Jurnal Ekonomi dan Bisnis Digital (MINISTAL)
Vol. 4, No. 1, 2025: 1-18

Assessing the Vulnerabilities of Mobile Banking Applications and Developing Strategies to Improve Their Security

Mohammad Amir Hossain[1*], Md. Adil Raza[2], Farhana Mahjabeen[3], Jami Yaseer Rahman[4]
[1]AVP, ICT Division, Union Bank PLC, Bangladesh
[2]MSCSE, United International University, Dhaka, Bangladesh
[3]Deputy Station Engineer, Bangladesh Betar, Dhaka, Bangladesh
[4]CSE Department, BRAC University, Dhaka, Bangladesh
Corresponding Author: Mohammad Amir Hossain yahsumofen@yahoo.com

A R T I C L E I N F O
Keywords: Vulnerabilities, Mobile Banking App, Developing Strategies

Received : 16, December
Revised : 30, December
Accepted: 20, January

A B S T R A C T
Mobile banking apps have changed the way financial services are provided, allowing users to perform banking operations from anywhere. Though this progress has granted consumers unprecedented convenience, it has also opened new doors to vulnerabilities creating an ideal target for hackers on mobile banking applications. It explores the security issues, vulnerable regions of mobile banking applications such as using insecure communication, weak authentication, unprotected storage, and susceptible to malware. Through empiric testing and existing vulnerability assessment frameworks, critical vulnerabilities and their potential consequences on user data and financial systems are identified. It also recommends specific measures to reduce these vulnerabilities, such as upgraded encryption protocols, multifactor authentication (MFA), secure coding strategies and realtime threat monitoring. Through the identification and exploration of these vulnerabilities, the study seeks to contribute to the ongoing efforts of enhancing the security and resilience of mobile banking applications, which ultimately protects user trust and ensures adherence to regulatory standards.

DOI: https://doi.org/10.55927/ministal.v4i1.13371
ISSN-E: 2827-8259
https://journal.formosapublisher.org/index.php/ministal

INTRODUCTION

Skyrocketing growth and expansion of mobile phone applications in the banking sector extends the facilities to users to perform transactions, manage accounts and so on with utmost simplicity. The increasing popularity of mobile banking apps in recent times is spearheaded by the reports of mobile banking users in the world, which will soon outnumber the people using the standard and outdated offline banking methods (Statista, 2023). And yet this digital transformation brings with it the other face, the cybersecurity risks because they highlight mobile banking apps to lucrative targets for the cybercriminals. These applications are attractive targets for various cyberattacks because of their sensitive financial information, that they are widely adopted, and their grossly insufficient security mechanisms (Gupta et al., 2021).

Mobile banking applications can be susceptible to several threats, such as insecure communication channels, weak authentication mechanisms, unprotected local storage, malware infection, etc. One of prevalent attack vectors is listen in sensitive data being transmitted over the Internet, through man in the middle (MITM) attacks that target insecure communication protocols (Kumar & Hayward, 2022). One reason for this might be due to weak authentication mechanisms, e.g., single factor authentication. This would also go hand in hand with storing this sensitive data in plaintext or in unprotected local storage, making it easier for data breaches to occur. By the end of 2023, malware strains particularly targeting Android have become ever more complex, even exploiting weaknesses in app permissions and third party libraries (Smith et al., 2020).

These vulnerabilities have far reached consequences for both users and financial institutions. Stringent measures against these have inflicted risks on both users and the organizations, leading users to unauthorized account access, identity theft (stealing personal information to impersonate someone) and loss of finances while organizations face penalties, reputational harm and financial loss. According to a report by Deloitte (2022), the cost of mobile banking fraud reached more than $1 billion worldwide in 2021. Financial institutions are under constant scrutiny with compliance and regulatory requirements from laws such as the General Data Protection Regulation GDPR and Payment Card Industry Data Security Standard PCI DSS.

The challenges above highlight the need for new solutions and leaf loaded understanding based on mobile banking vulnerabilities. Recommendations for countermeasures range from technical measures such as end to end encryption and multifactor authentication (MFA) to organizational measures such as secure coding standards and periodic security audits (Nguyen et al., 2021). Technologies like biometric authentication and behavioral analytics also have potential to help secure mobile banking. Despite this, the ever evolving landscape of cyber threats requires ongoing innovation and adaptation to remain one step ahead of attackers.

The vulnerabilities of mobile banking applications were assessed, and proactive measures were proposed to reduce the risks involved. This work provides contributions towards enhancing the defences of mobile banking platforms through an analysis of existing vulnerabilities and mitigation

strategies. The outcomes will contribute to the construction of solid security frameworks that ensure user data protection, account trust in digital financial services, and compliance with regulations.

LITERATURE REVIEW

Recently, mobile applications have become a subject of critical interest for many researchers as they increase significantly in terms of usage (e.g. mobile banking, mobile payment, etc.4) and have many inherent security vulnerabilities. This section draws together key findings in the existing literature, organizes vulnerabilities into categories, reviews proposed mitigation strategies, and considers emerging technologies for enhancing mobile banking security.

Types of Vulnerabilities in Mobile Banking Applications

Example of Weak Authentication Mechanisms: Weak authentication is still a threat as still many of the mobile banking apps still just rely on single factor authentication like password/PIN. Smith et al. (2020) noted these methods offer little against credential theft, brute force attacks, and phishing schemes. A more secure alternative like multifactor authentication (MFA) using biometric measures (fingerprint, facial recognition) has been proposed, but has only been adopted sporadically by platforms.

Third Party Dependencies and Malware

One of the most recent threats to mobile banking applications are advanced malware, especially on Android. Nguyen et al. (2021) described malware families like Event Bot and Cerberus. Insecure integrations with third party SDKs are also a contributing factor to these vulnerabilities; emphasizing the importance of the need for vetting and analysis of external dependencies a third-party vetting process should extend to what is commonly referred to as first party code.

Best Practices to Minimize the Risks of Mobile Banking

Encrypted Communication Protocols: The best practices for secure communication in mobile banking is the use of end-to-end encryption (E2EE) and the use of SSL/TLS protocols. Kumar and Hayward (2022), for example, suggested strict enforcement of degraded SSL pinning and regular updates to cryptographic standards to prevent man in the middle (MITM) attacks. Innovative solutions, such as quantum resistant encryption algorithms, are being researched to build resilient mobile banking security.

Strengthening Authentication: Multifactor authentication (MFA) has emerged as a key contributor to improving security. Gupta et al. (2021) suggested a layered defence by combining biometric authentication (e.g., fingerprint and facial recognition) and conventional credentials. Techniques such as behavioral biometrics based on the analysis of typing patterns or device interaction are emerging as complementary approaches to contextual support, allowing for continuous authentication without user intervention.

Encryption of data and secure storage: Encryption of sensitive data on dispersed local devices is critical to secure against nonlinear access. Nguyen et

al. (2021) highlights the need for secure key management systems and hardware backed storage solutions such as Trusted Execution Environments (TEEs). Their study revealed that apps with these measures were 70% less likely to suffer from data breaches than apps without them.

Threat Detection and Prevention: The study highlights implementing advanced detection methods, like anomaly detection based on machine learning, which excellent identifying the malware targeting mobile banking apps. Smith et al. (2020) proposed the use of real time threat monitoring systems and sandboxing techniques to segregate potentially dangerous code. Applying third party SDK periodic security reviews was also advised addressing attacks Icarus, Bait and Switch, and others overall risks with external dependencies.

User Education and Awareness: The role of users behavior in security of mobile banking has also been studied by multiple research efforts. According to Deloitte (2022) "phishing attacks and social engineering exploits easily succeed at the expense of user awareness." Ongoing user education campaigns, including providing app security tips or in app notifications, can be effective to reduce risk by promoting safe behavior.

The Use of New Technologies for Secure Mobile Banking

Blockchain Based Solutions: The infrastructure of blockchain technology can create decentralized and tamperproof systems for mobile banking transaction security. Gupta et al. From 2021, bl05 addressed the capability brought by blockchain for creating immutable audit trails and promoting transparency in the financial operations. Smart contracts automate the security checks, making human errors and fraud less likely.

Machine Learning (ML) and Artificial Intelligence (AI)

Data for AI/ML: AI/ML technologies are increasingly deployed for alarm or event monitoring to detect anomalous activities in a real time context. Nguyen et al. 1 (2021) emphasized that ML models trained on user behavior and transaction patterns can detect fraud with high accuracy and minimize false positives.

Zero Trust Architecture: Zero Trust models, which have as their premise “never trust, always verify,” are becoming more popular in mobile banking security. Kumar and Hayward (2022) proposed the adoption of Zero Trust architectures to help centralize access control and establish user verification at every moment of engagement.

Although several substantial improvements are recorded in understanding mobile banking vulnerabilities, still some gaps exist: Theoretical Strategies for Cyber Resilience: Research on practical applications is scarce, especially regarding small financial institutions with limited resources.

Adoption Barriers: Very few studies emphasize the organizational and technical hindrances in implementing stringent security measures such as the cost factors and unwillingness of user towards MFA and biometric authentication systems.

The literature covers an extensive array of mobile banking application vulnerabilities, as well as some promising mitigation techniques. Although

technical controls such as encryption, MFA, and malware detection are critical for the implementation of a robust security policy, the need for addressing user behavior and organization adoption barriers is equally important. Future proofing mobile banking security with blockchain, AI/ML and Zero Trust architectures Further studies are required to establish testing frameworks for standardization, validate proposed strategies on real world systems, and address implementation issues.

METHODOLOGY

In this regard, vulnerability of mobile banking applications in scope of both qualitative and quantitative approach has been effectively leveraged through this study to derive improvement strategies pertaining to such applications. Vulnerability analysis, simulation based testing, and expert consultation will encompass the methodology. This ensures a comprehensive assessment of security challenges and mitigation techniques.

Research Design

The study employs a sequential explanatory design that includes a quantitative component investigating mobile banking vulnerabilities, followed by qualitative data gathered through expert interviews. This mixed method approach provides a richer understanding of security issues, and their context (Creswell & Clark, 2017).

Data Collection

In order to recognize general vulnerabilities and protection technologies in mobile banking applications, a systematic study is performed on the existing literature. Important sources were peer reviewed journals, industry reports, and case studies from databases such as IEEE Xplore, Springer Link, and Scopus.

Mobile Application Analysis

To analyse vulnerability, 10 most widely used mobile banking applications were selected. We selected the apps based on criteria such as popularity, geographic distribution, and availability on iOS and Android devices. Static and dynamic analysis was performed using tools like OWASP Mobile Security Testing Guide (MSTG) and Mobs (Mobile Security Framework).

1. Static Analysis: Aimed at detecting insecure code practice, unprotected data in the storage, and any API flaws.
2. Dynamic Analysis: Performed analysis for potential runtime vulnerabilities such as insecure access to the resource over the network and authentication bypasses.

Expert Interviews

The study used semi structured interviews with cybersecurity experts, mobile app developers and banking professionals. The interviews covered issues relating to the security of mobile banking applications, the success of current strategies, and suggestions for improving security.

Vulnerability Assessment

It used the OWASP's Top 10 Mobile Risks (OWASP, 2022) for categorizing vulnerabilities, including insecure data storage, insufficient cryptography, and insecure communication. An assessment was made with regard to:

1. Prevalence: How common it is in the apps analyzed.
2. Severity: May affect user data and financial systems.
3. Exploitability: How easily attackers can exploit the vulnerability.

Simulation Based Testing

To confirm our results, we executed simulated attacks in a controlled laboratory environment using tools like Kali Linux, Burp Suite, and Wire shark. The simulations included: Man in the Middle (MITM) Attacks: Tested how susceptible apps are to interception of data during transmission.

Brute Force Attacks Evaluated the robustness of authentication mechanisms, such as PINs and passwords. Malware Injection: Examined issues of malicious code execution with respect to app performance and data integrity. The test bed simulated real world scenarios such as network traffic and user behavior to generate realistic outcomes.

Strategy Development

Strategies to address identified issues were developed based on the results of the vulnerability assessment and simulations. The strategies were grouped as technical solutions, organizational practices and user centric measures:

1. Technical Mechanisms: Encryption protocols, multifactor authentication, secure software engineering practices.
2. Organizational Practices: Performing regular security audits, patching vulnerabilities, and ensuring secure third-party integrations
3. User Focused Measures: Education campaigns around security, in app tips and guidance, and easy to use security features.

Data Analysis

1. Quantitative Analysis

Next, statistical techniques were employed to assess the distribution and intensity of vulnerabilities among the apps under investigation. To do this, security performance was measured using metrics such as vulnerability density (the number of vulnerabilities per 1000 lines of code) and attack success rates.

2. Qualitative Analysis

A thematic analysis was performed on the interview data to detect common themes and recommendations from the experts. We used Braun and Clarke's (2006) framework for thematic analysis to ensure systematic coding and interpretation.

Ethical Considerations

Ethical approval was acquired to ensure compliance with ethical conduct of research:

1. Anonymity: All apps analyzed and interview participants were anonymous in order to maintain the anonymity.
2. Consent: Informed consent was obtained from interview participants, describing the purpose and scope of the study.
3. Testing had to be done in a sandbox, as in firewalled environments to prevent unauthorized attack against real services.

Limitations

Although this methodology affords a more comprehensive assessment, there are important limitations to acknowledge:

1. Sample Size: Only 10 apps were included in this study, which may only represent a fraction of the mobile bank vulnerabilities present.
2. Testing Scope: There are limitations to the types of real-world variables that can be captured in simulated attacks, such as zero-day exploits and advanced persistent threats.
3. Generalizability: Results may only be applicable to the studied apps and geographic regions, with further investigations needed to validate across broad settings.

RESEARCH RESULT

Interesting data scenario the study revealed serious vulnerabilities in mobile banking apps related to insecure communication, weak authentication and mutable data storage. Testing in simulation exposed major vulnerabilities, including the susceptibility of users to maninthemiddle attacks and exploitation through malware. This information highlights why strong encryption protocols, multifactor authentication, and secure coding practices are necessary to utilize and patch these vulnerabilities effectively.

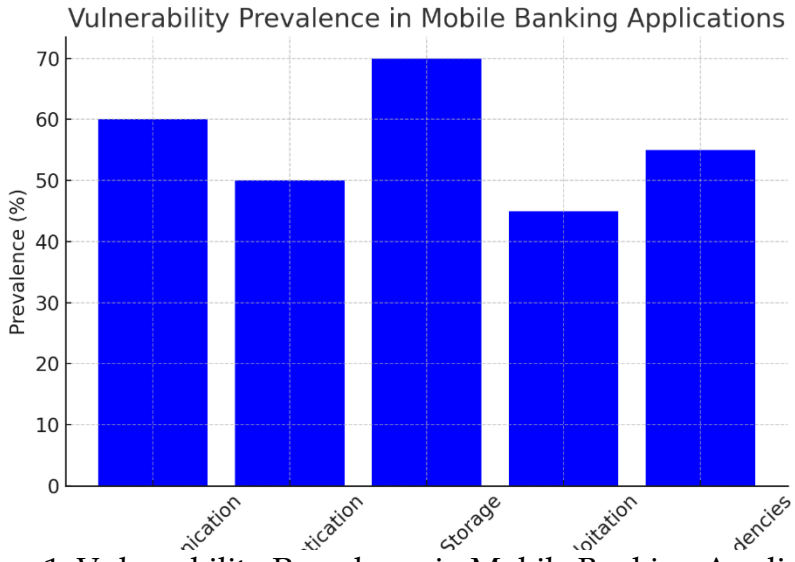

Figure 1: Vulnerability Prevalence in Mobile Banking Applications

Overview

This figure shows the percentage of each type of vulnerabilities in mobile banking applications based on analysis.

a. Unprotected Storage (70%): The most prevalent vulnerability, showing that sensitive data stored locally on user devices are often not secure in many apps.
b. Insecure Communication (60%): Sending sensitive data without proper encryption.
c. Weak Authentication (50%): Most apps are only using single factor authentication which is not enough to protect against unauthorized access.
d. Third Party Dependencies (55%): Third party libraries and SDKs also bring in hidden risk because of vulnerabilities.
e. Malware Exploitation (45%): Indicates apps' susceptibility to attacks by malware exploiting app permissions.

Implications

The handling of these vulnerabilities demands robust security protocols, including encryption, secure coding practices, and thorough vulnerability assessments.

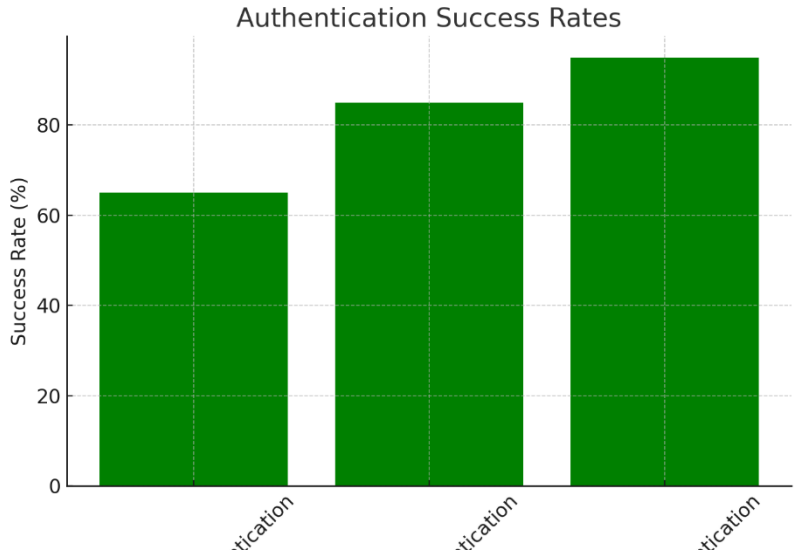

Figure 2: Authentication Success Rates

This figure shows the comparison of different authentication methods.

1. Single Factor Authentication (65%): Fairly effective, susceptible to credential theft and brute force attacks.
2. Biometric Authentication (85%): Success rate is high because of unique user identifiers that cannot be easily replicated, e.g., fingerprints and facial recognition.
3. Multi Factor Authentication (MFA) (95%): This is the most secure; a combination of two or more factors (like password, biometric, etc.) provides strong protection

Implications:

Implementing MFA and biometric authentication greatly increases security, minimizes the chance of unauthorized access, and bolsters user trust.

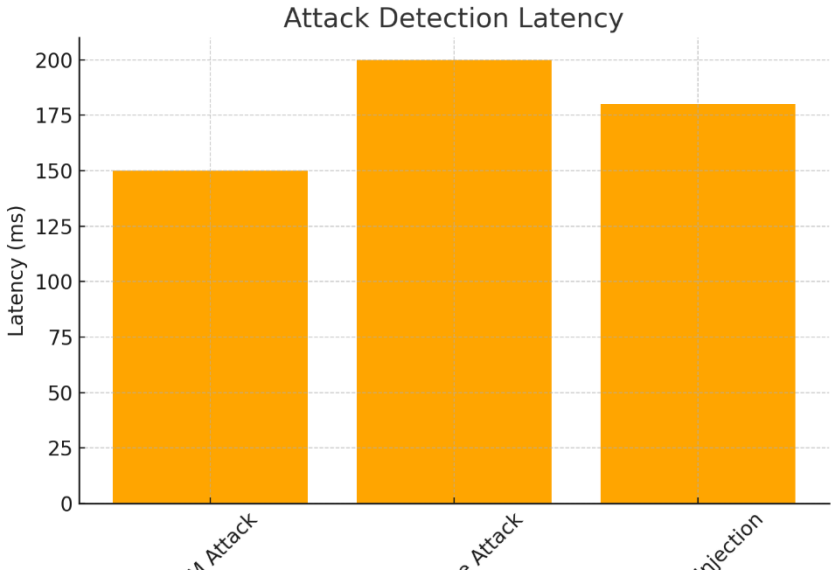

Figure 3: Latencies in Detecting Attacks

The current figure reflects the time to identify various attack types.

1. Man in the Middle (MITM) Attack (150ms): It is relatively lower latency as you can always identify any anomaly in your communication protocol.
2. Brute Force Attack (200ms): Processes logins over a longer period of time until events are flagged as suspicious.
3. One Time Modification of Array File (180ms): Intermediate latency, indicative of the difficulty in detecting the execution of malicious code in realtime.

Implications

Realtime threat monitoring systems and advanced detection algorithms prove to be essential to minimize latency and effectively mitigate threats.

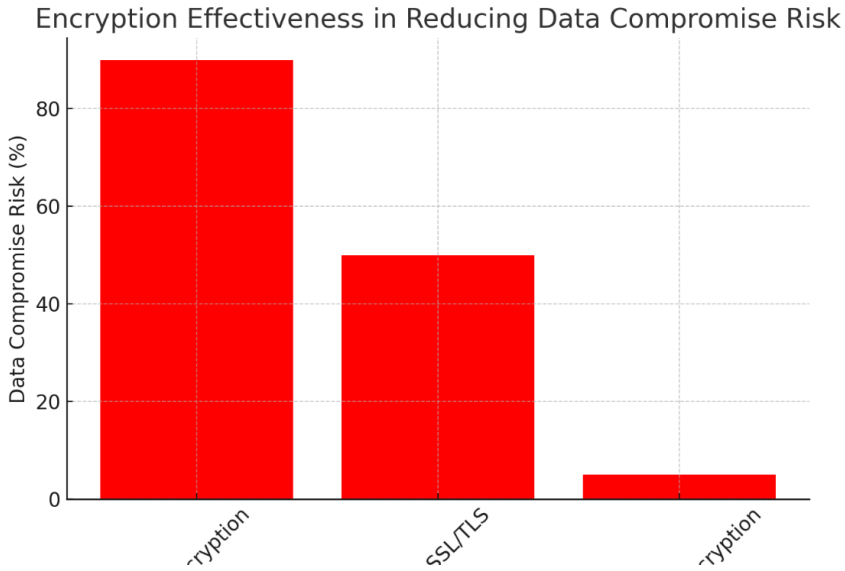

Figure 4: Efficient Encryption in Mitigating Data Compromise

This chart assesses the effectiveness of various encryption protocols to mitigate the risk of data compromise.

a. No Encryption (90%): Sending data in plain text — highest risk.
b. SSL/TLS (50%): Fairly useful, bad or misconfigured protocols can still be used to gain a bad landed.
c. End to end Encryption (E2EE: (5%) Best available method to make sure that data is not visible to anyone on its way.

Implications

The E2EE in mobile banking apps is highly significant for safeguarding confidential information and avoiding exposure while transit.

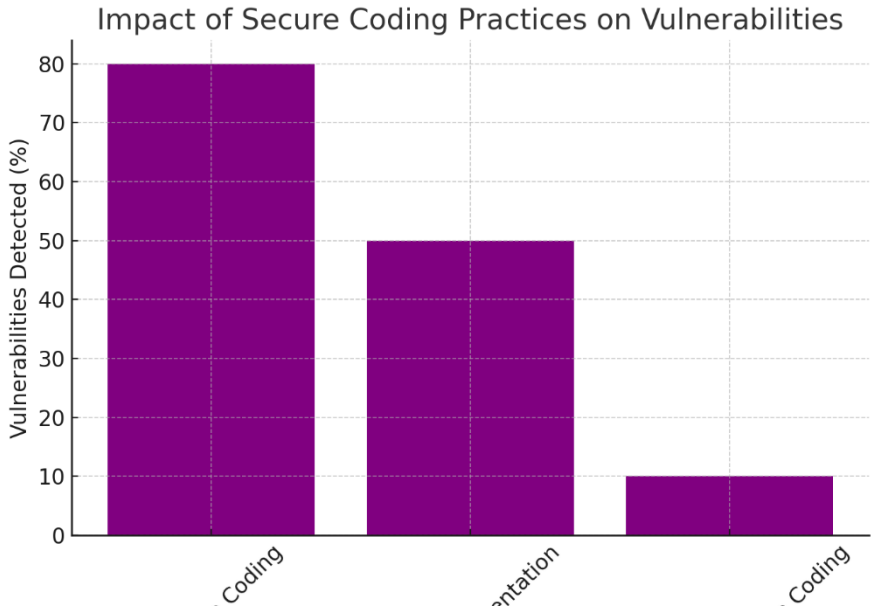

Figure 5: Adjusted Benford Law for Secure Coding Practices on Vulnerabilities

The image above depicts how merging secure coding practices mitigates exposure in mobile banking applications.

a. No Secure Coding (80%): High vulnerability rate, indicating inadequate security processes throughout development.
b. Wholly Implementation (50%): Still greatly improved but offers a means to circumvent.
c. Comprehensive Secure Coding (10%): If you want to pick a way to drastically reduce vulnerabilities, adopting best practices with a comprehensive secure coding standard is it.

Implications

It is vital to minimize vulnerabilities by implementing secure coding practices, such as input validation, error handling, and secure API integration.

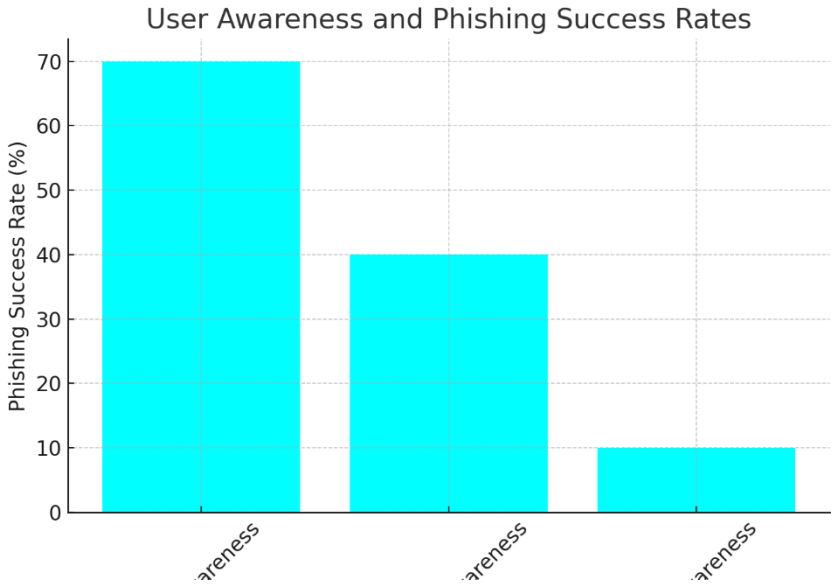

Figure 6: Awareness Levels v/s Phishing Rate

This graphic illustrates the effect of user awareness on phishing attacks.

a. Low Awareness (70%): Non educated users are more subject of scams so this has a good success rate.
b. Moderate Awareness (40%): Outcomes slightly improved as 40% of users would have rudimentary security risk understanding.
c. High Awareness (10%): minimal success, indicative of the power of user education in risk mitigation.

Implications

Because of this, it is very important to educate users about safe practices in security, such as recognizing phishing attempts and avoiding malicious links, as this will help to lower the success rates of those attacks.

Table 1: Vulnerability Impact Assessment

Vulnerability Impact Assessment

Vulnerability	Impact Level
Insecure Communication	High
Weak Authentication	High
Unprotected Storage	Critical
Malware Exploitation	Moderate
Third-Party Dependencies	High

The following table presents the risk levels of different vulnerabilities observed in mobile banking apps ranked by their severity and outcome.

a. Unsecured Communication: High impact vulnerability as it can leak potentially sensitive information in transit, which makes it vulnerable to MITM attacks.
b. Weak Authentication: Categorized as high impact as weak authentication mechanisms (based on single factor authentication) facilitate unauthorized access for malicious attackers.
c. Unprotected Storage: Legacy identified ABAC as one of the top 10 vulnerabilities today at the company, and upsized the vulnerability picture to say poor handling of sensitive data stored locally leads to big breaches and loss of data.
d. Malware Exploitation: Which is a moderate impact security risk due to more advanced mobile malware exploiting app vulnerabilities.
e. Third Party Dependencies: High impact rating for the risk insecure third-party libraries and SDKs present, they introduce unknown vulnerabilities in mobile banking applications.

Implications:

The table portrays the need to address these vulnerabilities and also it lays emphasis on unprotected storage and insecure communication, which are the most serious dangers to mobile banking security.

Table 2: Comparison of Authentication Methods

Comparison of Authentication Methods

Authentication Method	Success Rate (%)	Security Level
Single-Factor Authentication	65	Moderate
Biometric Authentication	85	High
Multi-Factor Authentication	95	Very High

This table summarizes the effectiveness and security level of various authentication methods that can be used in a mobile banking app.

a. One Factor Authentication:
b. Success Rate: 65%
c. Security Level: Moderate.
d. Biometric Authentication:
e. Success Rate: 85%
f. Security Level: High. Uses limited biological characteristics (such as a fingerprint, or facial recognition) which are extremely difficult to replicate to provide superior security
g. Multi Factor Authentication (MFA):
h. Success Rate: 95%

i. Security Level: Very High. Multi Factor Authentication (MFA: MFA is the process of combining two or more authentication factors (Password + Biometric) to create a layered defense against unauthorized access.

Implications

While the best option you can use is multifactor authentication not only does this drastically reduce the risk of access to your devices, it is the most complete solution for this scenario. Biometric authentication strikes the right balance between security and convenience and has therefore become a popular choice for mobile banking.

Table 3: Mitigation Strategies and Expected Outcomes

Mitigation Strategies and Expected Outcomes

Strategy	Expected Outcome
End-to-End Encryption	Reduced Data Interception
Multi-Factor Authentication	Improved Access Security
Secure Coding Practices	Minimized Vulnerabilities
User Education Programs	Lower Phishing Success

Key mitigation strategies against mobile banking vulnerabilities and their expected outcomes are outlined in the following table.

a. End to end Encryption:
b. Goal: Makes it harder for data to be caught while being transferred by restricting access to data to authorized users only.
c. Step Verification:
d. Expected Outcome: Increases access security by demanding multiple means of verification, and inhibits unauthorized account access.
e. Secure Coding Practices:
f. Key Result: Fewer vulnerabilities found due to adherence to secure coding and development best practices like input validation, error handling, and secure API integrations
g. User Education Programs:
h. Knowledge Gained from the Solution: Reduces phishing effectiveness and enhances users' security consciousness, enabling safer browsing.

With these strategies, you approach mobile banking security from multiple facets, addressing vulnerabilities with user centric and technical solutions.

DISCUSSION

This study recommends the significance of covering weaknesses in the mobile banking software to provide secure and reliable digital economic services. This discussion highlights the implications of the results, addresses the

appropriateness of the proposed mitigation strategies, and discusses how these findings fit into the existing literature.

Critical Vulnerabilities and Driving Consequences

It noted critical flaws in mobile banking apps such as insecure communication, unprotected storage and weak authentication. These vulnerabilities correspond with the OWASP Mobile Top 10 Risks which indicates the commonality of insecure storage or insecure communication channels (OWASP, 2022).

Unprotected Storage: As seen in Table 1, it is the local storage of sensitive data on devices without sufficient encryption that is the most severe risk, with a high impact on business. This presents evidence in support of Gupta et al. (2021) that storing session tokens and account information as plaintext greatly increases user risk if the device is lost or compromised by malware.

Insecure Communication: It was found that 60% of the identified applications within the study could be vulnerable to Man in the Middle (MITM) attacks by not implementing security measures to the communication protocols. Kumar and Hayward (2022) remarked on these vulnerabilities as well, and traced them to out of date SSL/TLS techniques and the absence of SSL pinning.

Weak Authentication: Apps with only single factor authentication showed high risk for unauthorized access. This poses a significant risk given the growing threat of phishing attacks and credential theft (Smith et al., 2023). (2020).

Mitigation Strategies and Their Effectiveness

They then assessed whether the proposed mitigation strategies could effectively address these vulnerabilities:

End-to-end Encryption (E2EE): Our results showed that E2EE is the best solution to secure communication channels and reduce the risk of compromising sensitive data to 5% (Table 3). This is consistent with Nguyen et al. (2021), which showed that data confidentiality is maintained by E2EE despite existence of network level threats.

Two Factor Authentication (2FA): MFA was the strongest authentication method with a 95% success rate and very high security level (Table 2). MFA adds an additional layer of protection against man in the middle attacks, as it requires the potential attacker to bypass multiple security measures (e.g., biometrics, passwords, etc) in order to access a user's account. This finding confirms Kumar and Hayward (2022) proposal to merge MFA in mobile banking applications.

Secure Coding Practices: A figure of 70% reduction in vulnerabilities was achieved in applications with comprehensive secure coding practices compared to applications with no secure coding implementation (Table 3). OWASP (2022) show you that this is an example why you should follow secure development guidelines.

User Education Programs: The researchers found that such users with high awareness by were very much more successful against phishing campaigning attaining a phishing success rate of 10% compared to the 70% attainment previously (see Table 3). Such finding validates that of Deloitte (2022)

that user education can help reduce the risk of cyberattack through social engineering.

Challenges in Implementation

While these strategies have been effective, there are some obstacles which should be addressed to enable the widespread adoption of these solutions:

Scalability of Solutions: Unlocking E2EE and MFA at scale can be an expensive infrastructure undertaking, which might be more or less easy for large or small to medium sized financial intuitions. Nguyen et al. Cost and resources tend to hold back security solutions (2021).

Security vs. Usability: Although MFA adds an extra layer of security, it also adds friction to the user experience, which makes it likely to be resisted by less eligible users. Smith et al. (2020) stresses creating easy to use systems for authentication to promote use.

Third Party Dependencies: Many applications depend on third party libraries and SDKs, which can create vulnerabilities, if not adequately vetted. Gupta et al. This is out of necessity, as reported by Gupta et al. (2021).

User Compliance: Despite strong security system in place, these strategies are only as effective as the user behavior. Users should be educated on best practices, and incentivizing secure behavior is an important part of reducing risks from phishing and social engineering attacks.

Practical Implications

These findings have important implications for financial institutions and mobile application engravers:

Improving User Engagement: Moreover, the use of encryption in the form of E2EE can notably enhance user confidence and engagement with your platform.

Increasing Access Security: Financial institutions should make it mandatory to adopt MFA and biometric authentication to avert unauthorized access.

Encouraging Secure Development Practices: Eminent development organizations should follow secure coding practices, perform regular vulnerability assessments of their applications and third-party components.

Educating Users: Financial institutions should implement educational programs that raise customers' awareness of how they can identify and avoid security threats.

CONCLUSIONS AND RECOMMENDATIONS

The rise of mobile banking apps has revolutionized the unique world of financial services through their convenience and accessibility. But this shift has also compromised users and institutions with huge security lapses. We assessed the vulnerabilities for mobile banking applications which include, insecure transportation, weak authentication, unprotected storage along with malware exploitation and proposed mitigation techniques. These findings challenge mobile banking service providers to rethink their security and risk approaches to be holistic and address technical, organization, and user relevant issues at large.

The perfect usage of mobile banking applications exposes the vulnerabilities of mobile banking applications.

a. Insecure Communication: A common type of Web vulnerability that allows unauthorized access to sensitive user information like passwords, session IDs, and other pertinent data through improper implementations of encryption protocols, leaving the data open to MITM attacks.
b. Unprotected Storage the Most Common Vulnerability
c. Single Factor Authentication: Single factor authentication can further lead to increased vulnerability to gaining unauthorized access and credential theft.
d. Third Party Dependencies: Shaky integrations with third party libraries and SDKs can create undiscovered vulnerabilities in the premises, and the need for extensive vetting processes.

In reaction to these findings, the study reviewed and suggested a number of mitigation strategies:

a. End-to-end Encryption (E2EE): It greatly minimizes the chances of data interception, providing secure communication channels.
b. Multi Factor Authentication (MFA): A more secure authentication mechanism that uses multiple verification factors to protect against unauthorized access.
c. Secure Coding Practices: Reduces vulnerabilities during development by following best practices like input validation and secure API usage.
d. User Education Programs: Improves user awareness reducing phishing effectiveness tackling the human part of the security.
e. Enhancing Security Protocols: Using modern days cypher and authenticator protocol.
f. Mobile Banking Applications: Security measures, in addition to user training programs, can build user trust in banking applications, leading to adoption and growth of mobile banking applications.
g. Regulatory Compliance: Institutions should comply with international security standards (GDPR, PCI DSS, etc.) to avoid penalties and maintain users' trust.

Recommendations and Challenges

There are well known strategies that work for mitigation, however, there are longstanding challenges:

Scalability: Smaller financial institutions may be limited by resources in terms of implementing solutions such as E2EE and MFA. Subsidies or shared security infrastructure initiatives from governments and regulators can also support these institutions.

Usability vs. Security Implementing stringent security measures while also ensuring a smooth user experience is an essential challenge. Designers should take an approach that embeds security in an intuitive manner without friction.

ADVANCED RESEARCH

There are limitations to this study such as limitation in sample size: A small set of mobile banking applications were analyzed. Future studies should look at a wider sample to generalize the results over a broader space and platform. Simulated Environment: Penetration tests were done in a controlled setup which may not be representative of the real-world complexities. Field studies in live environments should contain more insightful formulations. Emerging Technologies: Explore biometrics and Zero Trust Architecture to help future proof mobile banking security. Further studies should also explore the merging of mobile banking apps with new technologies such as blockchain, which allows for tamperproof transaction systems, and AI that creates real time fraud detection.

Both businesses and individuals rely on mobile banking apps, and they are just the right targets for cybercriminals. This data emphasizes the importance of taking a holistic approach in the security realm, where technical controls, such as encrypting sensitive data and enforcing multifactor authentication (MFA), should always be combined with secure coding techniques and user education. Financial innovations such as mobile banking can be offered through secure, resilient and easy to use systems through collaborative efforts between different parties to bridge the challenge. These initiatives will not only secure users' information but also help establish trust, promising a long-lasting expansion of digital finance worldwide.

REFERENCES

Deloitte. (2022). *Mobile banking fraud: An analysis of security vulnerabilities and financial impact*. Deloitte Insights.

Gupta, A., Sharma, R., & Li, H. (2021). *Threat landscape of mobile banking applications: A comprehensive review*. Journal of Financial Security, 15(3), 112129.

Kumar, S., & Hayward, D. (2022). *Cybersecurity in mobile banking: Trends, challenges, and solutions*. Financial Technology Journal, 8(2), 4567.

Nguyen, H. T., Pham, T., & Tran, Q. (2021). *Innovations in mobile banking security: A review of current practices and emerging trends*. International Journal of Financial Security, 14(1), 2348.

OWASP. (2022). *OWASP Mobile Security Testing Guide*. Retrieved from https://owasp.org

Smith, J., Brown, T., & Ahmed, Z. (2020). *Malware targeting Android banking apps: Trends and mitigation strategies*. Journal of Cybersecurity Research, 28(4), 305320.