Exploring Mobile Banking App Security from User's Perspectives

Olumide Bashiru Abiola
Beechnet Solutions Limited
Toronto, Canada

Abstract

Organizational support and improved performance have seen unprecedented enhancement due to the ability of internet technology that is constantly changing the ways and procedures for attaining organizational goals. However, given the volume of digital-related transactions today, especially with mobile internet banking systems, cybersecurity threats, and privacy concerns arising from Internet use by businesses, their employees, and external stakeholders have become prevalent. The detrimental effects resulting from cybersecurity threats have an adverse effect on the confidentiality, integrity, and availability of information for banks and users of their mobile banking app services. The users' knowledge of cybersecurity vulnerability hampers their decision-making about adopting mobile banking. This study examines factors that affect cybersecurity and how mobile banking app users perceive cybersecurity issues that may hinder the banks' ability to expand mobile banking usage amongst their customers. Additionally, this study suggests a conceptual research model that illustrates the relationships between the variables that affect cybersecurity. The study discovered that users view knowledge of potential identity theft, impersonation, and account hijacking as cybersecurity threats that impede their use of mobile banking. The review of literature conducted identified that mobile banking app users who regard these concerns to be real are hesitant to embrace mobile banking. Similarly, the knowledge about cybersecurity threats putting mobile banking app users in danger makes them reluctant to use the app for banking purposes. As a result, mobile banking serves as a reminder to strategically reinforce the security and privacy issues in relation to cybercrime in the banking industry. Practically, the survival of banking in the future will depend on the retention of its mobile banking app users. The study contributes to the theory of cybersecurity, particularly in using the Internet as a platform for mobile banking.

1. Introduction

Mobile banking is becoming commonly used as a means of financial transactions globally because of its ease of use and accessibility and how convenient it is to transfer money and manage accounts while on the go [1]. Nevertheless, mobile banking is still in its infancy and has many aspects that could be improved because it depends on non-financial services and technology [2]. Since there are so many different solutions, businesses, and platforms involved, it is more challenging to select not just the appropriate service but also a secure one as technology evolves.

Mobile banking users are more vulnerable than ever because of the increasing sophistication of cybercriminals [3]. Data from the mobile banking industry revealed that approximately one in twenty fraudulent attempts occurs through the use of malicious apps by mobile app users [4]. Cybercriminals create and upload rogue apps to top app stores, hoping vulnerable users will download them. It can be challenging to know if an app is from a reliable source or if it is just malware that has been deceitfully uploaded online to be downloaded by mobile app users.

This app may ask for payment information and login passwords with the aim of stealing money from victims' bank accounts [5]. The app could grant hackers elevated privileges as super-users, allowing them to control the users' mobile devices altogether. Undeniably, the Internet's exponential expansion has resulted in increased cyberattack incidents, many of which have tragic and distressing outcomes [6].

Even though information and communication technologies (ICTs) have produced exciting new possibilities for participation, cooperation, and transparency, this connectedness and cross-reliance has also resulted in an increase in the level of vulnerability for technology users and a new breed of threats that institutions and society have never faced [7].

The issue this study attempts to solve is that none of the mobile banking apps reviewed in this study had an appropriate level of security. Also, mobile phone users make errors that enable hackers to get around authentication, authorization processes, and user passwords by ignoring security recommendations not to store confidential information in plaintext on mobile devices. Due to these mistakes, mobile banking apps run the risk of sensitive user data, including credit card numbers and personal information, being stolen or fraudulently obtained.

The purpose of this study is to add to the body of knowledge already available about mobile banking

 | DOI: 10.20533/ijisr.2042.4639.2023.0122

vulnerabilities. Our knowledge of the perceptions of vulnerabilities in mobile banking apps will be increased by conducting a quantitative study that includes interviews with bank executives. This study intends to increase interest in developing a framework that will aid in designing and developing mobile banking apps with reduced vulnerabilities and add theoretical insight to the literature.

2. Literature Review

The introduction of Internet banking and associated technologies significantly improved banks' capability to offer their mobile banking app users great services [8]. Mobile banking app users may now access their banks whenever they want. They can access their account details, get bank statements, carry out banking transactions, including money transfers to other accounts [9], and pay their bills while lounging comfortably in their homes or offices.

The Internet has significantly impacted banks and other financial institutions by enabling mobile app users to access a wide variety of banking services around the clock [8, 10]. Additionally, it considerably reduced bank costs, online banking is the least-priced delivery option for banks [11]. The wireless technology and the capability to access numerous banking services from mobile phones without geographical or time limitations offer banks' mobile banking users a wider choice of value-added mobile banking services [12].

Mobile banking has had a significant positive impact on many banks because its average transaction cost is lower than that of traditional banks [13]. Banks have also been able to grow their market share and more effectively comprehend and meet the banking needs of their clients by analyzing the data acquired from the use of connected devices by their consumers [14].

There are several advantages for banking mobile app users, such as cost and time savings associated with not having to travel to the bank branch for transactions [15]. Mobile banking allows customers to access their bank accounts through cell phones and other portable devices so they may check their balances and make purchases. Due to its 24-hour operation, flexibility to do banking almost anywhere, and the variety of services offered via mobile gadgets, the number of mobile banking users is projected to increase [16]. It was predicted that mobile banking will surpass online banking as the preferred banking channel by the year 2020. Mobile banking app users can access capabilities through mobile banking that are unavailable online, such as person-to-person payments and remote check deposits [17].

Despite the increased financial performance mobile banking brought to the bank [15], there has not been a significant improvement in the level of security for mobile banking services [18], especially when it comes to the authentication methods that have replaced usernames and passwords with new ones like digital IDs and biometrics [19]. Mobile banking is becoming common, but mobile app users' security threats and worries are still an issue [20]. Along with assuring user authentication and protection, numerous encryption methods are required to protect the personal information of mobile banking app users [21].

Identity theft and fraud are two examples of the outcome when hackers infiltrate weak networks [22]. Identity fraud occurs when imposters use the personal details of a victim to open a false account [23], engage in deceitful transactions or withdrawals, or attempt to acquire services using their victim’s information [24]. Identity theft or compromise occurs when a victim's personal information is exposed to a third party without the victim's consent.

Since all internet transactions, including mobile banking, require some form of account-holder authentication, the vulnerability in mobile banking systems would most likely be triggered on the user's end or device, since banks and network providers typically have more secure procedures [25]. While focusing on the necessity for users to be aware of the potential risks they are exposed to by smartphones, Barth, de Jong [26] did not distinguish between attacks and self-inflicts due to user ignorance.

Banking customers may decide not to use mobile banking systems because they believe they cannot prevent direct and indirect online intruders or dangers. The risk of being hacked is the most serious of the many threats to banking security systems [27]. Threat actors or other intrusion sources may uncover the password by accessing the device's log data or temp files [28]. Mobile users frequently store passwords on their mobile devices or in the autofill options of forms, which makes it easy for an unauthorized person to access such passwords. While mobile app users' confidence is declining because of security concerns, uninformed consumers are more likely to be undisturbed by these problems. The effect of cybercriminals and the consequences of cybercrime cannot be managed using any existing paradigm.

2.1. A review of mobile app vulnerabilities

Mobile app vulnerabilities present a pressing issue for mobile banking app users; they can have far-reaching consequences, including breaching sensitive user data, financial losses, and damage to an application's reputation. Inadequate security measures

 | DOI: 10.20533/ijisr.2042.4639.2023.0122

leave 85% of Android and 70% of iOS mobile banking apps vulnerable [29]. Below are some of the well-known mobile app vulnerabilities.

2.1.1. Insecure data storage. Insecure data storage refers to the improper storage of sensitive information, such as login credentials and financial data, which makes it vulnerable to unauthorized access [30]. This vulnerability, at times, has to do with how mobile apps read or write files on smartphones; mobile apps can read or write to internal drives or external drives and can also write to temp files, thus increasing the risk of sensitive data exposure [31]. External drives like SD cards can easily be removed or stolen to access the contents [32].

At the global level, new regulations with enhanced secured processes for mobile devices are being promoted [30]. The following four protections can be employed for better storage security [32]:

a. Prevent the storage of crucial, sensitive data in external storage.
b. Implement monitoring technology and log monitoring data to record hacker activities.
c. Encrypt user data to enhance security.
d. Add an extra layer of permissions to restrict unauthorized access to user data.

However, while secure data storage practices generally recommend encryption, implementing blockchain over traditional encryption is even more secure [33].

2.1.2. Weak authentication. Weak Authentication occurs when the mobile app login process lacks robust security measures; it may be due to vulnerabilities that can be exploited [34]. Inadequate authentication methods, like simple Personal Identification Number (PIN) and weak passwords, can make it easy for attackers to gain unauthorized access. Weak passwords can be guessed easily; hackers can also use brute force to crack passwords [35].

Most mobile app developers still need to catch up in terms of ensuring adequate security measures are integrated with their apps; a study by Lamoyero and Fajana [36] discovered that most of the reviewed apps did not meet industrial standards. Many mobile apps make use of One Time Password (OTP), which is not a match for modern-day hackers [29]; having only one password or one type of authentication is generally categorized to be a weak authentication scheme [37]. To support this, Xu [38] asserted that OTP via SMS is very common but not the safest. Notwithstanding, most banks use the OTP option because it is relatively cheaper than other, more secure options [39]. Furthermore, authentication mainly involves users, and users are the most vulnerable in the mobile application ecosystem [34, 40].

This vulnerability can be mitigated by implementing good authentication standards like strong authentication methods, such as multi-factor authentication (MFA). While MFAs are essential, providing awareness training and implementing robust cryptographic protocols is also highly recommended where applicable [36]. MFAs can be implemented with a combination of processes, including:

a. MFA, OTP, and biometrics [37].
b. A multi-digit security code that relies on digital signatures, hash functions, and various cryptographic technologies [38]
c. USB drive, smart card, SMS verification, and OTP [39]

2.1.3. Phishing and social engineering. Phishing and social engineering are common vulnerabilities where attackers deceive users into revealing sensitive information, such as account credentials or personal data. By posing as a trustworthy entity, the perpetrator's goal is to obtain authenticated data of the user [40]. It can be carried out through emails, text messages, social media, or even fake mobile apps disguised as real ones [35].

Social engineering often does not involve computers [41]; it focuses on human behavior instead of technological methods to bypass bank security [29]. Social engineering poses a significant challenge, primarily because humans tend to have a natural inclination to trust [41]. These attacks share a typical pattern with four steps [41]: target research, getting acquainted with the target, executing the attack, and covering tracks. Social engineering is the cheapest, easiest, most effective, and most successful technique to exploit human error [42].

Phishing, on the other hand, is a social engineering tool, the following are the different types of phishing [40]:

a. Vishing (by telephone conversation)
b. Smishing (by SMS messages)
c. Spear phishing (directed at specific persons)
d. Whaling (directed at organizations' management)
e. Clone phishing (can be directed at a large audience)

To mitigate this vulnerability, banks must deploy policies, processes, awareness programs, training, and technology for customers and staff [42]. The awareness program should warn users about the dangers of downloading from non-secured links except for legitimate app stores like Apple or Google stores [43, 44] and also teach them to recognize phishing attempts [29]. While mitigation is not primarily technology-driven, technology can also be deployed as a support mechanism, such as performing

 | DOI: 10.20533/ijisr.2042.4639.2023.0122

penetration testing at each development phase [43] and deploying anti-phishing tools to block phishing sites [41].

2.1.4. Poor code quality. Poor code quality in mobile apps can result from the absence of good coding practices, leading to code errors or security flaws. These vulnerabilities can open the door to hacking techniques such as buffer overflows, SQL injection, or cross-site scripting [45]. Poor code quality related vulnerabilities are sometimes attributed to app developers' and vendors' rush to go to market with the product without due consideration for security [46].

Developers often make mistakes when they neglect comprehensive testing and validation procedures in the early stages of app development [47]; disregarding code writing standards is the biggest cause of these missteps [45]. Technical debt is sometimes blamed for this, where the developer focuses on meeting project deadlines and ends up writing less-than-optimal codes [48], leading to quality issues. Three causes of these vulnerabilities are [45]:

a. Developers' lack of knowledge of secure coding practices
b. Lack of familiarity with existing code
c. Unintended errors.

To mitigate this risk, app developers must follow secure coding practices, conduct regular security audits, and apply patches to address identified vulnerabilities. Effective code review practices for security flaws should be integrated with the quality assurance process [45]. Preventing security flaws in early development generally has more advantages and is more cost-effective [47]. Senanayake, Kalutarage [46] proposed and implemented a machine-learning technique for identifying and mitigating these types of vulnerabilities.

2.1.5. Outdated software. Outdated Software poses a significant challenge in mobile apps; Outdated software can contain vulnerabilities [44]. When apps and the underlying operating systems are not regularly updated, they become susceptible to exploits. Outdated apps may lack the fixes or patches to mitigate against known security issues [35]. Updates are essential and, if not done, can have security implications [49].

To mitigate this vulnerability, mobile app developers must prioritize timely updates to ensure the latest security patches are applied and vulnerabilities are mitigated. Regular software update is recommended to be included in software maintenance strategies, and such strategies have been shown to impact user adoption [50].

3. Conceptual Model Underpinning

The conceptual model underpinning this study is discussed under the following two headings: cybersecurity management and guidance as it affects the cybersecurity threat of mobile app users.

3.1. Cybersecurity Management

Cybersecurity management is the planning and implementing of security strategies, policies, technologies, and practices to safeguard digital assets. It is a challenge to predict, foresee, and take preventive action promptly, with the assumption that cyber-attacks might hit mobile app users [51]. Due to the lack of a developed cyber security management model that enables a response to cyber-attacks on mobile app users, unexpected scenarios, and vulnerabilities, it is essential to address cyber security issues to protect the user's interests and drive the continuous usage of mobile banking apps. Defenders are always behind attackers in developing new tactics and strategies to prevent cybersecurity attacks. It should be noted that technologic-driven solutions do not entirely solve the problems; critical infrastructure should also have a cyber security management model that is constantly updated to keep up with the changes in technology [52].

Although investing in more advanced security measures helps, cyber security policy must also cover the critical infrastructure investment in resources that can detect threats based on priorities rather than just the latest technology or systems [53]. It is of utmost importance to understand what kind of invaders could be interested in the transactional activities of mobile users and why. Understanding the value of technology assets is also very important so as to estimate the potential impact if compromised.

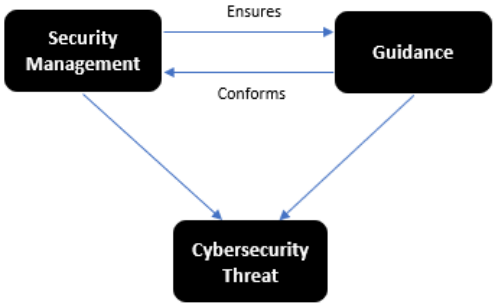

Figure 1. Conceptual research model for handling cybersecurity threats

 | DOI: 10.20533/ijisr.2042.4639.2023.0122

3.2. Guidance

This discussion is on mobile banking app best practices, principles and controls put in place to protect users and avoid security breaches on their mobile devices. Because the human factor is the most vulnerable aspect in the digital ecosystem, cyber safety must be a core and primary goal of every team member within an organization [54]. Modern tools and technology are utilized to fulfill specific security requirements, such as detecting an intruder. However, these controls and tools are crucial and must be implemented in the technical infrastructure as more than technology is needed to guarantee cyber safety [54].

Understanding external developments and trends in cyber security can help banks use these insights to create effective policies and plans for the long-term battle against cybercrime. The foundation of every cyber security strategy must be rooted in ongoing learning and improvement processes. Banks must learn to continuously monitor how risks change over time and proactively prepare for the associated threats.

4. Methodology

The conceptual study is the foundation for implementing the research regarding its present theme. We used a document analytical approach as one of our research approaches to complete our investigation and reach the study's overall goal. The document and its associated themes and analyses can be viewed as a streamlined study process. Still, more significantly, they serve as a great starting point for retrieving an existing and pertinent problem, given the topic's greater range of coverage areas. Due to this, and more specifically, the document (or content) analysis was founded on many scientific manuscripts retrieved from accessible public databases, including SCOPUS, EBSCO, Science Direct, Elsevier, and Google Scholar. We used theme analysis to determine the relationships and conformity of research constructs to gain a deeper understanding. Given the interaction of the current study focus, this approach provides the writers with the benefit of searching for relations and patterns across several connected papers. Despite this, the method provides existing literature with a more comprehensive understanding of cybersecurity threats regarding how mobile app users perceive cybersecurity threats toward mobile banking. As a result, we thought it was appropriate to use document analysis as the study's technique. To achieve the suggested goal of this study, document analysis will present a theme within the context of this study. This study's overarching objective is to conceptualize the research model shown in Figure 1 above. Other researchers agreed and claimed that considering a variety of preexisting literature, a research technique of this sort, such as document analysis, helped to find topics for a given study, thereby extending existing knowledge.

5. Conclusion

The present research conducted a comprehensive literature review; a crucial factor influencing banking mobile app users was identified to be that the awareness of cybersecurity risks significantly impacts their decision to embrace these apps for banking transactions. This revelation opens avenues for further research through qualitative methodologies with a dual approach.

The first part will be extensive interviews with a substantial sample of banking mobile app users. This aims to validate the hypotheses derived from our literature review, providing empirical evidence to strengthen the existing body of knowledge. A clear insight into the users' perspectives, concerns, and behaviors is fundamental to establishing a comprehensive understanding of the impact of cybersecurity awareness on their app usage. The second part will be interviews with key stakeholders such as banking executives and leaders in the banking mobile app development environments, to elucidate strategies for incorporating users' concerns and cybersecurity knowledge into the security models and designs of banking mobile applications.

User awareness training for customers should also be explored as it is an essential element in enhancing the overall security landscape. Proactive steps toward educating users about potential risks and protective measures can contribute significantly to fostering a more secure mobile banking environment. Given the implications of our overall findings, this research can make a valuable contribution to the body of knowledge for mobile banking app security research.

6. References

[1] Karjaluoto, H., A.A. Shaikh, H. Saarijärvi, and S. Saraniemi. (2019). How perceived value drives the use of mobile financial services apps. *International Journal of Information Management*. 47: p. 252-261.

[2] Lim, S.H., D.J. Kim, Y. Hur, and K. Park. (2019). An empirical study of the impacts of perceived security and knowledge on continuous intention to use mobile fintech payment services. *International Journal of Human–Computer Interaction*. 35(10): p. 886-898.

[3] Kangapi, T.M. and E. Chindenga. (2022). Towards a Cybersecurity Culture Framework for Mobile Banking in

 | DOI: 10.20533/ijisr.2042.4639.2023.0122

South Africa. in *2022 IST-Africa Conference (IST-Africa)*. IEEE.

[4] Baesens, B., S. Höppner, and T. Verdonck. (2021). Data engineering for fraud detection. *Decision Support Systems*. 150: p. 113492.

[5] Wazid, M., S. Zeadally, and A.K. Das. (2019). Mobile banking: evolution and threats: malware threats and security solutions. *IEEE Consumer Electronics Magazine*. 8(2): p. 56-60.

[6] Kuzior, A., et al. (2022). Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends. *Journal of Risk and Financial Management*. 15(12): p. 613.

[7] Kumar, R. and R. Goyal. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, 2019. 33: p. 1-48.

[8] Vishnuvardhan, B., B. Manjula, and R. Lakshman Naik. (2020). A study of digital banking: Security issues and challenges. in *Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018*. Springer.

[9] Haralayya, B. (2021). How Digital Banking has brought innovative products and services to India. *Journal of Advanced Research in Quality Control and Management*. 6(1): p. 16-18.

[10] Ho, J.C., C.-G. Wu, C.-S. Lee, and T.-T.T. Pham. (2020). Factors affecting the behavioral intention to adopt mobile banking: An international comparison. *Technology in Society*, 63: p. 101360.

[11] Thusi, P. and D.K. Maduku. (2020). South African millennials' acceptance and use of retail mobile banking apps: An integrated perspective. *Computers in Human Behavior*. 111: p. 106405.

[12] Siyal, A.W., D. Ding, and S. Siyal. (2019). M-banking barriers in Pakistan: a customer perspective of adoption and continuity intention. *Data Technologies and Applications*, 53(1): p. 58-84.

[13] Foroughi, B., M. Iranmanesh, and S.S. Hyun. (2019). Understanding the determinants of mobile banking continuance usage intention. *Journal of Enterprise Information Management*. 32(6): p. 1015-1033.

[14] Li, F., et al. (2021). Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality. *Technology in Society*. 64: p. 101487.

[15] Esmaeili, A., I. Haghgoo, V. Davidavičienė, and I. Meidutė-Kavaliauskienė. (2021). Customer loyalty in mobile banking: Evaluation of perceived risk, relative advantages, and usability factors. *Engineering Economics*. 32(1): p. 70-81.

[16] Hayashi, F. and Y.L. Toh. (2020). Mobile banking use and consumer readiness to benefit from faster payments. *Federal Reserve Bank of Kansas City, Economic Review*.105(1): p. 21-36.

[17] De Leon, M.V., R.P. Atienza, and D. Susilo. (2020). Influence of self-service technology (SST) service quality dimensions as a second-order factor on perceived value and customer satisfaction in a mobile banking application. *Cogent Business & Management*. 7(1): p. 1794241.

[18] Geebren, A., A. Jabbar, and M. Luo. (2021). Examining the role of consumer satisfaction within mobile eco-systems: Evidence from mobile banking services. *Computers in Human Behavior*. 114: p. 106584.

[19] AlHammadi, A.A. and M. Lataifeh. (2022). Examining the influence of national digital identity and smart pass platform on accelerating the processes of digital transformation. in *2022 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*. IEEE.

[20] Tao, C., H. Guo, and Z. Huang. (2020). Identifying security issues for mobile applications based on user review summarization. *Information and Software Technology*, 122: p. 106290.

[21] Ali, G., M.A. Dida, and A. Elikana Sam. (2021). A secure and efficient multi-factor authentication algorithm for mobile money applications. *Future Internet*. 13(12): p. 299.

[22] Chng, S., H.Y. Lu, A. Kumar, and D. Yau. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports*. 5: p. 100167.

[23] Zaeem, R.N. and K.S. Barber. (2021). Economics of Cybercrime: Identity Theft and Fraud, in *Encyclopedia of Cryptography, Security and Privacy*. Springer. p. 1-4.

[24] Whittaker, J. and M. Button. (2020). Understanding pet scams: a case study of advance fee and non-delivery fraud using victims' accounts. Aust. NZJ Criminol. 53 (4), 497–514.

[25] Liu, H., T. Spink, and P. Patras. (2019). Uncovering security vulnerabilities in the belkin wemo home automation ecosystem. in *2019 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE.

[26] Barth, S., et al. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and informatics*. 41: p. 55-69.

[27] Ghelani, D., T.K. Hua, and S.K.R. Koduru. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*.

[28] Tabrizchi, H. and M. Kuchaki Rafsanjani. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*.

 | DOI: 10.20533/ijisr.2042.4639.2023.0122

76(12): p. 9493-9532.

[29] Orucho, D.O., F.M. Awuor, C. Ratemo, and C. Oduor. (2023). Security threats affecting user-data on transit in mobile banking applications: A review.

[30] Schmeelk, S. and L. Tao. (2020). Mobile Software Assurance Informed through Knowledge Graph Construction: The OWASP Threat of Insecure Data Storage. *Journal of Computer Science Research*, 2(2): p. 17-29.

[31] Al-Delayel, S.A. (2022). Security Analysis of Mobile Banking Application in Qatar. *arXiv preprint arXiv:2202.00582*.

[32] Zhang, H., et al. (2019). Protecting Data in Android External Data Storage. in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*.

[33] Musa, H.S., M. Krichen, A.A. Altun, and M. Ammi. (2023). Survey on Blockchain-Based Data Storage Security for Android Mobile Applications. *Sensors*, 23(21): p. 8749.

[34] Rivers, O., Y.-H. Hu, and M. Hoppa. (2020). A Study on Cyber Attacks and Vulnerabilities in Mobile Payment Applications. in *Journal of The Colloquium for Information Systems Security Education*.

[35] Patil, H. and K. Sharma. (2023). Assessing the Landscape of Mobile Data Vulnerabilities: A Comprehensive Review. in *2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES)*.

[36] Lamoyero, Z. and O. Fajana. (2023). Exposed: Critical Vulnerabilities in USSD Banking Authentication Protocols. in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*.

[37] AlRousan, M. and B. Intrigila. (2020). Multi-factor authentication for e-government services using a smartphone application and biometric identity verification. *Journal of Computer Science*, 16(2): p. 217-224.

[38] Xu, R. (2022). Security Enhancement for SMS Verification Code in Mobile Payment. in *2022 11th International Conference of Information and Communication Technology (ICTech)*).

[39] Ozkan, C. and K. Bicakci. (2020). Security Analysis of Mobile Authenticator Applications. in *2020 International Conference on Information Security and Cryptology (ISCTURKEY)*.

[40] Leonov, P.Y., et al. (2021). The Main Social Engineering Techniques Aimed at Hacking Information Systems. in *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*.

[41] Salahdine, F. and N. Kaabouch, Social engineering attacks: A survey. *Future internet*, 2019. 11(4): p. 89.

[42] Arabia-Obedoza, M.R., et al. (2020). Social Engineering Attacks A Reconnaissance Synthesis Analysis. in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*.

[43] Yildirim, N. and A. Varol. (2019). A Research on Security Vulnerabilities in Online and Mobile Banking Systems. in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*.

[44] Rao, B. and S.G. Suvarna (2023). Trust and Security Issues in Mobile Banking and its Effect on Customers. *International Research Journal of Modernization in Engineering Technology and Science*, 5(5).

[45] Fahmawi, T., A. Nabot, I. Jebreen, and A. Al-Qerem. (2024). Exploring Code Vulnerabilities through Code Reviews: An Empirical Study on OpenStack Nova. *Journal of Statistics Applications& Probability. 13, No. 2, 681-689.*

[46] Senanayake, J., et al. (2022). POSTER: Developing Secured Android Applications by Mitigating Code Vulnerabilities with Machine Learning.

[47] Senanayake, J., et al. (2023). Android source code vulnerability detection: a systematic literature review. *ACM Computing Surveys*, 55(9): p. 1-37.

[48] Wilder, G., et al. (2023). An Exploratory Study on the Occurrence of Self-Admitted Technical Debt in Android Apps. in *2023 ACM/IEEE International Conference on Technical Debt (TechDebt)*. IEEE.

[49] Demir, N., T. Urban, K. Wittek, and N. Pohlmann. (2021). Our (in) secure web: understanding update behavior of websites and its impact on security. in *Passive and Active Measurement: 22nd International Conference, PAM 2021, Virtual Event, March 29–April 1, 2021, Proceedings 22*. 2021. Springer.

[50] Rula, J.P., P. Richter, G. Smaragdakis, and A. Berger. (2020). Who's left behind? Measuring Adoption of Application Updates at Scale. in *Proceedings of the ACM Internet Measurement Conference*.

[51] Kure, H.I., et al. (2022). Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. *Neural Computing and Applications*, 34(1): p. 493-514.

[52] Gunduz, M.Z. and R. Das (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks*, 169: p. 107094.

[53] Tvaronavičienė, M., T. Plėta, S. Della Casa, and J. Latvys. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into regional development*, 2(4): p. 802-813.

 | DOI: 10.20533/ijisr.2042.4639.2023.0122

[54] Aldawood, H. and S. Geoff. (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs-Pitfalls and Ongoing Issues. Future Internet Jurnal, 11 (73).

 | DOI: 10.20533/ijisr.2042.4639.2023.0122