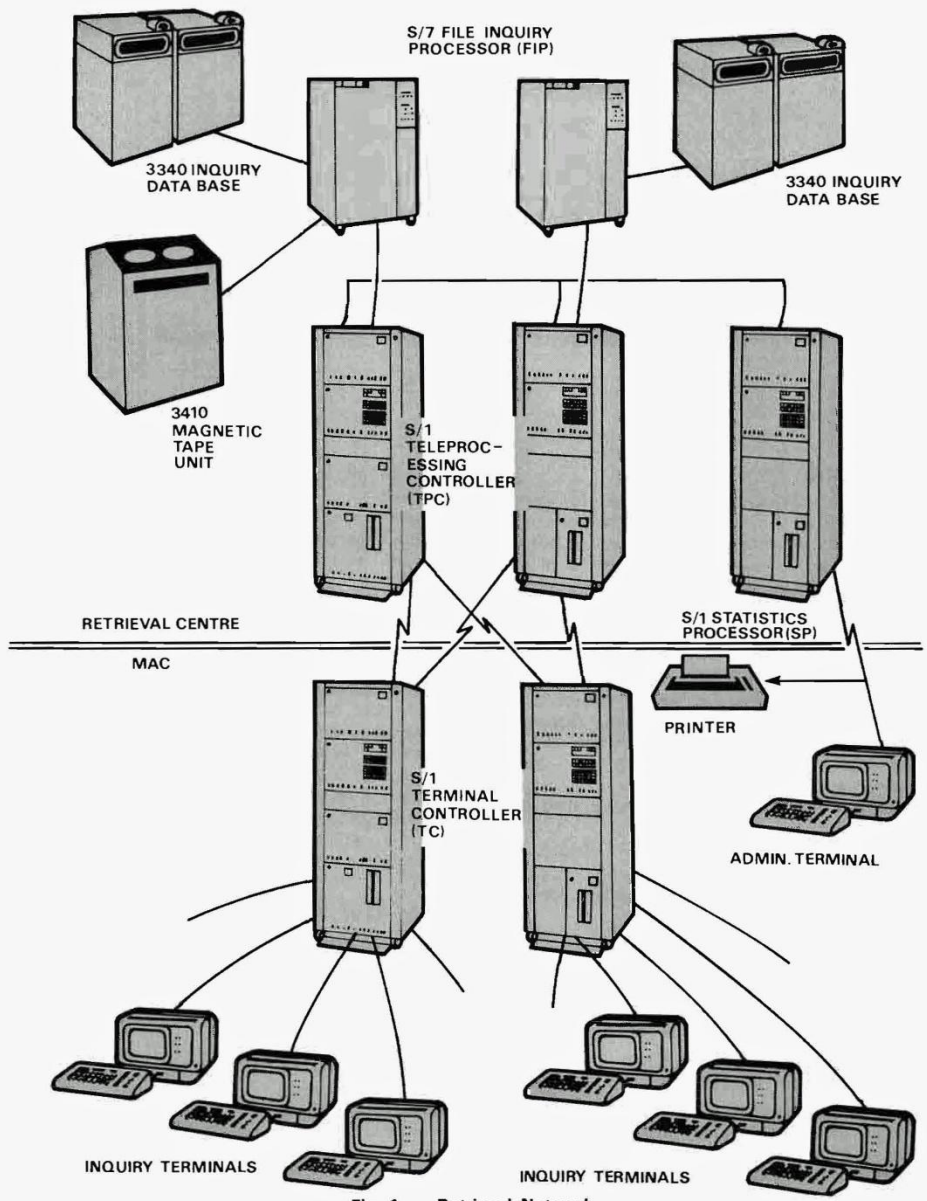


Fig. 1 — Retrieval Network.

When created, the data base will be updated daily from input provided from the DSC. Following completion of the MUC update cycle, tape copies of the new inquiry data base will be generated and conveyed via courier to each RC, daily.

Data Send Centre and Directory Inquiry Centre

DSCs and DICs are to be located in each Directories Branch.

Data Send Centre

The hardware constituting the DSC comprises an IBM Series 1 computer with visual display units. The directory entry information, after editing, is input to the Series 1 via the visual display units which have a formated overlay **(Fig. 2a and 2b).** The data passes through a validation process and is stored. At the end of the day's input (a

http://doi.org/10.18080/jtde.v13n3.1330

scheduled time each day) the data is sorted, formated and transmitted via a data link to the MUC.

At the MUC all data from all Directories Branches will be merged, sorted and interpreted for DAS/C master update. Simultaneously the information required for the various compilation systems will be formated, and output in hard copy.

With the introduction of DSCs in each State, the current telex links with the respective compilation contractors will be replaced. Data input at the DSC will be transmitted to the compilation contractor via the DAS/C MUC. This change in procedures will be almost transparent to the contractors.

Directory Inquiry Centre

The DIC consists of a number of retrieval terminals. The function of these terminals is to interrogate the inquiry data base (resident at the RC) for use in data preparation and error correction. Information, additional to that provided for DAS operators, is provided to permit precise identification of entries by Directories staff. This additional information is the DAS/C number. The prime use of this facility is in the area of complex directory entries.

Administrative Terminal

Within each Directories Branch an administrative terminal will be provided to facilitate file maintenance and error correction. This terminal has access via the statistics processor (SP) to the RC and provides for the following functions additional to normal inquiry:

- hard copy output from the inquiry data base;
- hard copy output of statistical data;
- on-line temporary update of the local inquiry data base.

It should be noted that the administrative terminal and the DIC retrieval terminals have access to the inquiry

Fig. 2a — Data Send Centre Work station.

data base in the RC ***not*** to the master data base in the MUC.

Data Base Partition

The master data base (at the MUC) and the inquiry data base (generated for the RC) are divided or "partitioned" into 53 separate "books" or "files". The partitions reflect the configuration of the current published directories.

The IBM DAS/C system was designed to utilise the locality field as one of the prime search arguments. In order to facilitate this, locality tables and associated pseudo-locality tables are established. The partitioning into 53 separate files enhances the use of this facility.

RETRIEVAL NETWORK

Retrieval Centre

RCs are to be located in each mainland capital city.

Ian Baxter commenced employment with IBM in February 1966 as a Customer Engineer servicing IBM computer equipment.

In June 1968 he moved to IBM Sydney to manage a refurbishing project and subsequently became an instructor teaching computer engineering and programming to customer engineers from the South East Asian region.

During that period, Mr Baxter studied at IBM locations in Europe and the USA acquiring new product education specifically in process control systems.

On return to Melbourne in 1972 he becamne a representative in the Office Products Division and later, the General Systems Division.

When Telecom expressed interest in investigating computerising the Directory Assistance Service in 1978 he was appointed to the team formed by IBM to study Telecom's requirements for the computerised Directory Assistance Service and to formulate a tender submission.

Currently he has the role of Account Manager with the responsibility of co-ordinating the IBM team and working with the Telecom staff in the imlementing of the National DAS/C system.

Howard Lyon joined the Australia Post Office in 1968 as a computer operator and subsequently undertook the Traffic Officer in Training course in 1970-71.

Mr Lyon worked in a number of Telecom District Offices in NSW between 1972 and 1980, in the Customer Service area.

In 1980 Mr Lyon took up duty with Directory Services, Headquarters, as Project Officer where he has worked on the development of computerised directory compilation systems and, more recently, the DAS/C project.

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 13 Number 3 September 2025

http://doi.org/10.18080/jtde.v13n3.1330

Fig. 2b — Data Send Centre Overlay Menu.

Fig. 3 — Retrieval Centre — Windsor, Victoria.

Tasmania is to share, with Victoria, the retrieval centre facilities located in Melbourne **(Fig. 3)**.

The RCs stand apart from, and have no direct links to, the MUC. They store copies of the DAS inquiry data base and are updated by means of a tape copy of each new inquiry data base delivered daily, via courier, from the MUC. The RCs are accessed by the following terminals:

- inquiry terminals located in MACs;
- directory inquiry terminals located in State Directories Branches and used during data preparation and error correction;
- administrative terminals located in MACs to access the statistics processor to produce performance reports and provide for on-line temporary updates;
- administrative terminals located in Directories Branches for on-line temporary updates and hard copy output.

The equipment making up the RCs comprises a System 7 file inquiry processor (FIP) with disc attachment for storage and retrieval of directory information. A Series 1 teleprocessing controller (TPC) links the System 7 FIP with the Series 1 statistics processor and the Series 1 terminal controller (TC) in the MACs via data links. The TPC manages the DA retrieval traffic.

Manual Assistance Centres (Terminal Equipment)

Directory Assistance Centres (DAC) will be installed in all States in accordance with the National MAC Plan (Ref. 1). The DACs will comprise terminal equipment (IBM Visual Display Units) from which DAS operators will be able to access the RC data base to obtain required directory information (Fig. 4).

Located with each group of VDUs will be a Series 1 TC the function of which is to accept, format, edit and concentrate the inquiry request prior to transmission of this request to the RC. This results in a highly effective operator/machine interface.

The actual installation of the DA centres will employ accepted ergonomic principles in the design, layout, environment and lighting of the positions.

FILE INQUIRY PROCESS

File records (or "listings") consist of a finding name, subscriber's title, occupation, business type, street address, area code and phone number, as appropriate. Listings fall into three basic categories, residence (RES), business (BUS) and government (GOV). To assist operators, certain listings will appear in both the RES and BUS files, eg doctors, barristers, etc. This will be under programme control.

Because the DAS search interval (including operator time to key a request on a terminal) must be significantly shorter than that of the current manual method, a custom inquiry terminal is required. The over-riding consideration in the design of this terminal is keying efficiency; the significant details of a request must be entered (and perhaps modified) with the least possible number of keystrokes. As a result, the keyboard functions are specifically designed to facilitate the DAS inquiry operation .

A keyed request may consist of up to four basic elements, but usually, less are required. These may be entered, re-entered, or modified in any order. The elements are finding name (FN), locality (LOC), street name (SN), and type (RES, BUS, GOV), and correspond to fields on the lower portion of the inquiry terminal display. The request is initiated by depressing one of the "type" keys (RES, BUS, GOV).

The finding name is the name under which an individual, business or governmental entity is listed in a telephone directory. The locality indicates the geographic vicinity in which a customer resides or does business. The street name is part of an address in a directory listing.

Alphabetic keys arranged in a standard typewriter (QWERTY) format are used to specify input field contents. The fields themselves are identified by control keys. For example, the FN key moves the cursor to the finding name field for subsequent entry or modification. The same is true for the LOC and SN fields. Other keys can be used to specify a word or phrase within a field with a single keystroke. For example, several "frequently used words" (eg AUST, BANK, STATE), and "frequently referenced locality" keys are provided.

Cursor control keys are used to rapidly access a portion of a field to be modified. A CLEAR key clears a field.

In general, the technique employed by the operator (called "keying strategy") is to key only enough details of a request to result in a manageable number of listings being displayed — perhaps eight to ten. One reason for this is to minimise keystrokes, but another is to avoid over-qualifying a search, since a customer may reject the

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 13 Number 3

http://doi.org/10.18080/jtde.v13n3.1330

Fig. 4 — Fully Equipped Work Station.

listing that appears to most closely match the request, and reasonable alternate suggestions must be available.

Residence Searching

To search the residence file, all or part of the surname must be keyed into the FN field. This surname is separated from any other FN data by a trailing blank (indicating a fully spelled surname) or a period (indicating a partially spelled surname). Other words of FN may then be keyed, each one terminated by a space or period.

The default book is that file to which the operator position is preset, ie the most commonly used file. This file will be searched unless the operator may choose to over-ride the default book. This is done by depressing one of the frequently referenced locality keys or the LOC key followed by a full or partial spelling of a locality and depression of the LOC STEP key.

The street name may optionally be provided (spelled in full or part) following the SN key.

Finally, the depression of the RES key initiates the computer search of the residence file.

If the locality data has been partly keyed, the system searches a locality table for the contents of the LOC input field. The table entry determines the exact, full spelling to replace the keyed contents of the LOC field, and the book (file area) to be searched. Also, if the specified locality is not in the default book, the book display field is replaced with a correct book name.

Next, the entire group of listings which match the keyed surname (or partial surname) is checked for closeness of match to the other search arguments (inputs). Whatever elements of FN(s) and SN fields are keyed, are compared to the FN and SN fields in the records. In addition, if a locality is specified (as opposed to a book only), the relative geographic location of the specified locality, is compared to those of the records. (If any of these parameters are not keyed, that element of the listing is not used in determining the closeness of the match).

When each keyed parameter has been compared to a particular listing record, the degree of match of each parameter is weighted. This weighted "match value" determines whether the current listing will be at least temporarily retained for display. The result of the entire scan is a display containing the group of best matched listings in alphabetical order to the top of the display, followed by the next best group, and so forth. No more than 20 RES listings are ever displayed on a single screen, or "page". If the first group of equally good listings overflows the display, all other "worse" groups are made available to the operator through the use of the "page forward" key. If the number of listings that match the keyed information exceeds a predetermined number, the operator will receive a "TOO MANY LISTINGS" message and will be required to provide additional data.

If the initial search results in a "Not Found", and if there are alternate spellings for the keyed surname, the operator may depress the alternate spelling key to display the alternates as they are currently shown in the directory. The operator may then select an appropriate alternate, followed by the RES key, to start a new search; it is not necessary to rekey any other parameters. The operator may also delete from the request that information about which the caller is least sure, eg street, initials.

Business Searching

The operator strategy is to select and key an uncommon word as the finding name.

Finding name words are keyed in full or in part along with a book specification and/or an optional locality for BUS searches. It is not necessary to know the first name of a business nor the compound entry header for an indented directory entry in order to retrieve the listing. During data base update a keyword is created for each

http://doi.org/10.18080/jtde.v13n3.1330

word of the finding name or indented entry text. These keywords are indexed to the actual listing on the data base. During retrieval, all listings in the specified book or locality containing the keyed words or abbreviations in their FN (in any order) are displayed in alphabetical order. If more listings are retrieved than will fit in a display, multiple "pages" are made available to the operator. The "page forward" and "page back" keys are used to review them. If too many listings match the keyed data the operator will be asked to modify the information.

Government Searching

Government directory listings are characterised by captions and indents. For example, Navy Recruiting might be included under Navy which is under Department of Defence, which is under Commonwealth Government. In a GOV search, full or partial spellings of words appearing in any indent level may be keyed. The resulting display will show all levels of captions above the indent level of the lowest level caption containing any of the keyed words. In addition, all indents below this caption will be displayed. The operator keying strategy and the system execution is the same as for business searches.

AUTOMATIC CALL DISTRIBUTORS

Network Automatic Call Distributors (NACDs) link the switching network to Telecom's manual service levels. Their function is to distribute incoming calls from the network to available manual operating positions in the most efficient manner. Operation of the NACD is on a State wide basis and will allow an incoming call from anywhere within the State to be routed to an available operator anywhere within that State, thus eliminating the condition of "busys" or lengthy delays in one location while other locations have operators available. The ACD terminal is shown on the right hand side of Fig. 4.

CONCLUSION

The implementation of DAS/C sees Telecom moving from a method of providing a service which has been traditional for at least 50 years. For some time it has been recognised that the traditional method has made it difficult to provide the standard of service expected by Telecom's customers. Like other business areas Telecom has turned to the computer to help satisfy the ever increasing demand for Directory Assistance. The general features of the DAS/C system have been discussed in this paper.

GLOSSARY OF TERMS AND ABBREVIATIONS

DAS/C Number:
A system generated number which uniquely identifies each line of entry.

DAS Inquiry Terminal:
Terminals which can access the inquiry data base excluding the DAS/C number.

Data Send Centre (DSC):
The remote data entry installation located in each State Directories Branch which inputs the update data.

Directory Inquiry Centre (DIC):
Directory inquiry terminals located in each State Directories Branch for use in data preparation and error correction. The terminals access the inquiry data base and the response includes the DAS/C number.

File Inquiry Processor (FIP):
A System 7 computer which executes the file search and passes the data back to the TPC.

Inquiry Data Base (IDB):
The data base created in the retrieval centres after each update of the master data base.

Master Data Base (MDB):
The data base retained at the master update centre and updated on a daily basis.

Master Update Centre (MUC):
The central computer installation located at Clayton, Vic. which holds and updates the national data base.

Retrieval Centre (RC):
Located in each mainland capital city and comprising two or more retrieval systems.

Retrieval System:
A file inquiry processor and disk attachment for storage and retrieval of the inquiry data base.

Statistics Processor (SP):
A Series 1 computer which collects statistical data from the TPCs and processes the data.

Teleprocessing Controller (TPC):
A Series 1 computer which co-ordinates inquiry traffic from associated TCs and passes this to and from the file inquiry processor. It also collects accumulated statistical records from the TCs and presents this data to the statistics processor.

Terminal Controller (TC):
A Series 1 computer which controls a number of terminals, accumulates system and operator data relating to inquiries and the data to a TPC and passes the required listing back to the inquiry terminal for display.

REFERENCES

1. MAC Plan — 1979 (1981 Version), Telecom Australia.
2. IBM Series 1, Directory Assistance System User Guide.

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 13 Number 3 September 2025

http://doi.org/10.18080/jtde.v13n3.1330

Comments on the Two Historical Reprints in Automation of Directory Assistance

Ian Campbell
Former Telecom/Telstra Executive

Abstract: This paper is a comment on the background to the two historical papers reproduced in "Automation of Directory Assistance" in this issue. The experience of this author is that, despite a rapid decline in the service quality and mounting operating costs, Telecom was slow to act on automation of the Directory Assistance Service, did not fully exploit the advantages of the automated system, and provided a Directory Assistance Service that was clearly inferior to world's best practice. Some benchmarking results are provided as evidence.

Keywords: Directory Assistance, Benchmarks, History of Australian Telecommunications

[**Editor's note:** The *Journal* is delighted that its articles encourage discussion amongst readers. We are happy to print written comments as well as to further the discussion.]

Introduction

My comments are based on my management of Telecom Australia's directory publishing service almost continuously from 1976 until 1991, my visit in 1977 to AT&T and attendance at a trial by AT&T of the CCI system to be trialled in Telecom, my close association with Telecom's directory assistance service from 1976 to 1991, and my management of the directory assistance service from 1989 to 1991.

In the late 1970s, Telecom's directory assistance service used a paper-based system for providing numbers to callers. My recollection is that, in the centres I visited, service operators worked in a room with paper lists of updated numbers for new subscribers (what Telecom called customers), such as weekly and monthly, spread over tables. My opinion was that the locations were primitive in terms of accommodation and ergonomics. The operators' hands were often ink-stained from the printed lists.

https://doi.org/10.18080/jtde.v13n3.1340

Telecom's Directory Assistance Service

I provide five comments about the trial and the final IBM DAS/C system described in the two historical papers from 1981 and 1982 reprinted in Moorhead (2025).

1. The papers make no mention of the approaching crisis in customer service quality, operating costs and worker satisfaction in the directory assistance service from around 1975 to 1980.

Calls to the service were escalating as more callers were preferring to use the service rather than the increasingly heavy and bulky metropolitan White Pages.

The quality of service was poor, as many calls were not connected, call waiting times for connection to the operator were too long, call holding times once connected were too long, and too many numbers could not be found. Operators' work satisfaction was low as customers increasingly reacted negatively to the poor service.

Costs, mostly for operators, were estimated to climb from about $23 million in 1976/77 to over $32 million in 1980/81.

2. The papers overlook the slow progress in establishing and completing the trial and the time for calling tenders.

In early 1977, I visited the headquarters of AT&T, then the world's leading telecommunications business, and saw an AT&T demonstration trial of a computer-based directory assistance service provided by Computer Consoles Incorporated (CCI). AT&T claimed at that time that every second that the call holding time was reduced was worth about $US 1bn in additional revenue from more calls handled and numbers found and a major reduction in operating costs. The value of such a system was obvious, even dramatic, in improved customer service, operating costs and worker satisfaction and productivity.

I arranged with CCI a 10-screen trial at no cost to Telecom in a location to be agreed within Australia (likely Sydney or Melbourne) with CCI and a local telecommunications manufacturer, STC, providing the equipment and a consultant, subject to Telecom approval.

The proposal for a trial was first made about April 1977 to Telecom's headquarters, which raised no interest. Preparation for a trial began in Sydney around late 1977 and headquarters eventual joined the project (as described in Dougall (1981), the first reprinted historical paper). The trial progressed over February to August 1979 and, after tenders were called, a contract was let to IBM in January 1981. My recollection is that national implementation was completed in 1985 (as described in Baxter & Lyon (1982), the second reprinted historical paper).

https://doi.org/10.18080/jtde.v13n3.1340

Over eight years is a long time to deploy a system offering such a radical improvement in the quality of customer service, operating costs, productivity and operator working satisfaction at a time when the service was faltering.

3. The considerable union and staff involvement and consultation as outlined in Dougall (1981) was common for the period, but the process still left Telecom unprepared for the predictably strong union opposition to the system.

The operators' union, the Australian Telephone and Phonogram Operators Association (ATPOA), covered employees connecting long-distance calls, international calls, paging calls and directory assistance. Over the 1980s, exchange automation would eliminate most of the call connection services and DAS/C would significantly reduce the number of directory assistance operators required. The fall in union membership caused an amalgamation in 1988 of the ATPOA with the Technicians, the ATEA.

Strong industrial action against the DAS/C system by the ATPOA found Telecom unprepared and resulted in the union exploiting the arguable impact of Repetitive Strain Injury (RSI), which hindered deployment of the system and accumulated workers compensation claims exceeding $120 million (Campbell, 2017).

4. In planning the implementation of the system, the emphasis was on operating the system within the Telecom environment, with little attention given to exploring the potential of the system without that constraint.

The result was that Australians experienced a directory assistance service that was seriously inferior to that routinely produced in the USA.

Some of the main structural actions towards the US model were:

- Fewer directory assistance service centres;
- An increase in the number of operator positions in each centre depending on the location;
- Fully separate operator centres from Telecom premises, which included leaving the main telephone exchanges, and locating the centres in areas that could provide motivated operators, such as those living in larger, industrially less influenced cities, such as Ballarat, Townsville, Perth, Adelaide and Geelong. The separation would help to moderate the influence of operators from Telecom and the union.
- With the number of centres and the location of the centres optimised, call queuing, processing and management of the directory services could move towards full optimisation — call collection and distribution, the number of centres and the number of positions in each centre — to service the call volumes.
- Attempt to move operator wages, conditions and working practices towards private sector standards. For more details on the industrial relations at the time, see Campbell (2017).

https://doi.org/10.18080/jtde.v13n3.1340

5. In 1988, I arranged a benchmarking study by Booz Allen Hamilton of Telecom's directory assistance service against four Regional Bell Operating Companies in the USA. The difference was shocking. Telecom delivered a clearly inferior service at a significantly higher cost.

Telecom's service quality was lower in fact and as perceived by the customer (Table 1).

Table 1. Comparative Performance Measures for Directory Assistance

Measure	Telecom	US Average
Calls Dropped	17%	Less than 1%
Average Speed of Answer	12 seconds (estimated)	3–6 seconds
Customer Perceived Quality Very Satisfied	86%	97%

Source: Benchmarking study

The cost of a US operator to handle a directory assistance call in the US was two-thirds that of a Telecom operator, and the main reasons were too many call centres, too few operators per centre, the locations of centres, conditions of employment, the workplace rules and labour cost.

With lower online hours per day, fewer work days per year, and a longer mean service time, a Telecom operator handled about 67% of the call volume per online hour of a US operator (Table 2).

Table 2. Comparative Efficiency Measures for Directory Assistance

Measure	Telecom	NY Tel	PacBell	Bell Atlantic
Number of Operators	2,248	2,195	5,200	7,180
Total Call Volume (millions)	166	350	873	1,217
Online Hours/Operator/Year	1,093	1,573	1,573	1,573
Calls/Online Hour/Operator	68	101	107	108

Source: Benchmarking study

Note the consistency and discipline of performance of the three US operators.

Conclusion

While the historical papers reproduced in Moorhead (2025) adequately describe the initial trial (Dougall, 1981) of an automated directory-assistance service and the subsequent deployment (Baxter & Lyon, 1982) of a nationwide DAS/C system, they do not describe the background leading to the new system, nor the service results from the final implementation. My comments are aimed at filling those gaps.

During the 1970s, Telecom's directory assistance service came under pressure from increasing call volumes and antiquated operating procedures and environments. There was a clear case for greater automation and improved working conditions. I had identified a working system

https://doi.org/10.18080/jtde.v13n3.1340

in the US that could be trialled in Australia, but it took some years before a trial was conducted and the system was operational. The trial showed clear advantages in service quality and improved operator performance.

After the new automated system for directory assistance had been rolled out and had been operating for a few years, I commissioned a benchmarking study that clearly showed that Telecom had not fully taken advantage of the benefits that could have been achieved. In particular, more consideration of the size and location of the directory-assistance call centres and the work practices therein could have yielded significantly improved service quality and efficiency. The summary performance indicators provided in these notes clearly make the case.

References

Baxter, I., & Lyon, H. (1982). The National Computerised Directory Assistance Service — DAS/C. *Telecommunication Journal of Australia, 32*(2), 96–100.

Campbell, I. (2017). Fact or Fraud?. *Journal of Telecommunications and the Digital Economy*, *5*(2), 75–97. https://doi.org/10.18080/jtde.v5n2.107

Dougall, C. J. (1981). Trial of a Computer Directory Assistance System — Sydney. *Telecommunication Journal of Australia, 31*(1), 79–84.

Moorhead, S. (2015). Automation of Directory Assistance. *Journal of Telecommunications and the Digital Economy*, *13*(3), 176–190. https://doi.org/10.18080/jtde.v13n3.1330

Clemens William ("Clem") Pratt

2 July 1936–16 January 2025

Leith H. Campbell
TelSoc Member

Abstract: This paper is an appreciation of the life and contributions of Dr C. W. (Clem) Pratt, who died in January 2025. He had a 38-year career with the PMG's Department and its successors, working first on traffic engineering and then expanding his career and interests into computing and operational support systems. He was a Distinguished Fellow of the Telecommunications Society of Australia, having been Vice-Chairman of the National Board for 17 years. He was active in the Statistical Society of Australia, serving as national Chairman for one term. He was a long-term member of the Advisory Council for the International Teletraffic Congresses and an influential educator on teletraffic engineering and related statistical methods.

Keywords: International Teletraffic Congress, Telecommunications Society of Australia, History of Australian Telecommunications

Introduction

Clem Pratt in 1982 (Source: *Telecommunication Journal of Australia*, *32*(3), 230)

Dr Clem Pratt, who has died at the age of 88, was a long-standing promoter of teletraffic engineering and statistical knowledge applied to telecommunications management and planning. He served as the Australian representative on the International Advisory Council of the International Teletraffic Congresses from 1970 to 2005 and received a Lifetime Achievement Award from that Council in 2005. He was President of the Statistical Society of Australia for 1969–1971. He served as Vice-Chairman of the National Board of the Telecommunications Society of Australia from 1982 to 1999. He

https://doi.org/10.18080/jtde.v13n3.1322

was a member of the Editorial Board of the journal *Australian Telecommunication Research* from 1974 to 1995.

Early Life and Education

Clemens William Pratt (2 July 1936–16 January 2025) was born in Albury, NSW, the second of four children of Malcolm and Olga Pratt. The family later relocated to Dalby, Queensland. Clem attended Dalby State School, Concordia Memorial College in Toowoomba and Brisbane High School, where he was Dux in 1954 (Schuller, 2025).

Like many aspiring electrical engineers of the period, he joined the Post-Master General's Department (PMG) in 1955 as a cadet engineer in order to finance his university studies. He remained with the PMG and its successor organizations for 38 years before taking early retirement in 1993.

He attended the University of Queensland and graduated in 1959 as a Bachelor of Engineering (Electrical) with First Class Honours and a University Medal for outstanding merit. He continued his studies at the University of Queensland, graduating with a Bachelor of Science in 1962 and a Master of Engineering Science in 1961. His Master's thesis title was "Telephone Traffic and Crossbar Switching". The technical interests that would guide his career were already apparent.

The Public Service Board (on the recommendation of the PMG) awarded him a two-year scholarship to undertake postgraduate studies and he decided to enrol for a Ph.D. at Birkbeck College, University of London, under the supervision of David Cox (later Sir David Cox), then a rising star as a statistician and educator. It was ambitious to attempt to complete a doctorate by research in only two years, but he succeeded, graduating in 1963. His thesis was entitled *Congestion Problems in Automatic and Semi-automatic Telephone Exchanges*.

Clem had married Lois Richards in May 1959 in Gympie, Queensland. After the sojourn in London, they returned to Melbourne and made their long-term home there. Their three children were born there between 1965 and 1970 (Schuller, 2025).

His Career in the PMG

While Clem was studying, he was also contributing to projects in the PMG. After his undergraduate degree, he was promoted to Engineer Grade 1 and participated in some transmission optimisation studies. By 1961, he was looking at alternative routing design procedures. His clear expertise in mathematical methods was being recognised.

After his Ph.D. research in London, he joined the Victorian Planning Branch where he worked on the planning of the 21 exchanges in the Melbourne metropolitan network. He undertook

https://doi.org/10.18080/jtde.v13n3.1322

various studies on economical or optimised designs. By 1966, he was an Engineer Class 3, Traffic Research (Pratt, 1993), using his knowledge of queuing theory and simulation. Importantly for his future career, it was becoming clear that future planning and design procedures would be increasingly computerised and Clem was formulating requirements for suitable computer programs. He did step back to earlier manual calculations, however, to advise engineers on how to do compound growth calculations on a slide rule (Pratt, 1968a).

At this time, Clem developed a two-week residential course in Traffic Engineering. This proved to be both timely and popular. As the final (and revised) published version of the course notes described it:

> In May 1967 the first Australian course in telephone traffic engineering was held in Kalorama, Victoria. This event was of special significance and marked the first venture by the Postmaster General's Department into residential training in an advanced technological field. Traffic engineering was chosen … because of its vital importance in the rapid expansion of telecommunications services using modern automatic switching systems.
>
> The course proved to be very successful and was repeated virtually unchanged in 1968, 1971, 1973 and 1974. The original course manual, prepared by Dr C. W. Pratt, who was the director of studies and principal lecturer throughout this period, was published in 1967 and received wide distribution in Australia and overseas (Telecom Australia, 1978, Foreword).

By 1972, he was Engineer Class 5, Traffic Engineering Section, and head of Traffic Engineering in Headquarters (Pratt, 1993). Here, he was a major contributor to a project to collect and analyse relevant measurements of network traffic, so that the data could be used for network management and planning. The project was called the Traffic Data Equipment project, because new equipment was installed in telephone exchanges, but the processing of this data by computer, the "TRA Application", was equally important. Clem contributed to both these aspects. He described the data to be collected and its processing in a paper for the *Telecommunication Journal of Australia* (TJA) (Pratt, 1973a). Clem's paper was described as "Part 1"; the "Part 2" paper, describing the actual exchange equipment, was written by Leo Tyrrell (1974).

At this time, Clem also began to contribute to international standards for traffic engineering and international network planning through the CCITT (now ITU-T), specifically Study Group XIII, Working Party 2 (Traffic Engineering). The work is described in Pratt & Tånge (1973), outlined below. Clem was Vice Chairman of the Working Party from 1970 to 1976.

https://doi.org/10.18080/jtde.v13n3.1322

On 1 July 1975, Telecom Australia was formed, separated from the postal business, but still in government ownership. Telecom could now develop appropriate computer systems to support its business. Clem became Manager, Systems Planning Branch (Pratt, 1993). His education and background equipped him well for the task.

At that time, much of business computing was considered to be "automated data processing"; widespread decision support and control would come later. Also, limitations on computer memory and processing meant that, for an organisation of Telecom's size and diversity, many different computer systems would be required; it was necessary to plan in a way that ensured high-impact systems would be given priority and that data was not duplicated.

By 1979, it was clear that systems planning and development should be closely aligned and Clem became Manager of the newly formed Systems Development Branch. Many different systems were in development. Clem introduced a number of important reforms, including a formalised method for systems development and the evaluation of user benefits in assessing development proposals.

With the proliferation of computer systems across all of Telecom's business, differences in style and procurement started to become apparent. General business systems for accounting, personnel and inventory, for example, could be sourced from external suppliers, while network operations and support systems were closely tied to the telecommunications networks and required specific computing techniques and coordination with network development. For a year, Clem gained valuable experience as a *user* of these systems as Acting Superintending Engineer, Network Operations Branch within Engineering. Then, in 1985, Clem became Chief Engineer, Computer Support Services Division within Network Engineering.

In 1985, George Hams (Black, 2023) had compared Telecom with comparable overseas telecommunications utilities and had found Telecom lagging in a number of areas, including "the development of major operational information systems" (Campbell, 2017, p. 22). While Ian Campbell believes that no significant follow-on actions occurred, the report did stimulate further development of network operations support systems. Clem led that effort for three years.

In the 1980s, the United States and other countries became concerned that they were lagging in productivity compared with Japan and looked to find ways to catch up. The work of Edwards Deming, an influential statistician and educator, building on the Japanese experience popularised "Total Quality Management" (TQM) (Deming, 1982) as a productivity multiplier. Telecom management, which had been building towards likely direct competition, joined the

https://doi.org/10.18080/jtde.v13n3.1322

TQM bandwagon and appointed Clem as General Manager, Performance and Quality in 1988 (Pratt, 1993) to lead the corporate drive.

Clem became an evangelist within Telecom for the TQM concept. In an address to an internal conference in 1989, he made a distinction between "quality" and "excellence" and noted:

> Total quality management philosophy holds that the customer is the final judge of quality and that improvement of quality in the eyes of the external customer in a competitive world demands improvement of all the activities within the enterprise (Pratt, 1989, p. 45).

Such a "philosophy" would require a profound culture change in Telecom. Clem was able to introduce new training, quality performance indicators and customer satisfaction surveys, but root-and-branch change eluded him and, indeed, remained an issue (couched in other language) in the organisation long after he left it.

With the merger in 1991 of Telecom and OTC into what became Telstra, there was a new push for network and systems modernisation to prepare Telstra for direct competition. This evolved into the "Future Mode of Operation" (FMO) project (Campbell, 2017, pp. 48–52). Clem was part of this as Manager, Network Modernisation Strategy. Clem was well suited to this role, with his wide understanding of the organisation and his background in modelling and simulation.

With the early stages of the FMO complete and the organisation and management continuing to churn with the advent of competition, Clem somewhat reluctantly took early retirement in 1993. Although it was "early" at the age of 57, he had by then chalked up 38 years in the PMG, Telecom and Telstra. He had witnessed and been a leader in the early computerisation of Telecom's operations and the greater quantification of business processes and management. These are trends that continue today.

International Teletraffic Congresses

The International Teletraffic Congress (ITC) series had been started under the chairmanship of Professor Dr Arne Jensen from Denmark in 1955, in order to bring together researchers, practitioners, academics and mathematicians to share knowledge and advances for understanding telecommunications traffic and its implications for network planning, design and management (ITC, 2016).

Tony Newstead from Australia (Newstead *et al.*, 2017) had attended the second ITC in The Hague and had prepared a paper for the third ITC in Paris in September 1961. Newstead had recently returned from London and asked Clem to present the paper on his behalf (Newstead *et al.*, 2017, Attachment A). This was Clem's first ITC. Subsequently, when in 1970 Newstead

https://doi.org/10.18080/jtde.v13n3.1322

relinquished his position as the Australian representative on the ITC's International Advisory Council, he arranged for Clem to replace him. Clem remained on the Council for 35 years until 2005, when he received a Lifetime Achievement Award for his service at ITC19 in Beijing, China.

Clem used his relationship with the ITCs not only to gain the latest knowledge and techniques and bring them back for application in Australia, but also to encourage teletraffic research and understanding within the Australian technical community. He brought ITC to Australia, with ITC8 being held in Melbourne in November 1976; and he was a main organiser of the 1989 ITC Specialist Seminar in Adelaide.

Clem contributed three technical papers to the ITCs. He attended ITC5, in New York, in June 1967 and gave a paper on "The Concept of Marginal Overflow in Alternate Routing" (Pratt, 1993). Unfortunately, papers from ITC5 are not available online.

His second paper, for ITC6 in September 1970 (Pratt, 1970) was entitled "A Group of Servers Dealing with Queueing and Non-Queueing Customers". This situation was applicable to the case where a telephone exchange would have incoming calls from operators and from ordinary callers: operator calls would be queued and the operator would get the next available circuit; ordinary callers would hear a busy signal if no circuits were available and would have to redial. The purpose was to find the probability that an ordinary customer would encounter a busy signal given the number of available circuits ("servers") under any traffic assumptions. This could be used to determine the appropriate size of an exchange given some traffic forecasts. Clem used standard queuing theory to show how to solve the general case and to give solutions to two limiting cases that could be used for exchange dimensioning. Some numerical examples were provided.

His third contribution was to ITC7 in June 1973 (Pratt & Tånge, 1973), entitled "On Traffic Engineering Studies in the CCITT". This described the outputs from the then-recent CCITT (now ITU-T) international standards on traffic engineering (included in the CCITT "Green Book" after the plenary in 1972), especially from CCITT Study Group XIII, Working Party 2. It outlined the relevant questions that would be pursued by the CCITT in the next study period (1973–1976) and encouraged ITC attendees to contribute. One issue highlighted was the effect of repeated call attempts that can cause overload in a voice network (which remained a problem for network operators for many years, causing some infamous network failures, for example (Gorman, 1985), when thousands of fans in the USA used auto-diallers to try to get through, mostly vainly, to an agency to buy tickets for a Bruce Springsteen concert).

https://doi.org/10.18080/jtde.v13n3.1322

Other Contributions and Interests

For the Telecommunications Society of Australia (TSA), Clem was appointed to the Council of Control, which later became the National Board, as Vice-Chairman in 1982. He remained in that position until 1999, when he was made a Distinguished Fellow of the Society ("New Distinguished Fellows", 1999, p. 31). The TSA published a second journal, *Australian Telecommunication Research* (ATR), from 1967 to 1995. Clem served on the Editorial Board from 1974–1995 (Gerrand, 1996, p. 35). He had been instrumental in setting a high standard for ATR from the beginning by submitting two papers to volumes 1 and 2 (Pratt, 1967; 1968b). He later provided a third paper (Pratt, 1973b), which was a version of his earlier ITC paper (Pratt, 1970).

Clem joined the Victorian Branch of the Statistical Society of Australia when it was founded and was a member of the Branch Council from 1965 to 1972. He served as President of the Victorian Branch, 1968–1969 (Pratt, 1993), and was the national President 1969–1971 (Gordon, 2025).

Clem had been a technical mentor and educator for many in the PMG and Telecom, and his abilities extended outside the organisation. In the 1960s, he had been a part-time lecturer and tutor at the University of Melbourne in Operational Research and Statistical Methods for Research Workers. He was the Telecom representative on the Mathematics and Operations Research Advisory Board at Footscray Institute of Technology from 1973 and chaired the board from 1979 to 1987. He was a member of the Institute's Council from 1987, transitioning to the Council of Victoria University of Technology when the Institute became a university. He was on the Advisory Board of the Teletraffic Research Centre at the University of Adelaide and became chair during the later years of the Telecom contract there. After his retirement from Telstra in 1993, he contributed to training courses in neighbouring countries, notably a course on "traffic engineering and forecasting" in Vietnam in November 1998.

Clem had a life-long interest in swimming and diving, starting in his school days and continuing during his university studies. In London, he joined the Highgate Diving Club and competed in competitions around the country, winning medals in springboard and firmboard events.

Clem had a love of classical music, playing the piano and organ, as well as singing. He was a member of the Royal Melbourne Philharmonic Choir, singing bass, for 12 years after his retirement from Telstra. He also played the organ at his local Lutheran church for 30 years.

https://doi.org/10.18080/jtde.v13n3.1322

In later years, Clem was plagued by various health problems that gradually reduced his abilities. He passed away on 16 January 2025 and his funeral[i] was held at the Redeemer Lutheran Church, Glen Waverley, where he had been a founding member of the congregation.

References

Black, S. (2023). George Edward Hams AM (1928–2023): A leader amongst Australian telecommunications engineers. *Journal of Telecommunications and the Digital Economy*, *11*(2), 252–261. https://doi.org/10.18080/jtde.v11n2.739

Campbell, I. (2017). Telstra's Future Mode of Operation - the transformation of the Telstra's Network - 1992/93. *Journal of Telecommunications and the Digital Economy*, *5*(4), 18–69. https://doi.org/10.18080/jtde.v5n4.123

Deming, W. E. (1982). *Quality, Productivity, and Competitive Position*. Cambridge, MA, USA: MIT Center for Advanced Engineering Study.

Gerrand, P. (1996). Adios ATR. *Telecommunication Journal of Australia*, *46*(2), 34–36.

Gordon, I. (2025, January 26). Vale Clem Pratt. Statistical Society of Australia. Available at https://www.statsoc.org.au/Forum-general-topics/13454881, Accessed 23 June 2025.

Gorman, S. (1985, July 22). Springsteen calls tangle Washington telephone lines. UPI Archives. Available at https://www.upi.com/Archives/1985/07/22/Springsteen-calls-tangle-Washington-telephone-lines/9999490852800/. Accessed 18 June 2025.

ITC [International Teletraffic Congress]. (2016). History of the ITC. Available at https://itc-conference.org/about-itc/history.html. Accessed 17 June 2025.

"New Distinguished Fellows of the TSA". (1999). *Telecommunication Journal of Australia*, *49*(4), 30–31.

Newstead, M., Pratt, C., Burke, J., & Gerrand, P. (2017). Tony Newstead (1923–2017). *Journal of Telecommunications and the Digital Economy*, *5*(4), 87–96. https://doi.org/10.18080/jtde.v5n4.135

Pratt, C. W. (1967). Marginal Overflow in Alternate Routing. *Australian Telecommunication Research*, *1*(1/2), 76–82.

Pratt, C. W. (1968a). Slide Rule Compound Growth Calculations. *Telecommunication Journal of Australia*, *18*(3), 279–280.

Pratt, C. W. (1968b). Filled Row Distribution in a Rectangular Array. *Australian Telecommunication Research*, *2*(2).

Pratt, C. W. (1970). A Group of Servers Dealing with Queueing and Non-Queueing Customers. International Teletraffic Congress 6, Munich, Germany. Available at https://gitlab2.informatik.uni-wuerzburg.de/itc-conference/itc-publications-public/-/raw/master/itc06/pratt70.pdf. Accessed 17 June 2025.

Pratt, C. W. (1973a). Development and Application of Telephone Traffic Measuring Equipment (Part 1). *Telecommunication Journal of Australia*, *23*(3), 205–209.

Pratt, C. W. (1973b). A Group of Servers Dealing with Queueing and Non-Queueing Customers. *Australian Telecommunication Research*, *5*(3).

Pratt, C. W. (1989). Quality as a Universal Motivator for Telecom. *Telecommunication Journal of Australia*, *39*(3), 43–47.

Pratt, C. W. (1993). Curriculum Vitae. Unpublished [provided by the family].

Pratt, C. W., & Tånge, I. (1973). On Traffic Engineering Studies in the CCITT. International Teletraffic Congress 7, Stockholm, Sweden. Available at https://gitlab2.informatik.uni-wuerzburg.de/itc-conference/itc-publications-public/-/raw/master/itc07/pratt732.pdf. Accessed 17 June 2025.

Schuller (née Pratt), H. (2025). Eulogy and Words of Tribute. A Funeral Service for Dr Clemens William Pratt, Redeemer Lutheran Church, Glen Waverley [provided by the family].

Telecom Australia. (1978). *A Course in Teletraffic Engineering*. Prepared by the staff of Traffic Engineering Section, Planning Services Branch, Headquarters 1978. Telecom Australia. [Regrettably, this book appears now to be out of print.]

Tyrrell, L. A. (1974). Development and Application of Telephone Traffic Measuring Equipment – Part 2. *Telecommunication Journal of Australia*, *24*(1), 36–43.

Endnote

[i] A video of the funeral may be viewed at https://www.youtube.com/watch?v=FHkUcfLKU-Y (accessed 22 July 2025).

https://doi.org/10.18080/jtde.v13n3.1322