International Journal of Computer Applications Technology and Research
Volume 12–Issue 08, 99 – 112, 2023, ISSN:-2319–8656
DOI:10.7753/IJCATR1208.1014

Enhancing Security Measures for Mobile Banking Applications: A Comprehensive Analysis of Threats, Vulnerabilities, and Countermeasures in Kenya Banking Industry

George N. Wainaina
Mr.
School of Science Engineering and Technology,
Kabarak University, Box: 20157
Nakuru, Kenya.

Denis K. Kiyeng
Mr.
School of Science Engineering and Technology,
Kabarak University, Box: 20157
Nakuru, Kenya.

Nelson Masese
Dr.
School of Science Engineering and Technology,
Kabarak University, Box: 20157
Nakuru, Kenya.

Abstract:

This study focused on the risks and vulnerabilities associated with mobile banking apps in the Kenyan banking sector. While these apps offer convenience and accessibility, they are also exposed to various threats that can compromise user information and financial transactions. The study aimed to identify these risks, vulnerabilities, and attack routes specific to Kenyan mobile banking apps and provide remedies to enhance their security. The research had three main goals. Firstly, it seek to examine and evaluate the primary vulnerabilities and attack vectors affecting Kenyan mobile banking apps and understand their impact on user data and financial transactions. Secondly, it aimed to assess the common flaws in these apps, considering both technological issues and user behavior patterns. Lastly, it aimed to propose appropriate security measures customized for the Kenyan banking sector, considering user behavior and technological advancements. This included exploring encryption, multi-factor authentication, and user awareness programs to promote secure banking habits. The research intended to assist financial institutions and customers in enhancing the security of their mobile banking experiences by conducting a thorough assessment of risks and vulnerabilities in Kenyan mobile banking apps and offering practical advice. It emphasized the importance of understanding and addressing the specific challenges faced by the Kenyan banking sector to ensure secure and reliable financial transactions through mobile platforms.

Keywords: Mobile banking apps, Cybersecurity, Threat actors, Malware, Phishing, Social engineering, man-in-the-middle attacks, Vulnerabilities, Countermeasures, User behavior patterns.

1. Introduction

Mobile banking apps have simplified and streamlined financial transactions. These apps let users check account balances, transfer money, pay bills, and apply for loans on their smartphones, transforming bank interactions. Smartphones and mobile internet access have made mobile banking services essential to the financial landscape (Shaikh et al., 2022). Mobile banking apps provide many advantages but pose hazards and obstacles. The quick speed of technological improvements has opened new opportunities for innovation and enhanced user experiences, but it has also uncovered weaknesses that malevolent actors may exploit. Financial organizations and customers now worry about mobile banking app security. Advanced hacks threaten user data and financial transactions on mobile banking apps. Data from mobile banking apps is stolen through malware, phishing, social engineering, and man-in-the-middle attacks (Cinar & Kara, 2023).

Such breaches can result from financial losses, identity theft, and bank-client distrust. Given the importance of mobile banking apps and the rising frequency and complexity of cyber-attacks, a complete examination of the Kenyan banking industry's risks, vulnerabilities, and responses is urgently needed.

Kenyans are increasingly using mobile banking apps for their financial demands (Misati et al., 2022). Thus, financial institutions and clients must comprehend the Kenyan banking industry's particular issues and find appropriate security measures. This study examines Kenyan mobile banking applications' dangers and attack vectors and how they exploit vulnerabilities to compromise user data and financial transactions. It also identified mobile banking apps' most prevalent vulnerabilities, including software defects, architectural weaknesses, and user behavior and awareness. Effective countermeasures and security measures may be created and executed by identifying the difficulties in limiting risks and improving Kenyan mobile banking application security.

A comprehensive analysis of threats, vulnerabilities, and countermeasures in mobile banking applications is essential to ensure the security, privacy, and integrity of financial transactions worldwide. By understanding the evolving threat landscape and implementing effective security measures, the banking industry can protect sensitive user information and maintain customer trust.

Recent research conducted in the field of mobile banking security has addressed several key aspects. For instance, a study by Suh, Lee, and Lee (2020) examined the effectiveness of various authentication methods in mobile banking applications, highlighting the importance of user-friendly yet secure authentication mechanisms.

In terms of vulnerabilities, researchers have explored areas such as secure coding practices, encryption techniques, and threat intelligence sharing. A study by Chang, Leu, and Chen (2021) investigated the impact of secure coding practices on mobile banking application security, emphasizing the significance of adopting secure coding guidelines and conducting regular code reviews. To combat emerging threats, financial institutions and app developers have implemented various countermeasures. For instance, the use of advanced analytics and machine learning algorithms has shown promise in detecting and preventing fraudulent activities in mobile banking (Huang et al., 2021).

Looking ahead, it is crucial to stay abreast of the latest developments in mobile banking security. Ongoing research and industry collaborations aim to identify emerging threats, vulnerabilities, and best practices. Keeping up with current research findings and incorporating them into security strategies will be vital for maintaining a strong security posture in the ever-evolving landscape of mobile banking applications.

1.1 Problem Statement

The Kenyan banking industry has witnessed a significant shift towards mobile banking applications, enabling customers to conduct financial transactions anytime and anywhere. However, this digital transformation brings inherent risks, as cybercriminals are continually evolving their tactics to exploit vulnerabilities in mobile banking applications. The increasing sophistication of threats and the potential compromise of user data and financial transactions pose a considerable challenge to the security of these applications (Cinar & Kara, 2023). Therefore, it is crucial to identify the primary threats, vulnerabilities, and attack vectors specific to the Kenyan banking industry to devise effective countermeasures and enhance the security of mobile banking applications.

1.2 Study Objectives

i. To identify and assess Kenyan mobile banking applications' main dangers and attack vectors.
ii. To assess the most common vulnerabilities in mobile banking applications used in Kenya, considering both technical and human factors.
iii. To offer appropriate security and countermeasures for Kenya's mobile banking apps.

2. Literature Review.

2.1 Mobile Banking

The fashion of using movable electronic devices, such as smartphones and tablets, to execute fiscal deals and access banking services is known as mobile banking. Checking account balances, transferring money, paying bills, and indeed remote check depositing are common aspects of mobile banking. Mobile banking's security is a major problem, despite the convenience it offers. None of the evaluated mobile banking applications offered an appropriate degree of safety, according to a study by Positive Technologies (Saprikis et al., 2022). The study looked at 14 fully functional mobile banking apps for Android and iOS, with the requirement that they be accessible through official app stores and have at least 500,000 downloads (Li et al., 2022). Based on the effects of a hypothetical attack on user data and the program itself, the vulnerability risk was evaluated.

According to the survey, 13 out of 14 mobile banking applications on the client side—that is, the application that is downloaded and installed on a user's device—allow attackers to access customer data. Without administrator rights, more than a third of vulnerabilities may be exploited. Compared to Android clients, iOS client applications often have fewer security flaws. However, 100% of mobile banking clients have flaws in their code, such as a lack of obfuscation and a lack of safeguards against code injection and repackaging (Muhammad et al., 2023).

Insecure deep link handling and the existence of sensitive data in the client-side file system of roughly half of the programs are two additional serious vulnerabilities that have been found. Banks may experience financial losses as a result of these vulnerabilities, and sensitive user data like card numbers and account balances may also be stolen.

Furthermore, problems such as a lack of certificate pinning to authenticate SSL certificates were discovered to make 13 out of 14 applications vulnerable to man-in-the-middle attacks. The majority of the vulnerabilities were on the server side, which is a web application that communicates with the mobile client via the internet and had 54% of all vulnerabilities (Shahid et al., 2022). Half of mobile banks were vulnerable to fraud and money theft, with each having an average of 23 server-side vulnerabilities. One third of banks had card information in danger, and five out of seven allowed hackers to acquire user passwords. Furthermore, none of the server sides had a security level higher than "medium," and more than half of mobile banks had high-risk server-side vulnerabilities.

2.1.1 Mobile Banking in Kenya

By allowing unprecedented levels of financial inclusion, mobile banking has transformed Kenya's financial environment. Kenya's financial system currently heavily relies on Safaricom's mobile money network, M-Pesa. Users of M-Pesa may easily deposit, withdraw, transfer, and pay for goods and services using a mobile device; these capabilities have significantly aided Kenyans in being financially included 8k account, and a sizable fraction of these people utilize mobile banking services like M-Pesa (Mulili, 2022).

The significance of M-Pesa goes beyond merely offering fundamental financial services. Additionally, it has aided in the growth of online lending platforms that provide microloans to previously unbanked or underbanked Kenyans (Mulili, 2022). These platforms allow Kenyans to obtain loans and other financial services through a new channel by using mobile data to assess creditworthiness. The widespread usage of M-Pesa has sparked a variety of innovations in other fields, such as health, agriculture, and energy, changing Kenya's socioeconomic environment. However, a further in-depth study is required on the specific effects of M-Pesa on these industries and the Kenyan economy as a whole.

Kenyan mobile banking applications, like those used globally, are vulnerable to many kinds of cyber-attacks in terms of security (Njenga & Muganda, 2021). Common vulnerabilities include unsecured direct object references, insecure communication, and inadequate data protection. When a user's input determines whether a program should have direct access to an object, this is known as an insecure direct object reference. Attackers can thereby circumvent authentication and gain direct access to data. On the other side, insecure communication occurs when data is transferred via a network without sufficient encryption, leaving it open to interception. Unauthorized access to data that is at rest, in use, or in transit is protected by insufficient data protection. Developers must use secure communication protocols, make sure certificates are validated correctly, and use secure application design to reduce these risks (Cinar & Kara, 2023). Despite these difficulties, mobile banking has the potential to be beneficial, especially in enhancing financial inclusion, making it a crucial area for ongoing growth and investment.

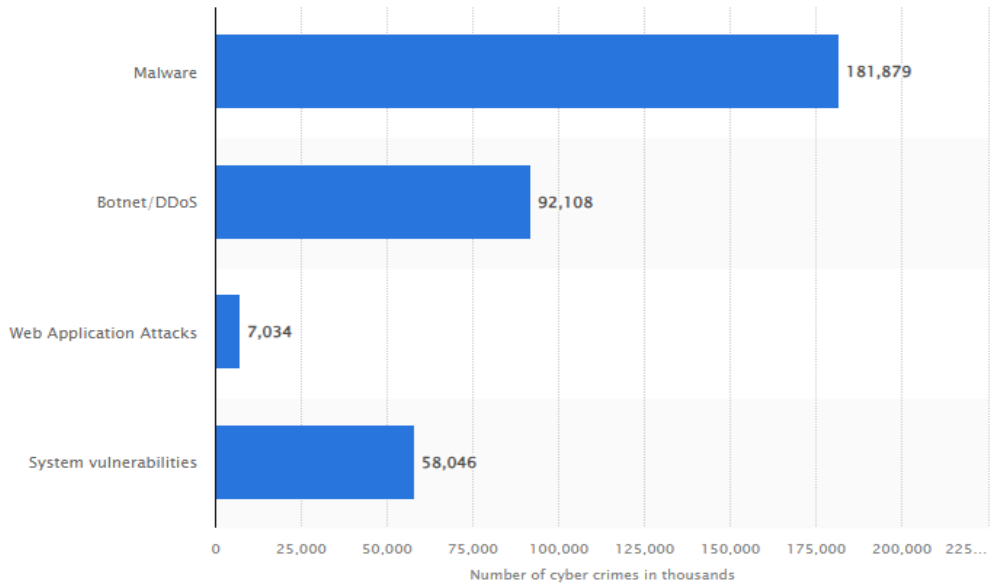


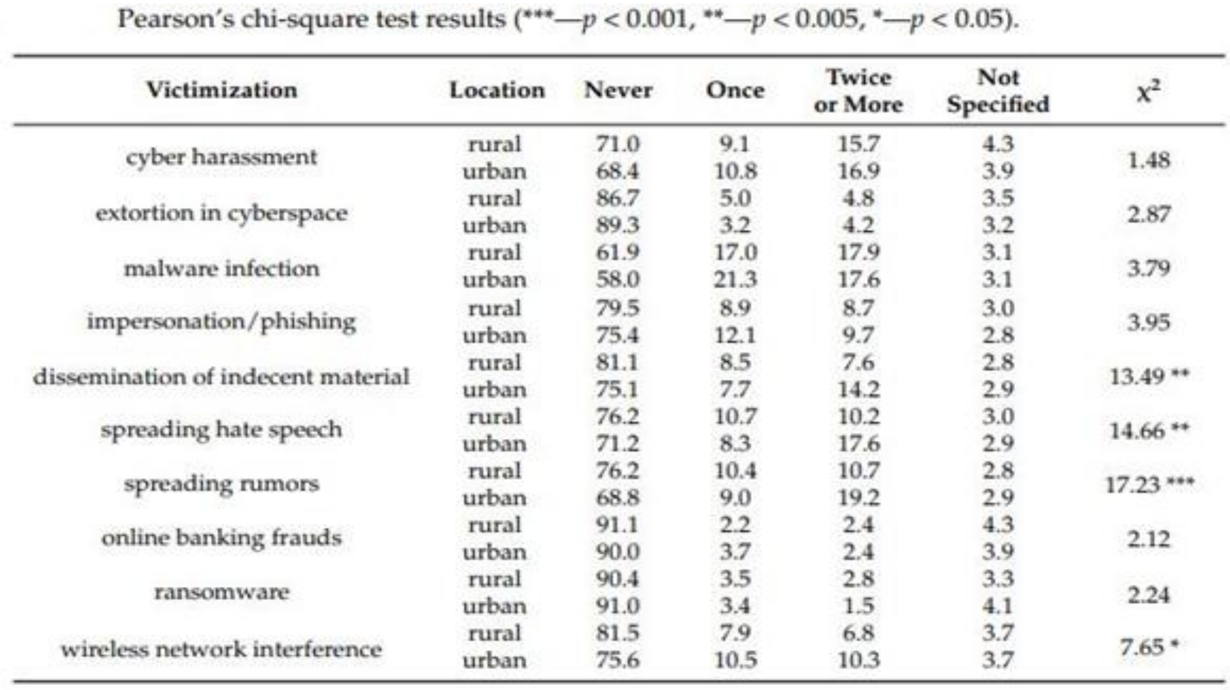
Figure 1: Number of online crimes reported in Kenya. Source, (Baron, 2021)

2.2 Cybersecurity Threats and Vulnerabilities in Mobile Banking.

Mobile banking applications are vulnerable to a range of cybersecurity risks and flaws that might be used by bad actors. In 2020 research by Positive Technologies, which looked at 14 fully functional mobile banking applications, it was shown that none provided an adequate degree of security (Positive Technologies, 2023).

The analysis discovered that these programs have flaws on both the client and server sides. Attackers were able to access customer data in 13 out of the 14 tested applications on the client side, which is the term for the mobile banking app that is installed on a user's device (Positive Technologies, 2023). In 76% of situations, these flaws could be exploited without requiring physical access to the device, and more than a third of them could be used without administrator (jailbreak or root) rights (Akpan et al., 2022).

In terms of individual flaws, improper deep link handling was one of the most hazardous ones found in Android applications. Attackers can use these deep connections to carry out harmful actions, including loading a webpage with malicious code and interacting with the JavaScript APIs of the application (Arogundade et al., 2023). Inadequate code protection was another flaw that might allow attackers to decompile the application's code and obtain sensitive information, including encryption keys and passwords. Each mobile bank had an average of 28% of cyber threats and Ransom malware vulnerabilities composed 50.2% (Bernik, 2022). The server side is a web application that communicates with the mobile client via the internet. Potential fraud, financial theft, and user credential theft were some of the threats linked to these vulnerabilities.



Pearson's chi-square test results (***—$p < 0.001$, **—$p < 0.005$, *—$p < 0.05$).

Victimization	Location	Never	Once	Twice or More	Not Specified	x^2
cyber harassment	rural	71.0	9.1	15.7	4.3	1.48
	urban	68.4	10.8	16.9	3.9	
extortion in cyberspace	rural	86.7	5.0	4.8	3.5	2.87
	urban	89.3	3.2	4.2	3.2	
malware infection	rural	61.9	17.0	17.9	3.1	3.79
	urban	58.0	21.3	17.6	3.1	
impersonation/phishing	rural	79.5	8.9	8.7	3.0	3.95
	urban	75.4	12.1	9.7	2.8	
dissemination of indecent material	rural	81.1	8.5	7.6	2.8	13.49 **
	urban	75.1	7.7	14.2	2.9	
spreading hate speech	rural	76.2	10.7	10.2	3.0	14.66 **
	urban	71.2	8.3	17.6	2.9	
spreading rumors	rural	76.2	10.4	10.7	2.8	17.23 ***
	urban	68.8	9.0	19.2	2.9	
online banking frauds	rural	91.1	2.2	2.4	4.3	2.12
	urban	90.0	3.7	2.4	3.9	
ransomware	rural	90.4	3.5	2.8	3.3	2.24
	urban	91.0	3.4	1.5	4.1	
wireless network interference	rural	81.5	7.9	6.8	3.7	7.65 *
	urban	75.6	10.5	10.3	3.7	

Figure 2: Cybercrime victimization categories. Source (Bernik et al., 2022).

2.3 Cybersecurity in Kenya.

Kenya has given substantial attention to cybersecurity. In August 2022, the Kenyan government released its National Cybersecurity Strategy, which serves as a guide for dealing with emerging cyberthreats (Kondlo et al., 2022). To coordinate multi-agency activities for cybercrime detection, prohibition, prevention, response, investigation, and prosecution, the strategy, which is in accordance with the Computer Misuse and Cybercrimes Act of 2018 (CMCA 2018), was developed (Khan et al., 2022). The development of strong governance structures, strong policy, legal, and regulatory frameworks, protection of crucial information infrastructure, development of more advanced capabilities and a skilled cybersecurity workforce, reduction of crimes and incidents, and promotion of cooperation and collaboration are the six main pillars that support the strategy.

The National Cybersecurity Strategy (NCS) 2020–2023 was developed by the Kenyan government to increase the country's cybersecurity readiness. Plans are presented for establishing a National Cyber Command Center, improving the legal and regulatory landscape, encouraging research and innovation, and strengthening expertise and competence in cybersecurity-related matters (Pavel, 2023). Cyberthreats are the most common type of vulnerabilities encountered by majority of the victims in Kenya. Cybercriminals are increasingly focusing their attacks on small organizations such as banks at prevalence rate of 43%, taking advantage of a lack of security knowledge and fundamental protection measures (Pawar et al., 2022).

According to the research, phishing, banking Trojans, and fraud involving ATMs are the most typical sorts of assaults, and the financial sector is the one that is most frequently targeted in Kenya (Maluleke, 2023). Due to their extensive use across the nation, mobile money services are also being targeted more frequently. The research does, however, point out various issues with Kenya's Cybersecurity environment. These include a large shortage of Cybersecurity experts, limited financing for initiatives, and lax enforcement of rules and laws relating to the field. Kenya's Cybersecurity capacity maturity is evaluated in 2021 research by the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford (GCSCC, 2021). The report rates a nation's level of Cybersecurity maturity using a five-stage model (from start-up to dynamic). Kenya received a "formative" grade across the board, meaning that while efforts are being made in these areas, they are not systematic, extensive, or part of a larger national plan. According to user behavior and awareness, the Serina research contends that internet users in Kenya have a low degree of Cybersecurity knowledge (David et al., 2022). According to the research, more needs to be done to inform people and companies about cyber threats and how to be safe online.

Through numerous efforts, the MPESA app in Kenya has proved its dedication to safety, making it a trustworthy and secure mobile money transfer platform. To begin, the app employs strong encryption techniques to safeguard user information and financial transactions, ensuring that personal information stays protected and secure. MPESA has also adopted multi-factor authentication, which requires users to provide additional verification procedures in order to access their accounts, preventing unwanted access (Mugo, 2023). The software also provides real-time transaction notifications, allowing users to spot and report any suspicious activity as soon as it occurs. Furthermore, MPESA works with regulatory organizations and financial institutions to adhere to high compliance standards and anti-money laundering legislation, which improves the platform's security.

Given the wide use of mobile banking services in Kenya, this study's conclusion that there's a considerable threat involved with using mobile banking operations is material. The results should be taken cautiously in the Kenyan context because the study did not explicitly examine Kenyan banking applications.

2.4 Security Measures and Countermeasures in Mobile Banking.

Over time, mobile banking has expanded significantly, and with that expansion have come more potential dangers and weaknesses. Encryption, multi-factor authentication, secure software development methods, and stoner mindfulness programs are just a few of the remedies that have been created and put into place to lessen these troubles (Mugo, 2023). Information or data is converted into a law through the process of encryption to help prevent unauthorized access. In the environment of mobile banking, encryption may be used to guard both data at rest (stored data) and data in conveyance (data being transferred).

For example, mobile banking operations generally employ the cryptographic protocols Safe Sockets Layer (SSL) and Transport Layer Security (TLS) to enable safe communication across a computer network (Muhammadovich, 2023).

These protocols cipher the data being transmitted between the stoner's mobile device and the bank's servers to make it harder for bushwhackers to block and crack the data.

2.5 Cybersecurity in Kenya.

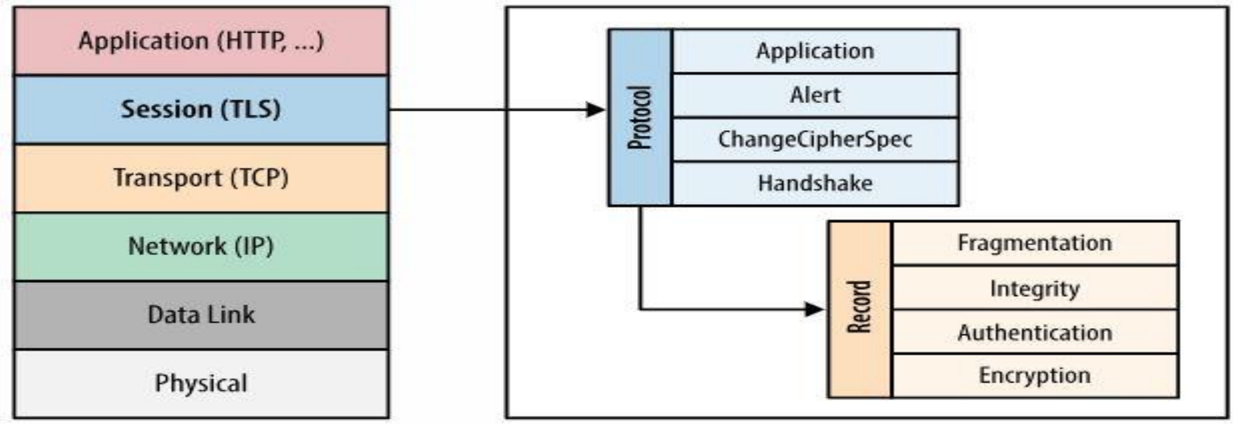


Figure 3: Transport Layer Security (TLS). Source. (Grigorik, 2023)

Multi-Factor Authentication (MFA) MFA is an authentication type that requires the stoner to provide two or more verification factors before giving access to a resource, similar to an online account or an These rudiments constantly include what the person performs (similar to a biometric point), what they retain (similar to a mobile device or a palpable commemorative), and what they know (similar to a word) (Suleski et al., 2023). By requiring several pieces of identity, MFA adds an extra layer of security, making it harder for unauthorized users to get access even if one element, like a password, is stolen (Taherdoost, n.d.). Implementing safe software development techniques is essential for avoiding vulnerabilities in mobile banking applications (Cinar & Kara, 2023).

In order to do this, security concerns must be included at each stage of the software development lifecycle. For instance, to find and address any security problems, developers should regularly do security testing, code reviews, and vulnerability assessments. Also, they should follow the concept of least privilege, ensuring that programs and processes have just the access they require.

Despite the finest technical defenses, the human factor still plays a big role in the security of mobile banking. Initiatives to increase user knowledge and education are therefore crucial. Users should be educated about the dangers of mobile banking and trained to recognize and stay clear of possible hazards like phishing scams (Mamolo, 2022).

They should be urged to adopt safe practices, including routine software updates, strong passwords, and only downloading programs from reputable websites.

These precautions would be very useful for the Kenyan banking sector, which, like many others, is struggling with the security issues posed by the quick uptake of mobile banking (Suleski et al., 2023). The nation's banks ought to research these best practices and put them into effect, always keeping in mind the particular context of their operations and clients. The security of mobile banking in the nation might also be improved by partnering with other players in the cybersecurity ecosystem and regulatory bodies.

2.6 Gap in Literature.

The analysis of the literature indicates a variety of security techniques and defenses used in mobile banking throughout the world. End-to-end encryption is recognized as a key element of safe mobile banking (Len et al., 2023). It guarantees that sensitive information sent across the network, including login passwords, account details, and transaction data, cannot be intercepted or read by unauthorized parties. The importance of multi-factor authentication as one of the security measures included in digital banking has also been acknowledged (Suleski et al., 2023). This technique combines something you have (a device or object) with something you are (a biometric) or something you know (a secret), creating a strong security layer that is less likely to be compromised by attackers and hackers.

These technologies have a lot of promise, but they also have a lot of drawbacks. For instance, users may overlook security precautions due to multi-factor authentication's hassle, leaving the system more open to infiltration (Pöhn et al., 2023). These methods have some potential, but there are several issues. Due to the inconvenience of establishing multi-factor authentication, for instance, customers may decide to take shortcuts, thereby increasing the vulnerability of the system.

The analysis also identifies blockchain technology as a potential future approach that might be utilized to develop a large-scale transaction system for banking that is more safe, practical, and effective. The research demonstrates a sizable gap in the context of the Kenyan banking industry, notwithstanding these developments. While worldwide trends are a good place to start, there is a distinct absence of in-depth studies focusing on the dangers, weaknesses, and defenses related to mobile banking apps inside the Kenyan banking sector.

It is crucial to perform localized research because of Kenya's distinctive socioeconomic and technical environment. The goal of this research is to not only identify the precise dangers and weaknesses that Kenya's banking sector is subject to but also to develop security measures and responses that are specifically tailored to the regional environment. By doing so, the sector may increase the impact of these initiatives while avoiding any possible drawbacks for the user experience.

3. Research Methodology.

This study uses a mixed-methods methodology, integrating qualitative and quantitative techniques, to provide a thorough knowledge of the possible security concerns in Kenyan mobile banking apps. Stages for data gathering and analysis are included in the process.

3.1 Data Collection.

3.1.1 Secondary Data Collection.

Secondary data is collected via a review of existing literature. The aim is to develop an understanding of the broader context as well as identify key trends and patterns in the field of mobile banking application security. This review includes scholarly articles, cybersecurity reports, regulatory documents, and relevant case studies. Secondary data will be extremely important to this study since it will give a thorough and complete knowledge of the security of mobile banking applications. This research will gain important insights into the larger context and major developments in the sector by a thorough assessment of the available literature, which includes scientific publications, cybersecurity reports, regulatory documents, and pertinent case studies. The researchers will be able to draw on the knowledge and discoveries of other researchers through the study of secondary data, enabling a more in-depth investigation of the research issue. This study will be able to enrich its analysis, strengthen its arguments, and produce solid and insightful conclusions by combining secondary data with the primary research findings, such as semi-structured interviews with cybersecurity experts, users of mobile banking apps, and law enforcement personnel.

4. Data Analysis.

The data analysis strategy will be modified as this study only uses secondary data sources. Thematic analysis will be used heavily in the study to evaluate the qualitative data gleaned from the studied literature. We will identify and analyze the main themes, trends, and patterns associated with the risks and shortcomings of Kenyan mobile banking applications. The replies of participants from the literature might be examined to get fresh perspectives and comprehensions.

In addition to theme analysis, statistical methods will be used to examine any quantitative information from the secondary sources that is accessible. This research attempts to characterize and investigate the general patterns and trends in the data, including the prevalence of certain vulnerabilities in mobile banking applications as well as the frequency and diversity of cyberthreats. The study can offer a quantitative viewpoint that supports the qualitative findings by using statistical analysis.

5. Way Forward for the Banking Sector in Kenya.

Like in many developing nations, Kenya's banking industry is going through a dramatic shift that is mostly driven by digital technology. Particularly with regard to mobile banking, this development has increased the potential for financial inclusion but also raised several security issues (World Bank, 2017). In view of these events, the following proposals are made regarding Kenya's banking system's future:

As the financial industry becomes more digital, security must be a top priority. Institutions must invest in innovative safety measures to safeguard their systems and customer data from cyberattacks. This necessitates the use of security solutions like end-to-end encryption and multi-factor authentication, as well as regular security audits to detect and fix any possible problems.

Enhance human awareness and education: It's important to inform clients about safe online banking habits because many security breaches are caused by human mistakes. Banks should create user awareness campaigns that educate people about issues including phishing scams, secure password usage, and the value of protecting personal devices.

Promote financial inclusion by reaching marginalized people who might not have access to regular banking services through mobile banking. To make their mobile banking systems more accessible and user-friendly, especially for consumers in rural regions or those who might not be tech-savvy, banks should continue to develop and improve them.

Create Regulatory Frameworks: The regulatory frameworks that control the banking industry should grow along with it. Regulators must keep up with the most recent advancements in digital banking and adjust their policies and procedures accordingly. This covers laws governing digital financial services, client data privacy, and cybersecurity.

Examine Emerging Technologies: The banking sector has to be open to investigating emerging technologies that might boost the safety and efficiency of their products. For instance, blockchain technology has the power to totally alter how payments are conducted and recorded, increasing security and openness.

Localize study and solutions: As was already said, little study has been done explicitly in the Kenyan setting. To fully comprehend the distinct difficulties and possibilities confronting the Kenyan banking sector going forward, further regionalized study will be required. The creation of specialized solutions that address the unique requirements and environment of the Kenyan market may then be guided by the study.

6. Conclusion.

Mobile banking security measures have significantly advanced over time as slice-edge technology is employed to ensure the secure processing of sensitive data. One of the crucial rudiments of safe mobile banking is end-to-end encryption, which encrypts all connections between a mobile device and a banking server.

This fashion prevents unauthorized parties from interdicting or reading sensitive data being transmitted over the network, such as login watchwords, regard information, and sale data.

Multi-factor authentication has been stressed as a pivotal security element in the environment of digital banking, coupled with encryption.

To log into a digital bank account, this approach combines a number of factors, similar to the stoner's knowledge (for example, a secret), their identity (for example, a biometric), or their power. Multi-factor authentication greatly lowers the chance of successful intrusions by offering robust authentication.

However, just as the technical environment is still developing, cybercriminals' risks are also growing. To keep up with these dangers, banks must constantly develop and modify their security measures. One innovative method that could offer transactions that are more effective, convenient, and secure is the combination of blockchain technology and multiple-factor authentication. Future research and development in this area have a ton of room.

Although security mechanisms have improved, it's important to keep in mind that no system is impervious entirely. Users must thus be aware of and follow suggested security procedures, including routine password changes, staying away from unsafe Wi-Fi networks, and not installing dubious applications. The entire security of mobile banking depends on the joint efforts of the banks in putting in place strong security measures and the users in abiding by safe practices.

7. References

[1] Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, *2*(1), 123-138.

[2] Arogundade, O. R. (2023). Network Security Concepts, Dangers, and Defense Best Practical. *Computer Engineering and Intelligent Systems*, *14*(2).

[3] Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks across Different Industries and Organization Types. *International Journal of Business Intelligence and Big Data Analytics*, *6*(1), 1-11.

[4] Baron, C. (2021). *Number of online crimes reported in Kenya as of 2021, by type*. Statista. https://www.statista.com/statistics/1278773/number-of-online-crimes-reported-in-kenya-by-type/

[5] Bernik, I., Prislan, K., & Mihelič, A. (2022). Country Life in the Digital Era: Comparison of Technology Use and Cybercrime Victimization between Residents of Rural and Urban Environments in Slovenia. *Sustainability*, *14*(21), 14487.

[6] Cinar, A. C., & Kara, T. B. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. *Multimedia Tools and Applications*, 1-13.

[7] Cinar, A. C., & Kara, T. B. (2023). The current state and future of mobile security in the light of the recent mobile security threat reports. *Multimedia Tools and Applications*, 1-13.

[8] David, F., Walsh, K., Jones, L., Sutton, S., & Opuda, E. (2022). What works to prevent online

violence against children: Executive summary.

[9] Grigorik. I. (2023). *High Performance. Browser Networking*. https://hpbn.co/transport-layer-security-tls/

[10] Hamid, K., Iqbal, M. W., Muhammad, H. A. B., Fuzail, Z., Ghafoor, Z. T., & Ahmad, S. (2022). Usability evaluation of mobile banking applications in digital business as emerging economy. *International Journal of Computer Science and Network Security*, *22*(1), 250-260.

[11] Khan, S., Saleh, T., Dorasamy, M., Khan, N., Leng, O. T. S., & Vergara, R. G. (2022). A systematic literature review on cybercrime legislation. *F1000Research*, *11*(971), 971.

[12] Kondlo, A., Leenen, L., & van Vuuren, J. J. (2022, June). An Ontological Model for a National Cyber-Attack Response in South Africa. In *ECCWS 2022 21st European Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited.

[13] Len, J., Ghosh, E., Grubbs, P., & Rösler, P. (2023). Interoperability in End-to-End Encrypted Messaging. *Cryptology ePrint Archive*.

[14] Li, T., Xia, T., Wang, H., Tu, Z., Tarkoma, S., Han, Z., & Hui, P. (2022). Smartphone app usage analysis: datasets, methods, and applications. *IEEE Communications Surveys & Tutorials*.

[15] Maluleke, W. (2023). Exploring Cybercrime: An Emerging Phenomenon and Associated Challenges in Africa. *International Journal of Social Science Research and Review*, *6*(6), 223-243.

[16] Mamolo, L. A. (2022). Students' evaluation and learning experience on the utilization of Digital Interactive Math Comics (DIMaC) mobile app. *Advances in Mobile Learning Educational Research*, *2*(2), 375-388.

[17] Ministry of Information Communication and Technology, Republic of Kenya. (2022). National Cybersecurity Strategy. https://ict.go.ke/

[18] Misati, R., Osoro, J., Odongo, M., & Abdul, F. (2022). Does digital financial innovation enhance financial deepening and growth in Kenya? *International Journal of Emerging Markets*, (ahead-of-print).

[19] Mugo, C. (2023). Fintech-driven Financial Inclusion and Consumer Protection: Kenya’s Case Study. *Colins Mugo,‘Fintech-driven Financial Inclusion and Consumer Protection: Kenya’s Case Study’(January, 2023) Issue*, *84*.

[20] Muhammad, Z., Anwar, Z., Javed, A. R., Saleem, B., Abbas, S., & Gadekallu, T. R. (2023). Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, Side-Channel Attacks, Google Play Attacks, and Defenses. *Technologies*, *11*(3), 76.

[21] Muhammadovich, N. M. (2023). The need to implement cryptographic information protection tools in the operating system and existing

solutions. *Central Asian Journal Of Mathematical Theory And Computer Sciences*, *4*(3), 1-4.

[22] Mulili, B. M. (2022). Digital Financial Inclusion: M-PESA in Kenya. In *Digital Business in Africa: Social Media and Related Technologies* (pp. 171-191). Cham: Springer International Publishing.

[23] Njenga, C. K., & Muganda, M. A. (2021). Security Analysis of Mobile Banking Apps in Kenya. *International Journal of Computer Science and Information Security, 19*(3), 103-116

[24] Pavel, T. (2023). National Cyber Policies Attitude Toward Digital Privacy. *Regulating Cyber Technologies: Privacy Vs Security*, 111.

[25] Pawar, S., & Palivela, H. (2022). LCCI: a framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights, 2*(1), 100080.

[26] Pöhn, D., Seeber, S., & Hommel, W. (2023). Combining SABSA and Vis4Sec to the Process Framework IdMSecMan to Continuously Improve Identity Management Security in Heterogeneous ICT Infrastructures. *Applied Sciences, 13*(4), 2349.

[27] Positive Technologies. (2023, June 1). *Cybersecurity Threats and Vulnerabilities in Mobile Banking.* Retrieved from https://www.bizjournals.com/seattle/news/2023/06/05/cybersecurity-what-business-leaders-need-know.html

[28] Rob. (2023, March 31). The Importance of End-to-End Encryption in Mobile Banking. MeritLine. https://www.meritline.com/the-importance-of-end-to-end-encryption-in-mobile-banking/

[29] Saprikis, V., Avlogiaris, G., & Katarachia, A. (2022). A comparative study of users versus non-users' behavioral intention towards M-banking apps' adoption. *Information, 13*(1), 30.

[30] Shahid, J., Hameed, M. K., Javed, I. T., Qureshi, K. N., Ali, M., & Crespi, N. (2022). A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. *Applied Sciences*, *12*(8), 4077.

[31] Shaikh, A. A., Alamoudi, H., Alharthi, M., & Glavee-Geo, R. (2022). Advances in mobile financial services: a review of the literature and future research directions. *International Journal of Bank Marketing*, (ahead-of-print).

[32] Suleski, T., Ahmed, M., Yang, W., & Wang, E. (2023). A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health*, *9*, 20552076231177144.

[33] Taherdoost, H. (n.d.). Multi-factor authentication in digital banking. Global Banking & Finance Review. Retrieved June 4, 2023, from https://www.globalbankingandfinance.com/multi-factor-authentication-in-digital-banking