Vol 5, Issue 6, June 2025 www.ijesti.com E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

An Evaluation of Security Risks and Data Protection Issues in Mobile Banking Applications

Amit Sahu [1], Dr. Dhirendra Kumar Tripathi [2]

[1, 2] Department of Computer Science, Mansarovar Global University, Sehore, M.P., India.

ABSTRACT

Users now have easy and instantaneous access to banking services, thanks to the fast adoption of mobile banking apps, which has drastically changed the financial services industry. Despite these benefits, there are a growing number of security threats and data protection problems that mobile banking systems face. Users' personal information and financial funds are at grave danger from threats such malware attacks, phishing, illegal access, data leakage, and unsecure communication routes. Data protection problems stemming from the management, storage, and transfer of sensitive customer information are investigated in this research, which also assesses the key security risks linked to mobile banking apps. Regulatory compliance, user knowledge, authentication methods, and encryption techniques are all emphasized in the report as ways to lessen these risks. In order to guarantee confidence, secrecy, and dependability in mobile banking services, this research highlights the need for strong security frameworks by identifying weaknesses and evaluating current protecting measures.

Key Words: *Mobile Banking, Security Risks, Data Protection, Cyber Threats, User Privacy.*

1. INTRODUCTION

In India, banking—a type of financial services—plays a significant role in the economy. As a business, banking is responsible for soliciting savings and rent payments from the public through various channels in order to improve the community's level of living. Banks' capacity to develop new electronic banking services and products is greatly affected by the rapid progress of information and technology. Financial technology encompasses a wide range of financial services that rely on technology. How well management is able to incorporate new technology will dictate how quickly innovations and services are developed. Due to the low-risk nature of Indian culture, banks play a crucial role in protecting the ordinary public's funds from potential risks. The entire process of providing services has changed due to new and quickly growing innovations in information technology and globalization. Progress in each nation's economy may be traced back to its innovative information technology. The banking sector is affected by technological innovation, competitive pressure, and globalization. Modern banking apps have evolved from the traditional brick-and-mortar model into mobile banking, which gives customers the freedom to bank whenever and wherever they choose using their mobile phones. With the simplicity, convenience, and helpful account information it provides, mobile banking has huge potential to increase client base.

When it comes to banking services, it's important to remember that all Indian people may get a wide range of them at affordable costs, thanks to high-quality, technologically sophisticated services that provide great value. An instance of this type of service is mobile banking. Getting every single Indian to use these services is no easy feat. If you want to see if a consumer is eager to accept technologically sophisticated services like mobile banking, you might start with adoption. Primary research that takes this approach might shed light on why Indians aren't interested in mobile banking if these feelings do in fact exist. Government officials should next work to eliminate any obstacles that would hinder this kind of profiteering. Under the banner of "Digital India," the Indian government is presenting itself as a leader in information technology, and thus would ensure the maximum level of adoption of technologically sophisticated networks.

Worldwide, the introduction of several mobile banking applications has changed the game. These programs include ICICI i-Mobile, HDFC Mobile Banking, SBI's YONO App, and countless more. To increase M-Banking's customer acceptance, the Indian government has lent its backing to mobile wallets via collaboration prototypes with many banks. Systematic use of clicks and portals has superseded that of bricks and mortals. Every aspect of banking has been revolutionized by IT, including account opening, processing transactions, record keeping, queue management, and information providing. Thanks to new technology, the bank can now process transactions in real time instead of in batches. Some of the emerging ideas that are changing mass services into personalized ones include automated teller machines, online banking, mobile banking, and plastic money. Thanks to technological advancements, financial institutions have been able to replace real currency with a more convenient, secure, and cost-effective alternative.

Offering financial services using mobile phones has been substantially enhanced by the meteoric rise of mobile communication and wireless technologies. An extraordinary system with enormous promise has the ability to entice a large number of customers to opt for mobile banking. Among the many channels accessible in today's technology age, the mobile banking system is one that stands out as novel and attractive for reaching a wider audience. This paper's objective is to investigate the variables that impact the adoption of m-banking services by Indian customers. Furthermore, the goal is to identify the main factors that have a substantial effect on the desire to use mobile banking.

The bank and its customers both gain from mobile banking, a new technical development. Banks offer services including financial transfers, account data, check book issuing, etc., through Mobile Banking Service, which clients use to contact with banks via mobile phones. Almost every bank in India now has a "Mobile Banking Service." In 2000, HDFC Bank introduced mobile banking to their customers, marking the beginning of a new trend in India. In developed countries, there has been a meteoric rise, with more than 300 million people using mobile banking services.

2. LITERATURE REVIEW

Yahya Imam, Abdullahi et al., (2024) The rapid adoption of fintech is pervasive over the globe. Several regulations that promote cashless banking were recently adopted by the Central Bank of Nigeria (CBN) to encourage increased usage in Nigeria. These days, customers of Nigerian banks may use their mobile banking apps to do much of their everyday banking from anywhere. Few studies have thoroughly assessed the security strengths and hazards of these applications in the literature. Financial fraud, privacy invasions, identity theft, and a general decline in user trust are all possible outcomes of mobile banking apps that lack adequate security measures. In light of this, studies that thoroughly evaluate application security are required. As a result, we listed some of the most widely used mobile banking apps in Nigeria and assessed their security in this study. We used both automatic and human static analysis methodologies to carry out the study. The apps' security was then assessed using a multi-criteria decision-making approach. The majority of apps suffer from several security issues caused by vulnerabilities and unsafe development methods, according to our findings. So, our research has shown that the apps might need some more work to make them safer and more secure.

Wodo, Wojciech et al., (2021) The purpose of this study is to lay forth new standards for evaluating the safety of online and mobile banking. Our extensive research with sixty Polish bank clients and our history of working with the Polish banking sector informed the development of these standards. The four primary areas of evaluation that were considered were user authentication and operations authorization, default settings in the bank's online and mobile apps, information and educational campaigns (with the goal of raising bank user awareness), and meta-data analysis of bank users. In light of these requirements, we have developed an assessment tool and conducted an initial analysis of the eight main Polish banks. Our

advice for designers and operators of banking security systems center on three main points: the critical requirement of increasing bank customers' knowledge, the use of biometrics for authentication or authorization procedures, and the adoption of an opt-in approach in default settings. Based on their present situation in Poland, certain concerns related to electronic and mobile banking security are touched upon.

Wainaina, George et al., (2023) The security holes and threats posed by mobile banking applications in Kenya were the primary research foci of this study. There are a number of risks that users' personal information and financial transactions might be compromised by, despite the fact that these applications are accessible and convenient. This research set intended to better secure Kenyan mobile banking applications by identifying their unique threats, weak spots, and attack vectors. Thirdly, the study set out to investigate... The main objective is to analyze the security of mobile banking applications in Kenya and identify the main points of attack that might compromise user data and financial activities. Second, it sought to evaluate the most prevalent problems with these applications by looking at both technical aspects and patterns of user behavior. Its final goal was to suggest security solutions tailored to the Kenyan banking industry that take user behavior and technical improvements into account. Investigations into user awareness initiatives, multi-factor authentication, and encryption to encourage safe banking practices were also part of this process. By analyzing the security of mobile banking applications in Kenya and providing practical recommendations, this study aimed to help both users and financial institutions make their mobile banking experiences safer. In order to guarantee trustworthy financial transactions using mobile platforms, it was stressed that the Kenyan banking industry must be understood and its unique problems solved.

Wazid, Mohammad et al., (2019) In this context, "mobile banking" means accessing one's bank accounts, making transfers, checking balances, and paying bills all from a portable electronic device, such as a smartphone, rather than relying only on one's home computer. While the mobile banking infrastructure offers a lot of benefits to users, it is vulnerable to a number of potential assaults. We describe the development of mobile banking and talk about the many dangers that come with it, including the most current malware assaults. Our article concludes with a survey of current security measures that make mobile banking a safe bet.

Mogos, Gabriela & Jamail, Nor. (2020). While e-banking and online banking have made banking much more convenient in terms of delivery costs, speed, and ease, they have also introduced numerous new concerns. New kinds of risk, as well as a new mindset about risk, have emerged as a result of online banking. When it comes to mitigating risk, technology is both a source and an instrument of paramount importance. Despite the fact that it is an e-banking application, this study aims to determine the current state of the application's security and to assess the dangers and potential assaults that consumers face. Several countermeasures were brought up to counteract assaults; for example, access control is a measure to prevent eavesdropping, which necessitates limiting who may access sensitive information. One other thing you can do to protect yourself against SQL injection is to always use the most recent updates and fixes. These attacks may compromise the whole program or specifically target a user, compromising their sensitive information. Additionally, this study reveals how to use a number of additional security measures to safeguard one's firm and oneself against cybercrime.

Sasikumar, Dr.G.. (2017). From traditional bank deposits to the increasingly popular mobile banking, banking services have come a long way. Customers are able to access their accounts and all the information on the bank's goods and services at any time, from any location, thanks to mobile banking. Although mobile banking is reliable, safe, and economical, it is also complicated and susceptible to network issues. Due to the fact that intruders affect the lives of others both dangerous and unpleasant,

security concerns are crucial. Cybercrime may affect a person in several ways. The goal of this article is to investigate mobile banking security issues, problems, and potential solutions.

Islam, Engr. Md Shoriful. (2014). While mobile banking has made banking more convenient and faster, it has also introduced new risks to the payment security system. The use of mobile phones for banking and other financial services is on the increase among early adopters, and many organizations and banks are seeing this as a way to expand their business. A large number of security concerns related to mobile banking and payment systems have been raised in recent years. In order to better understand where these concerns stand, we systematically reviewed the literature on mobile banking security issues that have been raised between 2008 and 2012.We extracted a huge number of challenges from the systematic review, which yielded 10 publications and 20 primary research, which are presented in this study. Through the use of qualitative data analysis techniques on the review's retrieved data. But most customers cite security concerns as the main reason they haven't used mobile banking yet. While assisting financial institutions in effectively implementing mobile banking technology, this assessment will endeavor to technically resolve these mostly unwarranted concerns about client security. The rise of mobile devices has opened up new avenues for financial transactions. The customer's mistrust in the safety of the services is a major obstacle to mobile banking and payment uptake. It is vital to solve the security problems by understanding the mobile banking and payments business and ecosystem. Mobile banking and payments provide new security concerns that need to be discovered and addressed.

3. IMPACT OF MOBILE BANKING

Positive Impact of Mobile Banking

- **Cost Reduction**

Mobile banking's primary benefit for financial institutions is the significant reduction in customer service expenses it entails. Mobile banking is the most promising avenue for expansion for service providers. Mobile banking is assisting service providers in countries like India, where mobile penetration is approaching saturation, in increasing revenues from the now stagnant subscriber base. In order to draw in new clients and hold on to existing ones, service providers are stepping up the sophistication of their supported mobile banking services.

- **To Control Fraud**

Providing clients with more accurate information could be a great approach to boost customer service. One example is the field of credit card fraud. Using mobile technology, a bank might notify cardholders whenever their card is used for transactions above a certain threshold. The owner will always be notified of the usage of their card and the amount deducted for each transaction in this manner.

- **Reminder Facility**

In a similar vein, the bank might notify the client that a bill is due or remind them of the due date for any outstanding loans or monthly payments. After that, consumers may call in to see their account balance, approve the necessary payments, and ask for further details if needed. In addition to being able to see transactions as they happen, they may also plan ahead to have payments or checks printed. In a similar vein, one might also use their cell phone to request services such as a stop check or a new cheque book.

- **Easy to Avail Mobile Services**

The consumer almost never is without a mobile device. Therefore, it may be used to a wide range of geographical regions. Customers may take use of the bank's services without ever setting foot in an ATM

or branch. According to studies, the introduction of automated teller machines (ATMs) significantly reduced the number of customers visiting bank branches. With mobile services, customers won't need to visit branches as often, which means banks may reduce staffing levels even more. As a result, banks and their clients both benefit from the use of mobile technology. Through automation, the banks enhance this tailored communication even further.

- **Security Features**

Only the customer's registered mobile number will get the notifications from the bank. Also, the account number and other sensitive data is not sent in its whole. However, the client will only get the last six numbers along with the kind of account. Once PULL Alert services are implemented, customers will be able to see their account balance and transactions by a request sent to the registered mobile phone number and verified by a 4-digit Code Number. The authentication credentials will be the mobile phone number and the code number that are used to access the service. It is imperative that the Code number remains secret.

Negative Impact of Mobile Banking

- **Security**

Due to the rarity of Trojan horses and other malware specifically designed for mobile devices, security professionals believe that banking via mobile device is safer than banking via PC. Although mobile banking is not completely safe from security risks, mobile users are more likely to fall victim to a kind of fraud similar to phishing known as "smashing." This occurs when a hacker pretending to be a bank sends a text message to a mobile banking customer requesting sensitive information. A lot of individuals have been scammed out of their money because they fell for this scheme. Even while most online banking services use encryption to prevent hackers from seeing your data, you should still think about what would happen if someone took your mobile device. Despite the fact that all banking apps need a password or PIN, a lot of users either set up their phones to remember passwords or use weak, easily-guessed ones.

- **Compatibility**

Unfortunately, not all devices can access mobile banking. You won't find mobile banking options at all with certain banks. Still others need the use of an exclusive mobile banking program that is compatible with just the most widely used smartphones. Not all third-party mobile banking apps are supported. Most mobile banking services have restrictions on the features you may use if you don't have a smartphone. Although it's not an issue to check your bank balance via text message, more complex capabilities like account transfers are often unavailable to those with "dumb phones."

- **Expense**

The fees for using the network may build up rapidly. Even with a capable smartphone, the cost of mobile banking may still add up due to bandwidth and text messaging expenses. You could have to shell out more cash to use mobile banking at certain banks, and software can be an additional expense. These additional fees may build up fast, particularly if you use your mobile banking often.

4. SECURITY ISSUES IN MOBILE BANKING

There are two distinct areas in mobile banking: the user's cell-phone and the bank's infrastructure. According to the research, there is a chance that mobile financial transactions can be vulnerable to security breaches.

a) Wireless Application Protocol (WAP)

Wireless application protocol allows devices such as digital mobile phones, the internet, personal digital assistants, and more to communicate with one another. Customers may access additional features of online banking using WAP. The present method of encrypting data transfer between banks and their customers isn't enough to safeguard sensitive information sent between banks and their customers. The rationale for this is that security measures need more robust processing capabilities and more storage space. Online banking, for example, makes use of robust computing infrastructure and a well-defined, intricate encryption method to guarantee safety.

Due to the limited processing power of mobile devices, we are unable to implement sophisticated encryption systems. Technology has progressed to the point that end-to-end security is now a need. The data transactions are safe at the bank end, but not at the user end; hence, the data is susceptible to assaults if the user uses their mobile device for mobile banking. The difficulty of providing end-to-end security with WAP was pointed up. The reason for this security problem for WAP mobile banking is that data is not encrypted at the gateway during the protocol change procedure.

b) Authentication Risks and Issues

The login technique is one of the authentication methods used in mobile banking. The PINS authentication technique, on the other hand, is somewhat outdated and has a number of security flaws, including the possibility of password and identity theft. The client may lose faith in the security firm as a consequence of the disclosure of the secret. Mobile banking is subject to certain security protocols that the bank observes. Customers and banks have an unbreakable bond. Customer information such as phone number, SIM card number, PIN, etc. is used to implement this security measure. Customers like mobile banking because it allows them to access their accounts from any location or at any time. Thanks to the intuitive interface, they can move funds across accounts more quickly. In addition, they have the option to see their account status at any given time. However, due to security concerns, not all bank clients are prepared to utilize this service. Mobile banking systems aren't ready for adoption just yet since they're inconvenient for customers and because they don't believe they can withstand direct or indirect assaults.

c) SMS based Mobile Banking

There are end-to-end security issues with SMS-based mobile banking, despite its convenience and ease of use. Issues with SMS and GPRS protocols as well as security in financial transactions occur. These days, you may get mobile banking via almost any bank in the globe. Customers may access databases, files, and crucial documents using mobile phones as well, as can be seen in any mobile banking system. At the moment, mobile banking by SMS is also available in South Africa, Bangladesh, and a few more nations.

d) Virus Attacks in Mobile Banking

More than 50,000 distinct kinds of Trojan horses, malware, and computer infections are out there. Trojan horses and similar software may steal your browser password or any data stored in your operating system's cache. Codes that are malicious are often designed to communicate remotely.

e) Risk with Digital Signature

Digital signatures are attractive to designers because they cut down on hardware costs. For authentication purposes, most firms are looking into digital signatures because of how efficient they are. Digital signatures are known to be computationally expensive. Date and amount, two examples of unsigned values, varied from one transaction to the next. It follows that a signed template may include many unsigned values, such as dates, amounts, etc.

5. THREATS AFFECTING USER DATA IN MOBILE BANKING APPLICATIONS

There have been benefits and drawbacks for banks and customers alike due to the fast and intermittent technical improvement in mobile banking. Nonetheless, both customers and financial institutions are understandably worried about the safety of mobile banking. The vast number of access routes offered by mobile banking systems makes them vulnerable to assaults. Along with the evolution of mobile banking technologies, the danger environment is also constantly changing. The three main categories of mobile banking security risks are device-specific, network-related, and data center-related. Mobile banking apps are the focus of the study's subsequent sections, which address potential dangers and assault vectors.

Mobile Malware

Malware assaults take use of vulnerabilities that allow unauthorized users to access computer systems. Motivated by financial or political gain, attackers get into as many network devices as they can to complete their damaging aims, which includes transferring key information packets from one attack to another. There is some theoretical classification for mobile malware according to the harmful goals and actions it does. Distribution strategies have their own unique benchmarks and additional requirements. Social engineering and self-propagation are the two most common methods of dissemination. One approach employs automated means, such worms, to install malware into mobile devices. The second way takes advantage of users' curiosity and lack of knowledge to actively install software, like adware. Along with these popular categories, there are other lesser-known forms of malware. Trojan horses, backdoors, spyware, and adware are the four most common forms of mobile malware. The most common kind of Trojans are banking Trojans, which target specific mobile banking services and activities. Whenever a network connection is available, it may steal sensitive user data and passwords, hide them, and then send them to a command and control server.

Trojan horses in banking emerged at the same time as customers began shifting their banking habits from desktop computers to mobile phones. Regular program updates, mobile security software, a firewall, screen lock protection, and app downloads from legitimate shops are some ways to eliminate mobile malware in mobile banking apps. Running the most current versions of apps on a smartphone is a common practice for updating mobile banking apps and operating systems. Updating to the latest security patches and updates is ensured by this method. The second point is that mobile banking apps may be protected from viruses and malware by using mobile security software, such as antivirus for smartphones. Furthermore, you can be certain that mobile banking programs have been through safety tests if you download them from official outlets like the Apple Store or the Google Play Store. So, it's wise to only download apps from legitimate and authorized sources.

Packet Sniffing Attacks

Packet sniffing is the process of monitoring data packets as they traverse a network. It is a program that records every action taken by a network. It can also record and eavesdrop on any kind of network communication, whether it's coming in or going out. Packets are the building blocks of data transmission via a network. One way to transfer data across a network is to break it up into smaller packets, each of which contains the addresses of a different machine. It is possible to evaluate a network's performance or identify a bottleneck (whether it's at the source or the destination) by installing a packet sniffer at any of the network's nodes. The primary user of sniffer packets is the network administrator.

Man-in-The-Middle Attacks

An attack known as a "Man-in-the-Middle" (MITM) happens when a hacker mediates communication between two parties. Passive man-in-the-middle attacks include the hacker just identifying client-server activity and watching it with the intention of using what they learn later on. Active man-in-the-middle

attacks involve the hacker actively interfering with or altering the sent information. Bypassing the bank's primary server through the mobile banking app compromises both the security and privacy of the data sent between the two systems. A number of methods exist for carrying out active man-in-the-middle attacks; they include spoofing domain name systems, poisoning the Address Resolution Protocol (ARP) cache, and secure socket layer hijacking. Placing a sham IP or MSA pair into a host's ARP cache is known as ARP cache poisoning. The return of an incorrect MAC address is possible. The host sends an ARP request to a valid IP address, such the IP address of the gateway. Gateway ARP requests are broadcast over LANs and often result in a response being sent back to the requesting host. Consequently, a LAN-connected attacker may listen to this inquiry and reply if it were to activate its adapter in promiscuous mode. Lastly, the attacker can use the ARP cache update policy to set their MAC address against the IP address of the gateway, causing traffic to bypass the genuine gateway and go via themselves.

Eavesdropping Attacks

To launch an eavesdrop attack, one must be able to intercept data transfers across a network. An adversary interjects themselves into data transmissions between a bank's server and a mobile banking app without the knowledge or permission of the parties involved. In order to get sensitive information, the attacker uses insecure network communications. The transmission of unencrypted data via a communication channel often results in this. While passive eavesdropping simply involves listening to network message transmissions, active eavesdropping requires the hacker to appear as a helpful unit and ask questions to transmitters in order to obtain information. Scan, probe, or meddle with it is how you describe this. The communication network's weak Secure Shell (SSH) layer administration and encryption keys are being utilized by attackers to their advantage. An eavesdropper has broken the confidentiality of the conversation.

Denial of Service Attacks

Denial of Service (DoS) attacks are initiated when an attacker redirects traffic from a customer's mobile banking app to the server using their own personal wireless network. That is why the attacker is able to intercept and discard every single packet that tries to communicate with the bank's server and system application. Consequently, the mobile banking software runs into timed-out connections, which deplete system resources. The most common type of protocol vulnerability that prevents network devices from functioning correctly is a denial-of-service attack that targets the application layer. In both cases, the intended users are prevented from accessing the network's resources or services. It is quite difficult to detect these assaults due to the fact that Internet traffic consists of both normal and unusual patterns. A further characteristic of attack traffic is its seeming normalcy. Two main types of denial-of-service attacks that might occur at the application layer are protocol-specific and general. There are several types of protocol-specific attacks, such as those targeting the Network Time Protocol, time shifting, Slow Hypertext Transfer Protocol, and DHCP Hunger.

Social Engineering Attacks

The largest dangers to banking organizations' cyber security framework are social engineering assaults. Social engineering is preventable but may not be identified easily. Despite their differences, social engineering attacks all have a similar pattern. Four steps make up the typical pattern: researching the target, getting to know the target, applying what you've learned to carry out the attack, and leaving no evidence. In order to circumvent a bank's security restrictions, enemies therefore do study on human behavior rather than using technological system assault methods. Social engineering assaults frequently use phishing, spear phishing, scareware, pretexting, and baiting. Phishing attacks' main objective is to

deceitfully obtain the targets' private banking details over the phone or through emails. To get private and sensitive information, attackers trick bank clients by utilizing websites, emails, adverts, scareware, anti-virus software, PayPal websites, prizes, and freebies to deceive bank clients. Snapping on e-mail links or receiving calls from fictional bank department asking for personal information, for instance is a social engineering behavior attack. These efforts are geared towards mining important confidential bank details that could be used to access private accounts by utilizing mobile banking channel.

Cross-Site Scripting Attacks

A programming problem known as Cross-Site Scripting (XSS) happens when a user enters data into a system that has not been sanitized. By exploiting security holes, an attacker can compromise an online application, steal sessions, take over user accounts, and redirect traffic to their own domain. A cross-site scripting (XSS) attack can compromise any vulnerable website, regardless of the programming language it was built in. Users' browsers can execute scripts due to the XSS vulnerability. When a user makes modifications to a script that is created dynamically, it becomes risky. Multiple forms of cross-site scripting (XSS) attacks exist, including those that rely on mutations or document object models. on this kind of attack, the perpetrators launch malicious JavaScript code on the victim's browser with the intention of stealing sensitive data. This security hole is common in today's web sites. Computers, mobile devices, and IoT nodes are common targets of malware assaults, which often seek to undermine online privacy. Furthermore, the victims are oblivious to the invader as they believe the communication link is secure. Several signature-based scanning approaches exist for the detection of malware that specifically targets Windows operating systems. To differentiate between static and dynamic approaches, malware identification analysis is divided.

SQL Injection Attacks

A popular programming language for managing relational databases, Structured Query Language (SQL) finds extensive use in online applications. Questions, expressions, clauses, and statements are some of the declarative components that make it up. One kind of code injection attack is known as Structured Query Language Injection Attack (SQLIA). In this attack, the attacker inserts SQL code into the user's input in order to access resources that should not be there. This might happen if the query is constructed without validation by merging user input (e.g., data submitted into an interactive online form) with unwanted data (e.g., data gathered from URLs or cookies). Serious consequences, including data loss and system compromise, can result from a SQLIA that is successful. The hacker can access sensitive information like login credentials and financial data and can also alter database data. The attacker may even be able to take complete control of the hacked machine in extreme cases. Because of the serious consequences of a SQL injection attack, financial institutions must ensure the security of their online application by implementing effective methods of prevention and detection.

Having measures to identify and avoid SQLIA is crucial since they may cause significant damage to banks. Log analysis, IDSs, and honeypots are the most widely used detection techniques. Reviewing the log files of the web server and the database server is what log analysis is all about when it comes to finding security risks and SQL injection vulnerabilities. The process of doing log analysis may be done either manually or automatically. In order to detect SQLIA, manual log analysis requires reading log files line by line. In contrast, automated programs can detect signs of an attack in log files in real-time and notify the appropriate parties. A complete record of all requests made to the web application may be found through log analysis, which simplifies the process of identifying and addressing security issues. Nevertheless, log analysis is a laborious and difficult process, especially when dealing with large log files.

6. CONCLUSION

To their ability to streamline financial transactions, mobile banking apps have quickly become an integral part of today's financial systems. But worries about security and data protection have grown in tandem with our reliance on these apps. From malware and data breaches to phishing and sloppy security measures, this review shows that mobile banking services are susceptible to all sorts of dangers. Inadequate resolution of these issues may result in monetary losses, theft of personal information, and loss of confidence from customers. Strong encryption, multi-factor authentication, secure application architecture, and constant monitoring are critical advanced security techniques to minimize these dangers. Further important in protecting sensitive information is ensuring compliance with data protection standards and raising user awareness. The continued development of mobile banking technologies highlights the critical need for a thorough and proactive strategy to safeguard data and prevent unauthorized access in order to maintain secure and long-lasting online banking platforms. In order to keep users' trust and encourage the continuous expansion of mobile banking services, it is essential to reinforce these safeguards.

REFERENCES

1. Y. I. Abdullahi, H. Usman, and A. Abba, “Security analysis and evaluation of mobile banking applications in Nigeria,” *International Journal of Informatics and Communication Technology (IJ-ICT)*, vol. 13, no. 3, pp. 354–361, 2024, doi: 10.11591/ijict.v13i3.pp354-361.
2. G. Wainaina, D. Kiyeng, and N. Masese, “Enhancing security measures for mobile banking applications: A comprehensive analysis of threats, vulnerabilities, and countermeasures in Kenya banking industry,” *International Journal of Computer Applications Technology and Research*, vol. 12, no. 8, pp. 99–112, 2023, doi: 10.7753/IJCATR1208.1014.
3. W. Wodo, P. Błaśkiewicz, D. Stygar, and N. Kuźma, “Evaluating the security of electronic and mobile banking,” *Computer Fraud & Security*, vol. 2021, no. 10, pp. 8–14, 2021, doi: 10.1016/S1361-3723(21)00107-X.
4. G. Mogos and N. Jamail, “Study on security risks of e-banking system,” *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 21, no. 2, pp. 1065–1072, 2020, doi: 10.11591/ijeecs.v21.i2.pp1065-1072.
5. Bicaku, M. Tauber, and J. Deising, “Security standard compliance and continuous verification for industrial internet of things,” *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, 2020.
6. S. Cho, J. Cho, S. Hyun, and H. Kim, “SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles,” *Applied Sciences*, vol. 10, no. 9, p. 3149, 2020.
7. M. Wazid, S. Zeadally, and A. K. Das, “Mobile banking: Evolution and threats—Malware threats and security solutions,” *IEEE Consumer Electronics Magazine*, vol. 8, no. 2, pp. 56–60, 2019, doi: 10.1109/MCE.2018.2881291.
8. Foroughi, M. Iranmanesh, and S. S. Hyun, “Understanding the determinants of mobile banking continuance usage intention,” *Journal of Enterprise Information Management*, vol. 32, no. 6, pp. 1015–1033, 2019.
9. J. P. Kaleta, J. S. Lee, and S. Yoo, “Nudging with construal level theory to improve online password use and intended password choice,” *Information Technology & People*, vol. 32, no. 4, pp. 993–1020, 2019.
10. G. Sasikumar, “Mobile banking and security challenges,” *International Journal of Scientific Research and Management*, vol. 5, no. 7, pp. 6014–6018, 2017, doi: 10.18535/ijsrm/v5i7.26.

11. Alarifi, M. Alsaleh, and N. Alomar, "A model for evaluating the security and usability of e-banking platforms," *Computing*, vol. 99, no. 5, pp. 519–535, 2017.
12. W. Bai, D. Kim, M. Namara, Y. Qian, P. G. Kelley, and M. L. Mazurek, "Balancing security and usability in encrypted email," *IEEE Internet Computing*, vol. 21, no. 3, pp. 30–38, 2017.
13. M. S. A. Al-Khuja and Z. A. B. Mohamed, "Investigating the adoption of e-business technology by small and medium enterprises," *Journal of Administrative and Business Studies*, vol. 2, no. 2, pp. 71–83, 2016.
14. M. B. Joshi and K. Patel, "Enhanced mechanism for online banking system through cyber crime investigation," vol. 1, no. 7, pp. 242–246, 2015.
15. B. Merdenyan, O. Kocyigit, R. Bidar, O. Cikrikcili, and Y. B. Salman, "Icon and user interface design for mobile banking applications," *International Journal of Advances in Computer Science and Its Applications*, vol. 4, no. 2, pp. 54–59, 2014.
16. M. S. Islam, "Systematic literature review: Security challenges of mobile banking and payments system," *International Journal of u- and e-Service, Science and Technology*, vol. 7, no. 6, pp. 107–116, 2014, doi: 10.14257/ijunesst.2014.7.6.10.