

Towards a Cashless Transactional Society Through the Adoption of Digital Banking Services

Matipa Ricky Ngandu¹, Gardner Mwansa², Siwongiwe Queenest Ntoyabo³

rngandu@wsu.ac.za¹, gmwansa@wsu.ac.za², siwongiwelissa@gmail.com³

^{1,2,3} Walter Sisulu University

Article Information

Received : 3 Jan 2025

Revised : 5 Mar 2025

Accepted : 3 Apr 2025

Keywords

Cashless transactions,
Cybersecurity,
Cybersecurity
Awareness, Digital
banking, Digital literacy,
Financial inclusion,
Information Security

Abstract

This study explores the adoption of digital banking services in a rural South African town in the Eastern Cape, emphasizing its contribution to a cashless society. Employing a quantitative method, it examines digital banking usage, adoption challenges, and information security awareness. Data were collected through surveys and analyzed using descriptive statistics. Findings show that mobile and online banking are widely used for convenience and accessibility, with most users engaging in money transfers, credit payments, and online shopping.

However, challenges such as poor digital literacy, infrastructure issues like internet access, cost of access, and cybersecurity concerns persist. Users face risks like phishing, hacking, and social engineering, revealing gaps in security awareness and trust. These issues particularly affect older users and those with limited technological experience.

While digital banking improves financial inclusion and economic engagement in rural areas, its full potential is hindered by these barriers. The study underscores the need for digital literacy programmes, infrastructure improvements, and robust cybersecurity measures to build trust and ensure secure adoption. Future research should evaluate interventions, explore emerging technologies like blockchain and AI, and compare regional strategies for inclusive digital financial systems.

A. Introduction

Digital technology has significantly transformed economic and social structures, shaping modern societal interactions, business models, and economic policies [1], [2]. This transformation is characterized by enhanced connectivity, the emergence of new business paradigms, and shifts in governmental strategies aimed at fostering digital economies [3]. Digital banking refers to the access of banking services and transactions through internet or mobile networks [4]. It includes electronic banking and open banking, where banking services are made accessible through APIs by third-party providers [5]. Researchers often use the terms internet banking and digital banking interchangeably [6].

Traditional sectors of global and local economies are experiencing transformative effects resulting from the need to transition to a digital economy. The integration of technology is not only changing operational processes but also redefining customer engagement and service delivery. However, achieving the full potential of these advancements necessitates addressing issues related to the digital divide, data privacy, and cybersecurity [3].

Global cashless payment volumes are set to increase by over 80% from 2020 to 2025, highlighting the urgency of embracing digital transformation [7]. Africa's Digital Transformation Strategy for 2020–2030 emphasizes the creation of an inclusive digital society [8]. In South Africa, government strategies promote digital payments as part of broader financial inclusion goals, driving economic activity, digital trade, and societal opportunities [9], [10]. This shift to a cashless society emphasizes reducing the need for physical cash and in-bank transactions, placing digital banking and cybersecurity at the forefront of discussions. Sustainable Development Goals (SDGs) addressing economic growth and inclusivity have driven investments in financial inclusion projects [11]. South Africa's achievement of widespread ICT access has facilitated digital banking adoption [12]. Achieving SDGs has realized the broader digital banking adoption phenomenon [7], [13]. Digital banking offers numerous advantages, including reduced operational costs for banks and improved accessibility for consumers. Banks have transitioned from physical branches to technology-enabled, branchless services, offering features such as electronic fund transfers, credit payments, and account management [14], [15]. However, significant disparities remain between developed and developing economies regarding internet penetration, digital finance technology, and innovation levels [13], [14], [16].

While developed countries have broadly adopted digital banking, developing nations face gradual adoption rates [17]. Moreover, billions of annual online financial transactions are vulnerable to cybercrime [18]. Threat actors, including state-sponsored groups, cybercriminals, and hackers, exploit vulnerabilities, leaving customers particularly those lacking cybersecurity knowledge exposed [19], [20]. This adversely affects many customers, most especially those who are not knowledgeable nor have the requisite skills to practice cybersecurity when making decisions on how and whether to do banking transactions on-line. Designing user-friendly, practical, and dependable solutions is important if digital banking is to be adopted and used as intended [20], [21]. Therefore, the regulators of electronic

banking must influence consumer perceptions of the benefits, simplicity, and security of electronic banking [20], [21].

Strengthening technological safeguards, raising user awareness, and ensuring institutional vigilance are critical to mitigating these risks [22]. Cybersecurity risks in online banking are advancing, as perpetrators employ advanced strategies like phishing, social engineering, and malware assaults to take advantage of system weaknesses and ill-informed users [23]. Whenever an individual navigates the web, their device is exposed to risks targeting the theft of personal data or obtaining unauthorized entry to financial accounts [24]. Advanced strategies such as phishing, social engineering, and malware assaults require financial organizations to implement multi-layered security measures and customer education initiatives [25], [26]. Although banks take steps to protect customer transactions and personal information behind the scenes, the customer can also have a significant impact on how safe or unsafe their banking and personal information is [27], [28].

The aim of this study is to investigate the adoption of digital banking services in a South African rural community of the Eastern Cape, specifically in relation to achieving a cashless society. The study also determines how rural communities have adopted the use of digital banking services, how these banking consumers use these digital financial services, and what factors are preventing them from doing so. Hence, seeking to ascertain how customers use of digital banking services and how it can jeopardize their banking information.

B. Review of Literature

The digital banking industry has expanded rapidly in recent years and is expected to expand further as financial institutions encourage customers to access their banking and financial services on-line [29]. In 2017, it was predicted that Internet banking would have 2 billion global users by 2020 [30]. This transformation is driven by technological advancements, evolving consumer demands, and a dynamic regulatory environment. According to [31], banking has experienced a rapid metamorphosis which is being driven by technological advancements, changing consumer demands, and a dynamic regulatory environment. The COVID-19 pandemic further accelerated shifts in consumer behavior [32].

Digital banking services have revolutionized the financial sector by providing convenience and accessibility, especially in underserved rural areas. However, factors influencing customer decisions to adopt digital banking, particularly in Africa, require further exploration [17]. Concerns over data security and trust remain significant barriers to adoption [33], [34]. According to [35], concerns include the perceived risks of loss, uncertainty about data usage, lack of control over personal information, and inadequate disclosures in privacy policies, which can diminish trust in these services. It is critical to understand how users feel about utilizing technology to access banking services and how they perceive the issues of security when using digital banking services.

Adoption and Benefits of Digital Banking Services

The widespread acceptance of digital banking stems from its convenience, on-demand availability, and cost-effectiveness [36]. Internet banking has reduced customer costs and increased operational efficiency for banks [33]. As a result, to remain viable, banks must incorporate digital banking into their service offerings [37]. Although most transactions are traditionally conducted at branch counters, new technologies have reduced customer costs [38].

In rural areas, the proliferation of mobile phones, increased internet penetration, and government initiatives have driven adoption [39], [40]. Collaborations between banks and telecom firms have created innovative solutions, such as mobile money, to enhance financial inclusion [41]. The benefits of digital banking services in rural regions are numerous, including economic empowerment [42], improved financial inclusion [43], and greater efficiency in financial transactions [44], [45].

Challenges to Digital Banking Adoption

Despite its benefits, digital banking adoption faces hurdles such as limited digital literacy, distrust in technology, and inadequate infrastructure [46], [47]. Many users are hesitant due to concerns about ease of use, required skills, and security [48], [49]. The Technology Acceptance Model (TAM) highlights perceived usefulness and ease of use as significant factors influencing adoption [50]. Studies emphasize the importance of trust, perceived value, and financial literacy in shaping attitudes toward digital banking [51]. Concerns over cybersecurity, such as identity theft, phishing scams, and fraud, further hinder adoption. These fears are exacerbated in developing regions with weak cybersecurity infrastructure [52], [53]. Addressing these issues requires robust security protocols, regulatory frameworks, and consumer education initiatives.

Cybersecurity Threats in Digital Banking

Cyberattacks pose significant risks to digital banking, including phishing, social engineering, malware, and data breaches [55], [56]. Threats include: 1) *Software Supply Chain Attacks* - Exploiting vulnerabilities in third-party systems damages reputations and compromises security [57], [58]; 2) *Phishing* - Deceptive tactics to extract sensitive information [59], [60]; 3) *Social Engineering* - Psychological manipulation to exploit individuals [61]; 4) *Malware and Ransomware* - Infiltrating systems to steal data [57]; 5) *Cloud-Based Threats* - Exploiting API vulnerabilities and conducting DDoS attacks [62]; 6) *Customer Behavior* - Poor cybersecurity practices increase vulnerabilities [63], [64]; 7) *Spoofing* - Impersonating trusted entities to extort information [65]; 8) *Unencrypted Data* - Exposing sensitive information [66], [67]; 9) *Fraud and Identity Theft* - Misusing personal data for unauthorized transactions [68], [69]; 10) *Manipulated Data* - Altering data to compromise systems [58].

Strategies to Enhance Digital Banking Adoption

Banks must understand consumer needs and address barriers to adoption through tailored strategies. Periodic surveys can help identify factors influencing user acceptance [37] such as 1) *Education and Awareness* - Providing web preparation

tutorials for users with low digital literacy can improve trust and security [46]. Consumer awareness initiatives should address cybersecurity risks and promote safe online behaviors; 2) *Security Enhancements Technological solutions* such as multi-factor authentication, encryption, and real-time fraud detection can mitigate risks [70], [71]. Social engineering attacks require combined technology and policy strategies, including spam filtering, AI-based traffic monitoring, and disaster recovery plans [72]; 3) *Mitigating Cyberthreats* such as employing cryptanalysis, cyber deception technologies, and access controls [72], securing data at rest, in use, and in transit with encryption and authentication measures [73], human protection strategies that include password security and phishing awareness training [74], the use of Artificial Intelligence such as deep learning-based Deep Neural Network and conducting device profiling can also lead to the detection of spoofing attacks [75], and collaboration among stakeholders to implement biometric applications, digital signatures, and AI solutions [76], [77] can address fraud and identity Theft.

C. Research Method

This section gives an outline of the research method followed in this study. A quantitative approach was chosen for this study with a questionnaire survey for data collection and descriptive statistics for data analysis. The objective of this study was to determine the rate of adoption of digital banking services, identify the obstacles that prevent the use of digital banking services and, determine the information security practice whilst using digital banking services. These objectives informed the elements covered in the survey which included respondents' personal information, including age group, gender, residence status in the rural community, employment status, and income sources. Subsequent questions elucidated respondents' opinions on preference in banking channels, device of most convenience to access banking services, information security and cybersecurity hygiene practices and qualities valued in digital banking services. This resulted in a survey that was divided into the sections: demographic factors; rate of adoption of digital banking services; preventive factors to the use of digital banking services and; how banking services are used.

After constructing the questionnaire, a pilot test was conducted to check clarity, reliability, and relevance. The pre-test assessed how the questions would be perceived by respondents to help identify any issues with question ambiguity, structure, and flow, ensuring the instrument aligns closely with the purpose of achieving stated objectives. It also evaluated the potential for response fatigue as well as adequacy of instructions and the availability of response options. The pre-test involved three peer participants and aimed to obtain constructive feedback on language, time allocation, and familiarity with the terms used. Based on the pre-test findings, some amendments were made to the original instrument, including adding a glossary of technical terms for certain questions so that respondents would not skip technical-related questions.

Whilst the population for this study refers to the community residing within rural Eastern Cape, the sample used in this study represented a selected group of individuals from the population for the purpose of gathering information about the phenomenon. Due to constraints in time, resources, and access, it is impractical to

collect and analyse data from the entire population. Therefore, a non-probabilistic sampling method was employed, as it is not possible to determine the probability of an individual belonging to the population. A simple random sampling technique was used to select respondents based on easy accessibility even though this technique may not yield all groups resident in the rural community. It therefore should be taken into account that the data obtained from this sample cannot be generalized to the entire population.

D. Results

This section presents the results which were obtained using the data collecting tool discussed in the preceding section. The survey was sent out to 100 respondents via emails and social media sites like WhatsApp using Google Forms. There were 17 separate sets of questions on the survey. Only respondents who resided in the rural based town under investigation were considered in this survey. The demographic characteristics of the study's respondents are shown in Table 1 and discussed in the subsections that follow. Data about the participant's gender, age, place of residence, and job status are also included. The purpose of this is to have a better understanding of the types of respondents in the study.

The rate at which residents use digital banking services is presented. Information about the respondents' preferences for these on-line services, the actions taken when using them (for respondents who use digital banking services), and the methods used by respondents to access and use on-line and internet banking services is also discussed. The use of financial services by respondents in a safe and secure manner is also discussed. These inquiries were made to learn how consumers protect their data from potential threats to their finances and private information.

Finally, the study explored the obstacles that some locals face while trying to use internet financial services. The questions in this section were created to help readers better comprehend how users interact with digital banking services and how they first learned about it.

Demographic Factors

In this study, the initial total number of respondents was 100. However, inconsistencies were identified in the demographic breakdown presented in Table 1. Specifically: 1) *Gender and Age* - Both categories reflect data from 93 respondents, leaving 7 responses missing to align with the total respondent count of 100; 2) *Employment Status* - This category also reflects data from 93 respondents, consistent with Gender and Age; 3) *Residence Status* - This category includes data from 100 respondents, suggesting that all participants provided responses for this question.

Furthermore, in Section B.1, 3 respondents were excluded from analysis due to being unbanked. This exclusion reduces the effective sample size to 97 respondents, which impacts the percentages reported for subsequent analyses. Missing data entries for Gender and Age categories are treated as non-responses, and percentages were calculated based on the effective sample size of 97 respondents.

The 100 responses reported in Residence Status were verified to include all respondents, including the 3 unbanked individuals excluded from further analysis. Adjustments to percentages reflect the effective sample size of 97.

Table 1. Demographic Factors

Item	Category	Frequency	Percentage
Gender	Female	63	65%
	Male	30	31%
	Missing	7	7%
	Total	97	100%
Age	18-21	7	7%
	22-45	77	79%
	46-59	6	6%
	≥60	3	3%
	Missing	4	4%
	Total	97	100%
Employment Status	Student	28	29%
	Employed	41	42%
	Self-employed	8	8%
	Unemployed	14	14%
	Senior Citizen	2	2%
	Total	97	100%
Residence Status	Resident	96	99%
	Non-Resident	1	1%
	Total	97	100%

Gender

As indicated in Table 1, 65% of the respondents were females and 31% were males. An additional 7% of responses were considered missing from the respondents. However, these findings carry a potential risk due to the uneven representation of genders, which may have an impact on the data collection objectives and the overall adoption of these banking services in this specific rural town.

Age

Table 1 indicates that 79% of respondents in this study tended to be young adults and middle-aged individuals (between the ages of 22 and 45). This observation alone sheds light on the adoption of on-line/internet banking because the survey was conducted using a web-based processor, and respondents in other studies that examined whether factors such as gender, education level, and age affect the uptake of internet banking, found that young adults are the majority of Internet users and are highly attracted to using cutting-edge technology.

Employment Status

Table 1 shows that 41% of the respondents indicated that they were employed while 28% of the respondents said that they are students, 14% were unemployed, 8% self-employed and 2% were senior citizens.

Residence Status

Table 1 also summarizes the residence status of the respondents. Out of the 97 valid respondents, the large majority (96 respondents, 99%) considered themselves as residents of the rural town, whereas just 1 respondent (1%) was classified as a non-resident. This significant representation of residents illustrates the localized focus of the research and offers a solid foundation for examining the adoption of digital banking services in this particular rural community.

Rate of adoption of digital banking services

The key objective of this sub-question is to determine how many residents utilize digital banking services and some of the reasons for doing so. By doing so, it will be possible to determine which benefits have persuaded certain customers to use these services. These questions also shed light on the numerous channels' consumers use to contact their banks. These questions also provide a window into the reasons why certain customers do not wish to adopt on-line services for those users who do not utilize digital banking services.

Bank Accounts.

As seen in Fig. 1, the respondents were asked about whether they had bank accounts. 3% of the respondents said they did not own bank accounts, compared to 97% of respondents who said they did. The three respondents who gave a negative response to this question were not permitted to complete the survey since it is possible that they do not engage with banks in general or utilize internet banking if they do not have bank accounts.

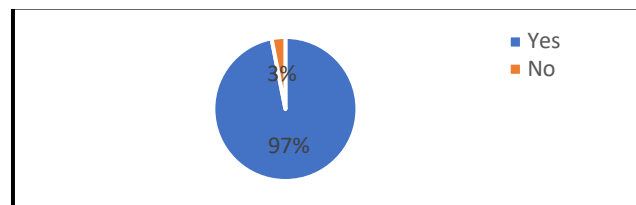


Figure 1. Respondents with Bank Accounts

Forms of Income.

When asked about their sources of income, respondents provided the answers depicted in Fig. 2. 52% of respondents said they had a regular source of income (salary, wage, etc.), 25% said they had allowance (from family members, spouses, etc.), 17% said they had no regular source of income, and 6% said their income came from social grants from the government.

The purpose of this question was to determine whether a reliable source of income would be one of the variables influencing the rate of adoption of on-line/internet banking.

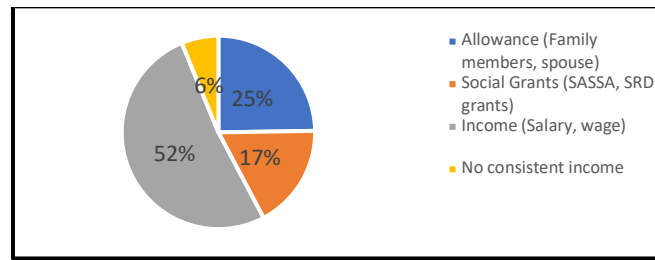


Figure 2. Respondents Forms of Income

Preferred form of Banking.

The researcher asked the respondents, and their responses are presented in Figure. 3, whether they preferred internet banking or physical banking. Among the respondents, 42% stated they liked using internet banking, 21% said they preferred using physical banking, and 37% said they preferred using both types of banking. This results show a total of 79% of the respondents being confident using on-line/internet banking.

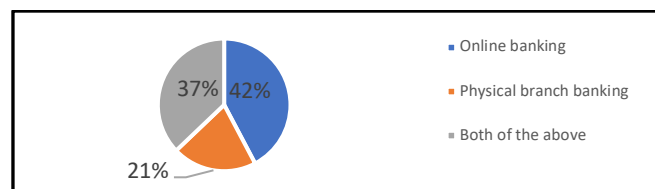


Figure 3. Preferred form of Banking

Views on different forms of Banking.

The respondents' opinions on various banking types are shown in Fig. 4. Among the respondents, 66% stated that they believe digital banking is quick and secure, 20% that they believe it is quick but unsafe, and 8% that they believe physical banking is quick but unsafe. 6% of respondents indicated that they thought traditional branch banking was a quick and secure choice.

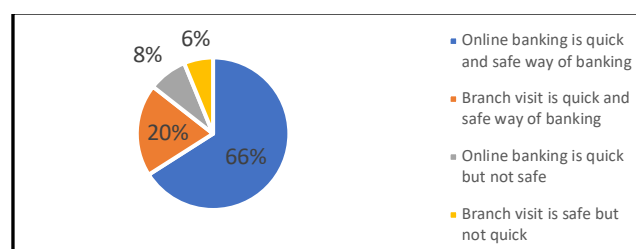


Figure 4. Respondents' views on different forms of banking

Devices used for digital banking.

When the researcher asked the respondents about the different devices they use for on-line/internet banking, their responses are shown in Fig. 5. Respondents were given the chance to choose from a variety of answers for this research question, indicating their preferred methods of carrying out banking tasks.

Ninety percent (90%) of respondents said they use smartphones for digital banking, compared to 24% who said they use ATMs, which are typically found in bank branches and other designated locations. Twenty percent (20%) said they use laptops, and 3% said they use desktops. Smartphones appeared to be the most popular device for digital banking, with a total of 90% of respondents choosing this option.

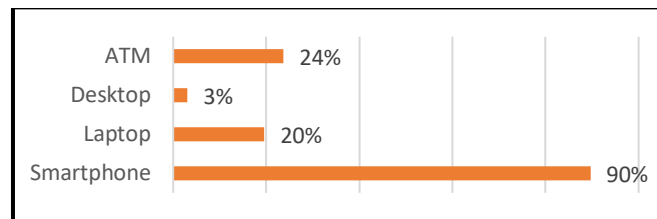


Figure 5. Devices used for digital banking

Activities users perform using digital banking services.

Figure 6 illustrates the respondents' replies to a question about the various digital banking activities they frequently engage in. For this query, respondents were allowed to choose from a variety of possibilities.

Sixty-four percent 64% of respondents indicated that they use digital banking services to transfer money between bank accounts while 58% that they use these services to make purchases on-line (also known as on-line shopping), 48% said that they use these services to check their account balances, 44% said that they use them to pay their bills, and 12% said that they use them for other tasks that they must perform.

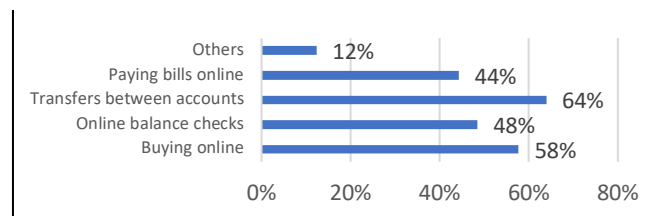


Figure 6. Activities users perform using digital banking services

Concerns with using on-line/internet Banking services.

The researcher was interested in hearing the respondents' reservations about using digital banking services from their perspective. The respondents' responses are shown on Fig. 7. Thirty-eight percent (38%) of respondents said they were concerned about someone having access to their devices and misusing funds and banking information while 36% were worried about someone getting access to their devices remotely and misusing funds and banking information. Nineteen percent (19%) were concerned with a possibility of banking staff accessing their banking details and using it fraudulently while 12% were concerned about other factors not included on the options.

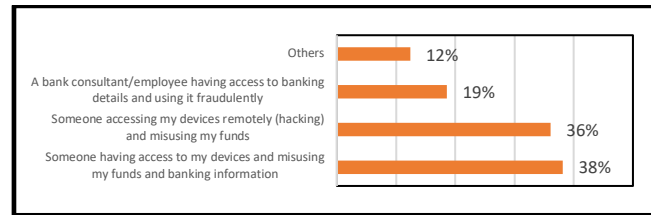


Figure 7. Respondents concerns with using on-line/internet banking services

Preventive factors to the use of digital banking services

One of the objectives of this study was to understand respondents' perspectives about some of the challenges they run into when using on-line/internet banking services, which could occasionally cause them to become wholly hesitant to use them or occasionally cause some users to stop utilizing the services. This offers an insight into how widely these financial services are used by residents and what, if anything, banks might modify to improve the user experience for users in the rural town under investigation and, potentially, all users in the Eastern Cape province and, eventually, the entire country.

Introduction to use of on-line/internet Banking services.

When asked if bank consultants had given them the concept of on-line/internet banking, the respondents' responses are shown in Fig. 7, fifty-one percent (51%) of the respondents said bank consultants introduced them to utilizing these services while 49% said they were self-taught and learned about these services on their own.

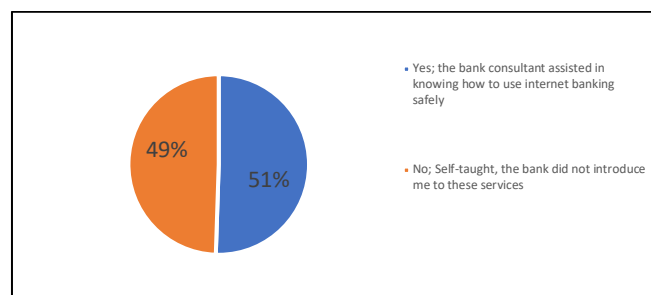


Figure. 8. Respondents' introduction to use of on-line/internet banking services

Experience with using on-line/ internet Banking services.

Referring to Fig. 8, when asked about their experience using on-line/internet banking services, 74% of the respondents said they had a positive experience and found the platforms to be user-friendly, while 16% said they only understood the basics of the transactions they frequently made and did not know much about the platforms, 7% said they had nothing to add about their experience with the platforms, and 3% said they had a negative experience, as they find these platforms hard to use and understand.

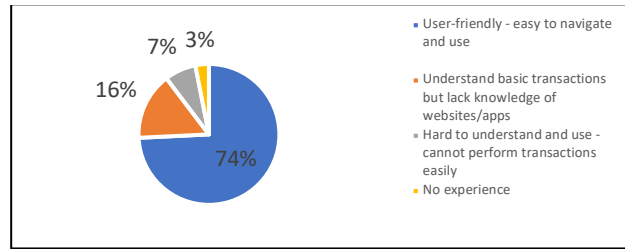


Figure 9. Respondents experience with using digital banking services

Factors affecting the use of on-line/internet Banking services.

The factors influencing the adoption and use of digital banking services in the residential zones were a question the researcher posed to the respondents based on their perspective. Fig. 10 presents their responses.

According to the statistics in the figure, 32% of the respondents indicated that network connectivity is one of the barriers preventing the use and acceptance of digital banking services in their community. However, 28% of these residents claimed that their devices are not compatible with the banking systems while 27% of respondents complained about not having data or airtime. Lastly, 13% said that there are still more obstacles other than the ones considered that prevent residents from using digital banking services.

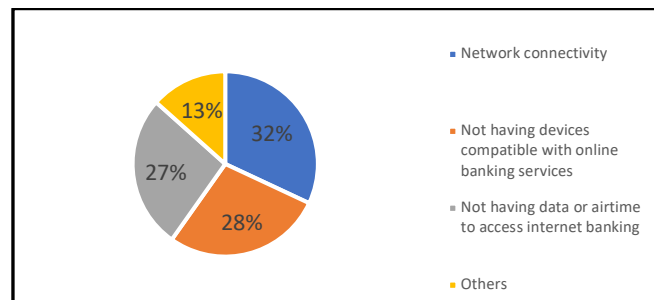


Figure 10. Factors affecting the use of on-line/internet banking services

How Banking services are used

When using digital banking services, user behaviour is crucial since it protects users from any threats to their banking information. This is the users' responsibility, so it was critical to comprehend the safeguards they take to prevent their information from being misused.

Disclosure of personal Banking information.

The respondents were asked about sharing their personal financial data, including CVV numbers, passwords, and card numbers, in relation to the safe and secure usage of digital banking services.

In Fig. 11, 64% of the respondents agreed that they do not share this information with anyone and that it is kept a secret while 28% said they do and occasionally share their personal banking information, and 8% said were neutral on the manner they share information.

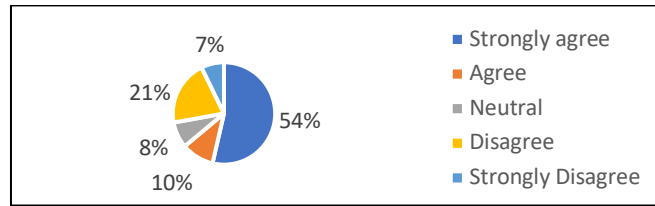


Figure 11. Respondents disclosing of personal banking information

Utilization of digital banking services safely and securely.

When asked if they had ever shared their information or made an electronic payment on websites, emails, SMS, or other forms that they didn't trust, the respondents' replies are shown in Fig. 12.

According to their responses, 59% of the respondents agreed that they had never used websites or shared their information on websites they don't trust while 32% said they may have or might find themselves in such situations, and 9% were neutral about sharing their banking information in situations they didn't trust.

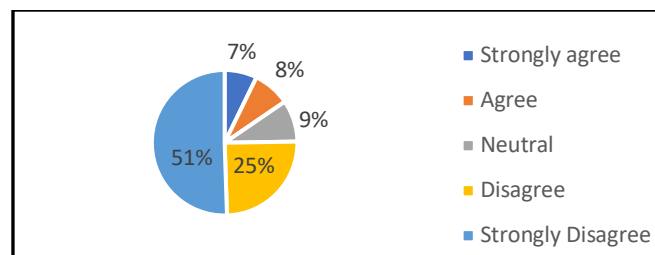


Figure 12. Utilization of banking services safely and securely

E. Discussion

The results of this research highlight the significant impact digital banking has on promoting financial inclusion in rural communities of South Africa. The findings align with existing literature emphasizing the transformative possibilities of digital financial services in historically neglected regions [44], [45]. The dominance of smartphones as the primary platform for accessing digital banking services aligns with studies showing the role of mobile technology in overcoming geographical and infrastructural challenges [39].

Adoption factors and behavioural trends

The study observed high levels of digital banking adoption, with 97% of respondents owning bank accounts and 42% preferring online banking. These adoption rates are driven by services such as money transfers, online purchasing, and credit settlements, aligning with literature highlighting convenience and lower transaction costs [42]. However, security concerns persist, as 38% of respondents fear unauthorized access to their accounts, and 36% worry about remote hacking. This contrast underscores the need to address the behavioral and psychological aspects of adoption, as suggested by [6].

The skewed gender representation in the sample (65% female) presents a limitation, as it may affect the generalizability of findings. Moreover, the shift toward digital banking among younger and middle-aged individuals reflects the influence of age and digital skills on technology usage. Expanding digital literacy initiatives targeting older demographics could further broaden adoption.

Difficulties in Awareness of information security

A problem in users' understanding of information security remains a critical concern, with many respondents highlighting risks such as unauthorized access, data breaches, and fraudulent activities by bank staff (19%). These findings echo global concerns about cybersecurity risks [52], including phishing and hacking. While 64% of respondents follow secure habits, a significant minority engages in risky behaviors, such as sharing passwords or using unsecured platforms. This emphasizes the necessity for enhanced training programmes and awareness campaigns, consistent with suggestions in the literature [51].

Structural and infrastructural obstacles

The results highlight key infrastructural issues such as network connectivity problems (32%), incompatible devices (28%), and high data costs (27%), which align with earlier research identifying the digital divide as a continuing obstacle in rural areas [17], [49]. Addressing these issues requires collaborative solutions among governments, financial organizations, and technology providers to enhance infrastructure and broaden access to affordable internet [78],[79].

Furthermore, even with technological progress such as biometric authentication and encryption, perceived threats persist in obstructing adoption. These results are supported by studies highlighting the importance of transparent privacy policies and consumer trust [34].

Implications for policy and practice

The results of this study indicate numerous practical implications for policymakers and financial organizations. Firstly, there is an urgent requirement to enhance digital literacy initiatives, especially in rural regions, to provide users with the abilities and understanding needed to safely operate digital banking services. This corresponds with international best practices that emphasize education and awareness as essential elements of cybersecurity strategies [25, 26].

Secondly, financial organizations should improve user experience by streamlining digital banking interfaces and offering multilingual assistance to cater to varied user demographics. This might alleviate worries regarding usability and boost adoption levels among groups with low technical skills [50]. Thirdly, collaborations among banks, telecommunications companies, and government bodies might assist in subsidizing internet expenses and enhancing network coverage, thus tackling the infrastructural limitations recognized in this research.

Ultimately, building trust in digital banking demands a comprehensive strategy that merges technological advancements, like blockchain for safe transactions, with clear communication regarding data security policies. Financial institutions can

foster and maintain consumer trust by showing their dedication to protecting user data, which is essential for the enduring success of digital banking efforts [19].

F. Conclusion

This research emphasizes the major progress achieved in embracing digital banking services in rural South African areas, driven by the ease of access and convenience provided by mobile and internet banking. However, the results also uncover significant obstacles that impede the complete fulfilment of digital banking's ability to enhance financial inclusion and economic empowerment. These obstacles, such as a lack of awareness about information security, skepticism towards digital platforms, and infrastructural issues like network access and cost, illustrate a wider story reflected in the research on digital banking adoption in developing areas.

The study confirms that digital banking provides various advantages, such as greater financial inclusion, lowered transaction expenses, and increased efficiency in financial services. However, these advantages are not equally shared, especially among groups with lesser digital skills and technological access. The results highlight the necessity for customized approaches to meet the unique requirements of these groups, guaranteeing fair access to digital financial services.

The research further emphasizes the ongoing issues related to cybersecurity with 36% of respondents expressing concerns about hacking and 38% fearing unauthorized access. Although numerous users have embraced secure methods, a considerable segment continues to be at risk from threats like phishing, hacking, and social engineering. These weaknesses not only put individual users at risk of monetary loss but also present reputational threats for financial organizations. The study results confirm the importance of comprehensive cybersecurity measures, user education, and transparent communication to promote trust and confidence in digital platforms.

The research also highlights the ongoing issues related to cybersecurity. Although numerous users have embraced secure methods, a large segment still faces risks from threats like phishing, hacking, and social engineering. These vulnerabilities not only put individual users at risk of financial loss but also present reputational threats for financial institutions. These findings underscore the necessity of thorough cybersecurity practices, educating users, and clear communication to build trust and assurance in digital platforms.

G. References

- [1] D. Hanandini, 'Social Transformation in Modern Society: A Literature Review on the Role of Technology in Social Interaction', *Jurnal Ilmiah Ekotrans & Erudisi*, vol. 4, no. 1, pp. 82–95, Jun. 2024, doi: 10.69989/j0m6cg84.
- [2] G. Abashidze, 'Unveiling The Digital Economy: How Digitization Transforms Economic Structures', *Innovative economics and management*, vol. 11, no. 1, pp. 17–26, Mar. 2024, doi: 10.46361/2449-2604.11.1.2024.17-26.

- [3] Omar Al-Kasasbeh, 'The Transformation of the Economy: Exploring the Impacts and Opportunities of the Digital Economy', *ORGANIZE: Journal of Economics, Management and Finance*, vol. 3, no. 1, pp. 10–17, Feb. 2024, doi: 10.58355/organize.v3i1.75.
- [4] E. Indriasari, H. Prabowo, F. L. Gaol, and B. Purwandari, 'Digital Banking', *International Journal of E-Business Research*, vol. 18, no. 1, pp. 1–20, Sep. 2022, doi: 10.4018/IJEER.309398.
- [5] R. Babin and D. Smith, 'Open banking and regulation: Please advise the government', *Journal of Information Technology Teaching Cases*, vol. 12, no. 2, 2022, doi: 10.1177/20438869221082316.
- [6] T. S. Szopiński, 'Factors affecting the adoption of online banking in Poland', *J Bus Res*, vol. 69, no. 11, pp. 4763–4768, Nov. 2016, doi: 10.1016/j.jbusres.2016.04.027.
- [7] PWC, 'Payments 2025 & beyond', Pwc, 2021.
- [8] African Union, 'The Digital Transformation Strategy for Africa (2020-2030)', *Science and Technology Progress and Countermeasures (Chinese)*, 2020.
- [9] SARB, 'The national payment system framework and strategy: Vision 2025', 2018.
- [10] S. Ogawa, P. Khera, S. Ng, and R. Sahay, 'Is Digital Financial Inclusion Unlocking Growth?', *SSRN Electronic Journal*, 2022, doi: 10.2139/ssrn.4026364.
- [11] E. Sardianou, A. Stauropoulou, K. Evangelinos, and I. Nikolaou, 'A materiality analysis framework to assess sustainable development goals of banking sector through sustainability reports', *Sustain Prod Consum*, vol. 27, 2021, doi: 10.1016/j.spc.2021.04.020.
- [12] StatsSA, *Sustainable Development Goals: Country Report 2023*. Statistics South Africa, 2023. [Online]. Available: www.statssa.gov.za/info@statssa.gov.za,Tel+27123108911
- [13] A. Tarhini, C. Mgbemena, M. S. A. Trab, and R. Masa'deh, 'User adoption of Online Banking in Nigeria: A Qualitative Study', *Journal of Internet Banking and Commerce*, vol. 20, no. 3, 2015, doi: 10.4172/1204-5357.1000132.
- [14] M. Z. Salem, S. Baidoun, and G. Walsh, 'Factors affecting Palestinian customers use of online banking services', *Int. J. Bank Mark.*, vol. 37, no. 2, p. 426 451, 2019.
- [15] A. A. Alalwan, Y. K. Dwivedi, and N. P. Rana, 'Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust', *Int J Inf Manage*, vol. 37, no. 3, pp. 99–110, Jun. 2017, doi: 10.1016/j.ijinfomgt.2017.01.002.
- [16] S. Jain and J. P. Sahu, 'Banking the unbanked: exploring the impact of internet penetration on accessibility to banking services in developed and developing economies', *Digital Policy, Regulation and Governance*, Jul. 2024, doi: 10.1108/DPRG-02-2024-0021.
- [17] A. Botta, A. Fjer, E. Gold, N. Amaah, N. A. Ofusu-Amaah, and E. Seshie, 'The future of payments in Africa | McKinsey', *McKinsey & Company*, no. September, 2022.
- [18] P. J. Marshall, 'Online Banking: Information Security vs. Hackers Research Paper', *Int J Sci Eng Res*, vol. 1, no. 1, pp. 1–5, 2010, doi: 10.14299/ijser.2010.01.001.

- [19] T. Maurer and A. Nelson, 'The Global Cyber Threat', *Finance Dev*, vol. 58, no. 1, 2021.
- [20] Nadim Jahangir and Noorjahan Begum, 'The role of perceived usefulness, perceived ease of use, security and privacy, and customer attitude to engender customer adaptation in the context of electronic banking', *African Journal of Business Management*, vol. 2, no. . 032-040, 2008.
- [21] M. Musinga, M. M. Eloff, and J. H. Kroeze, 'System usability scale evaluation of online banking services: A South African study', *S. Afr. J.*, vol. 114, 2018.
- [22] Adedoyin Tolulope Oyewole, Chinwe Chinazo Okoye, Onyeka Chrisantus Ofodile, and Chinonye Esther Ugochukwu, 'Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio', *World Journal of Advanced Research and Reviews*, vol. 21, no. 3, pp. 625–643, Mar. 2024, doi: 10.30574/wjarr.2024.21.3.0707.
- [23] K. Raghavendra, 'CHALLENGES IN SECURING BANKING SYSTEMS: EMERGING TRENDS, RISKS, AND DEFENSIVE STRATEGIES', *Int Educ Res J*, vol. 9, no. 8, Jul. 2023.
- [24] Dr. Y. Perwej, S. Qamar Abbas, J. Pratap Dixit, Dr. N. Akhtar, and A. Kumar Jaiswal, 'A Systematic Literature Review on the Cyber Security', *International Journal of Scientific Research and Management*, vol. 9, no. 12, pp. 669–710, Dec. 2021, doi: 10.18535/ijstrm/v9i12.ec04.
- [25] M. N. Kondratyeva, D. D. Svirina, and A. I. Tsvetkov, 'The role of information technologies in ensuring banking security', *IOP Conf Ser Mater Sci Eng*, vol. 1047, no. 1, p. 012069, Feb. 2021, doi: 10.1088/1757-899X/1047/1/012069.
- [26] K. R. Pundareeka Vittala, S. S. Ahmad, R. Seranmadevi, and A. K. Tyagi, 'Emerging Technology Adoption and Applications for Modern Society Towards Providing Smart Banking Solutions', 2024, pp. 315–329. doi: 10.4018/979-8-3693-5261-8.ch018.
- [27] D. Z. Al Balqa, N. Gharaibeh, and N. Zanoon, 'The Impact of Customer Knowledge on the Security of E-Banking', *Nabeel Zanoon Natheer Gharaibeh Int. J. Comput. Sci. Secur.*, no, vol. 7, p. 2013, 2013.
- [28] J. Rupal and R. Singh, 'Evaluating the Impact of E-Banking on Customer Satisfaction: A Comprehensive Systematic Review', *AiBi Revista de Investigación, Administración e Ingeniería*, vol. 11, no. 3, pp. 115–125, Sep. 2023, doi: 10.15649/2346030X.3375.
- [29] R. Yazdanifard, W. F. Wanyusoff, A. C. Behora, and A. B. Sade, 'Electronic banking fraud; The need to enhance security and customer trust in online banking', *Advances in Information Sciences and Service Sciences*, vol. 3, no. 10, pp. 505–509, 2011, doi: 10.4156/AISS.vol3.issue10.61.
- [30] V. Wang, H. Nnaji, and J. Jung, 'Internet banking in Nigeria: Cyber security breaches, practices and capability', *Int. J.*, vol. 62, 2020.
- [31] T. Onunka, A. Raji, A. Nkemchor Osafiele, C. Daraojimba, B. Afeyokalo Egbokhaebho, and C. Chinazo Okoye, 'BANKING: A COMPREHENSIVE REVIEW OF THE EVOLUTION AND IMPACT OF INNOVATIVE BANKING SERVICES ON ENTREPRENEURIAL GROWTH', *Economic Growth and Environment Sustainability*, vol. 2, no. 2, pp. 66–78, 2023, doi: 10.26480/egnes.02.2023.66.78.

- [32] S. P. Vilhena and R. Navas, 'THE IMPACT OF COVID-19 ON DIGITAL BANKING', *Journal of Entrepreneurial Researchers*, vol. 1, no. 1, pp. 21–42, Jul. 2023, doi: 10.29073/jer.v1i1.11.
- [33] R. Zhu, 'Customer Awareness of Internet Banking Security in China', *Fourteenth Wuhan International Conference on E-Business*, pp. 391–399, 2015.
- [34] M. Terlizzi, L. Brandimarte, and O. Sanchez, 'Replication of Internet Privacy Concerns in the Mobile Banking Context', *AIS Transactions on Replication Research*, vol. 5, pp. 1–18, 2019, doi: 10.17705/1attr.00040.
- [35] M. Terlizzi, L. Brandimarte, and O. Sanchez, 'Replication of Internet Privacy Concerns in the Mobile Banking Context', *AIS Transactions on Replication Research*, vol. 5, pp. 1–18, 2019, doi: 10.17705/1attr.00040.
- [36] A.-S. Oertzen and G. Odekerken-Schröder, 'Achieving continued usage in online banking: a post-adoption study', *International Journal of Bank Marketing*, vol. 37, no. 6, pp. 1394–1418, Sep. 2019, doi: 10.1108/IJBM-09-2018-0239.
- [37] A. M. Selase and A. Benedict, 'An assessment of customer attitude towards internet banking in Ghana', *Int. J. Econ. Bus. Manag. Res.*, vol. 5, no. 5, no. 07, p. 2021, 2010.
- [38] R. Hernández-Murillo, G. Llobet, and R. Fuentes, 'Strategic online banking adoption', *J Bank Financ*, vol. 34, no. 7, pp. 1650–1663, 2010, doi: 10.1016/j.jbankfin.2010.03.011.
- [39] A. Sharma, A. Mohan, A. Johri, and M. Asif, 'Determinants of fintech adoption in agrarian economy: Study of UTAUT extension model in reference to developing economies', *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 10, no. 2, p. 100273, Jun. 2024, doi: 10.1016/j.joitmc.2024.100273.
- [40] Banking Association South Africa, 'Banking Association South Africa'. Accessed: Dec. 31, 2024. [Online]. Available: <https://www.banking.org.za/>
- [41] L. Grzybowski, V. Lindlacher, and O. Mothobi, 'Mobile money and financial inclusion in Sub-Saharan Africa', *Information Economics and Policy*, vol. 65, p. 101064, Dec. 2023, doi: 10.1016/j.infoecopol.2023.101064.
- [42] A. Demirgüç-Kunt, L. Klapper, D. Singer, and S. Ansar, *The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19*. World Bank Publications, 2022.
- [43] W. Jack and T. Suri, 'Risk Sharing and Transactions Costs: Evidence from Kenya's Mobile Money Revolution', *American Economic Review*, vol. 104, no. 1, pp. 183–223, Jan. 2014, doi: 10.1257/aer.104.1.183.
- [44] H. Sharma and S. Aggarwal, 'Study on Digital Banking Financial Services in India: Trends, Opportunities & Challenges', 2023.
- [45] S. Klus, N. Łukasiewicz, Z. Urbanowicz, and L. Wanat, 'E-Banking Security Dilemmas Of Users Living In Rural Areas – The Case Of Konin County In Wielkopolska', *Annals of the Polish Association of Agricultural and Agribusiness Economists*, vol. XXIV, no. 1, pp. 115–133, Jan. 2022, doi: 10.5604/01.3001.0015.7102.
- [46] M. O. Richard, 'User Adoption of Online Banking in Kenya: A Qualitative Study', *SSRN Electron. J.*, 2019, doi:, vol. 10., 2019.

- [47] S. Kaur and S. Arora, 'Understanding customers' usage behavior towards online banking services: an integrated risk-benefit framework', *Journal of Financial Services Marketing*, vol. 28, no. 1, pp. 74–98, Mar. 2023, doi: 10.1057/s41264-022-00140-5.
- [48] T. S. Szopiński, 'Factors affecting the adoption of online banking in Poland', *J. Bus. Res.*, vol. 69, no. 11, p. 4763 4768, 2016.
- [49] S. Elhajjar and F. Ouaida, 'An analysis of factors affecting mobile banking adoption', *International Journal of Bank Marketing*, vol. 38, no. 2, pp. 352–367, Jul. 2019, doi: 10.1108/IJBM-02-2019-0055.
- [50] G. Wu and Q. Peng, 'Bridging the Digital Divide: Unraveling the Determinants of FinTech Adoption in Rural Communities', *Sage Open*, vol. 14, no. 1, Jan. 2024, doi: 10.1177/21582440241227770.
- [51] V. Priyadarshini, M. S. Ahmed, R. Sathya, and V. C. Lekha, 'Digital transformation in the banking and financial services among rural users: Disruptive technology acceptance model', 2024, p. 020016. doi: 10.1063/5.0198901.
- [52] N. N. Cele and S. Kwenda, 'Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review', *J Financ Crime*, Apr. 2024, doi: 10.1108/JFC-10-2023-0263.
- [53] C. Kim, W. Tao, N. Shin, and K.-S. Kim, 'An empirical study of customers' perceptions of security and trust in e-payment systems', *Electron Commer Res Appl*, vol. 9, no. 1, pp. 84–95, Jan. 2010, doi: 10.1016/j.elerap.2009.04.014.
- [54] D. Mangala and L. Soni, 'A systematic literature review on frauds in banking sector', *J Financ Crime*, vol. 30, no. 1, pp. 285–301, Jan. 2023, doi: 10.1108/JFC-12-2021-0263.
- [55] M. M. More, M. P. Jadhav, and K. M. Nalawade, 'Online Banking and Cyber Attacks : The Current Scenario', *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 12, p. 743 749, 2015.
- [56] M. Lehto, 'Cyber-Attacks Against Critical Infrastructure', 2022, pp. 3–42. doi: 10.1007/978-3-030-91293-2_1.
- [57] J. Lee, L. Wewege, and M. C. Thomsett, 'Disruptions and Digital Banking Trends', *Journal of Applied Finance & Banking*, vol. 10, no. 6, 2020.
- [58] A. Bouveret, 'Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment', *IMF Working Papers*, vol. 18, no. 143, 2018, doi: 10.5089/9781484360750.001.
- [59] ilker Kara, 'DON'T BITE THE BAIT: PHISHING ATTACK FOR INTERNET BANKING (E-BANKING)', *Journal of Digital Forensics, Security and Law*, vol. 16, no. 2, Nov. 2021, doi: 10.58940/1558-7223.1743.
- [60] Chandra sekhar and M. Kumar, 'An Overview of Cyber Security in Digital Banking Sector', *East Asian Journal of Multidisciplinary Research*, vol. 2, no. 1, pp. 43–52, Jan. 2023, doi: 10.55927/eajmr.v2i1.1671.
- [61] D. Airehrour, N. Vasudevan Nair, and S. Madanian, 'Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model', *Information*, vol. 9, no. 5, p. 110, May 2018, doi: 10.3390/info9050110.

- [62] R. Ranjan and S. Ness, 'Cyber security Threats to Cloud Banking Systems', *International Journal of Research Publication and Reviews*, vol. 5, no. 10, pp. 1698–1698, Oct. 2024, doi: 10.55248/gengpi.5.1024.2837.
- [63] M. A. Sasse, S. Brostoff, and D. Weirich, 'Transforming the "Weakest Link" — a Human/Computer Interaction Approach to Usable and Effective Security', *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, 2001, doi: 10.1023/A:1011902718709.
- [64] N. P. Matlala, 'Behavioural Insights Into Cybersecurity Practices Among Digital Banking Consumers in South Africa', *Indonesian Journal of Business Analytics*, vol. 3, no. 4, pp. 1425–1442, Sep. 2023, doi: 10.55927/ijba.v3i4.5515.
- [65] J. Goh et al., 'Cyber Risk Surveillance: A Case Study of Singapore', *SSRN Electronic Journal*, 2021, doi: 10.2139/ssrn.3545291.
- [66] S. Giri, 'Cloud Computing and Data Security Challenges: A Nepal Case', *International Journal of Computer Trends & Technology*, vol. 67, no. 3, 2019, doi: 10.14445/22312803/ijctt-v67i3p128.
- [67] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, 'A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions', *Electronics (Basel)*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.
- [68] J. Phiri, T. Lavhengwa, and M. A. Segooa, 'Online banking fraud detection: A comparative study of cases from South Africa and Spain', *S Afr J Inf Manag*, vol. 26, no. 1, Mar. 2024, doi: 10.4102/sajim.v26i1.1763.
- [69] A. J. P. Lazar et al., 'Analysing the User Actions and Location for Identifying Online Scam in Internet Banking on Cloud', *Wirel Pers Commun*, 2021, doi: 10.1007/s11277-021-08585-y.
- [70] M. J. Hossain Faruk, M. Tasnim, H. Shahriar, M. Valero, A. Rahman, and F. Wu, 'Investigating Novel Approaches to Defend Software Supply Chain Attacks', in *Proceedings - 2022 IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2022*, 2022, doi: 10.1109/ISSREW55968.2022.00081.
- [71] S. Waelchli and Y. Walter, 'Reducing the risk of social engineering attacks using SOAR measures in a real world environment: A case study', *Comput Secur*, vol. 148, p. 104137, Jan. 2025, doi: 10.1016/j.cose.2024.104137.
- [72] H. Alshaikh, N. Ramadan, and H. Ahmed, 'Ransomware Prevention and Mitigation Techniques', *Int J Comput Appl*, vol. 177, no. 40, pp. 31–39, Feb. 2020, doi: 10.5120/ijca2020919899.
- [73] J. Singh, 'Comprehensive Solution to Mitigate the Cyber-attacks in Cloud Computing', *International Journal of Cyber-Security and Digital Forensics*, vol. 3, no. 2, pp. 84–92, 2014, doi: 10.17781/P001294.
- [74] K. C. Archana and N. Harini, 'Mitigation of Spoofing Attacks on IOT Home Networks', *Int J Eng Adv Technol*, vol. 9, no. 1s, pp. 240–245, Dec. 2019, doi: 10.35940/ijeat.A1047.1091S19.
- [75] V. Hnamte and J. Hussain, 'Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation', *Telematics and Informatics Reports*, vol. 14, p. 100129, Jun. 2024, doi: 10.1016/j.teler.2024.100129.

- [76] O. E. Akinbowale, M. P. Mashigo, and M. F. Zerihun, 'Fraud investigation and mitigation', in Understanding and mitigating cyberfraud in Africa, AVARSITY Books, 2024, pp. 19–46. doi: 10.4102/aosis.2024.BK485.02.
- [77] N. L. Piquero, A. R. Piquero, S. Gies, B. Green, A. Bobnis, and E. Velasquez, 'Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders', Vict Offender, vol. 16, no. 3, pp. 444–463, Apr. 2021, doi: 10.1080/15564886.2020.1826023.
- [78] G. Mwansa, "Promoting adoption and utilization of cloud computing services for agile software developers," Journal on Innovation and Sustainability RISUS, 2023. <https://doi.org/10.23925/2179-3565.2023v14i3p138-150>.
- [79] Dyongo, A.B., Mwansa, G. (2022). Investigating the Effectiveness of Zero-Rated Website on Students on E-Learning. In: Jacob, I.J., Kolandapalayam Shanmugam, S., Bestak, R. (eds) Expert Clouds and Applications. Lecture Notes in Networks and Systems, vol 444. Springer, Singapore. https://doi.org/10.1007/978-981-19-2500-9_56