Assessing security vulnerabilities in Sri Lankan banking mobile applications: challenges and solutions.

RAVICHANDRAN, L., PIYUMANTHA, K., WICKRAMASINGHE, W.S., WEERASINGHE, M. and SENANAYAKE, J.

2025

Assessing Security Vulnerabilities in Sri Lankan Banking Mobile Applications: Challenges and Solutions

Lavanya Ravichandran
dept. of Industrial Management
University of Kelaniya
Dalugama, Sri Lanka
rlavan0927@gmail.com

Kavindu Piyumantha
dept. of Industrial Management
University of Kelaniya
Dalugama, Sri Lanka
silvatkp@gmail.com

Waruna Sri Wickramasinghe
dept. of Industrial Management
University of Kelaniya
Dalugama, Sri Lanka
warunasri44@gmail.com

Malshan Weerasinghe
dept. of Industrial Management
University of Kelaniya
Dalugama, Sri Lanka
malshanweerasinghe25@gmail.com

Janaka Senanayake
dept. of School of Computing,
Engineering and Technology
Robert Gordon University
Aberdeen, United Kingdom
j.senanayake@rgu.ac.uk

***Abstract*—Mobile banking plays a crucial role in Sri Lanka's financial sector, offering convenience through self-service technologies. Despite its rapid adoption, concerns about security continue to affect customer trust, underscoring the critical need for enhanced protections and user experience. This study examines the security vulnerabilities present in mobile banking applications in Sri Lanka, evaluating their compliance with established security standards and the effectiveness of their security measures. Utilizing a quantitative methodology, the research employed the Mobile Security Framework (MobSF) to conduct static analysis on 17 mobile banking and digital wallet applications, selected to comprehensively represent nearly all mobile banking apps available in Sri Lanka. The findings reveal significant security flaws, including weak encryption methods, insecure data storage practices, and the absence of runtime integrity checks, resulting in widespread deviation from best practices. Most applications were classified as medium risk due to notable vulnerabilities. The research underscores the need for enhanced security protocols to safeguard user data, uphold customer trust, and ensure compliance with regulatory standards. It also identifies key areas for future research, including the integration of dynamic analysis, implementing real-time threat monitoring, and improving user awareness to mitigate risks and enhance the security landscape of mobile banking in Sri Lanka.**

Keywords—Android Security Vulnerabilities, Data Protection, Encryption Practices, Mobile Banking, Mobile Security Framework

I. Introduction

Mobile banking has become a cornerstone of Sri Lanka's financial sector, fueled by advancements in Information and Communication Technology [1]. Despite rapid adoption and the convenience of self-service technologies, concerns about security continue to impact customer satisfaction and trust [2]. App instability, poor customer service, and functional errors further highlight the need to enhance user experience [3] [4].

Banks in Sri Lanka promote Mobile Banking Services (MBS) through social media and television, but interpersonal communication remains the most effective way to build customer trust and drive adoption [1]. During the pandemic, health consciousness significantly influenced intentions toward mobile payments, presenting an opportunity for targeted campaigns [6]. Additionally, perceived risk and trust are key factors shaping public intentions toward Mobile Money Transactions (MMT), highlighting the importance of minimizing risks and fostering trust [2].

The introduction of innovative mobile money interfaces in Sri Lanka has shown mixed success in increasing savings deposits [7]. Addressing these challenges and capitalizing on opportunities are critical for sustaining the growth of mobile banking in the country [8].

Application security plays a crucial role in safeguarding user data and maintaining trust in digital transactions. Research emphasizes that application security significantly influences user trust in digital payments, highlighting the importance of secure platforms in prevent hacking, fraud, and phishing [9]. Organizations focus on application security to prevent data theft and minimize vulnerabilities, encompassing hardware, software, and procedures [10]. The increasing risks of unauthorized access and data misuse further stress the need for robust security measures to protect personal information, uphold privacy, and maintain public trust [11]. Implementing advanced data protection systems, such as utilizing blockchain technology for field-level encryption, enhances security without requiring extensive modifications to existing applications, ensuring comprehensive data protection and user trust [12].

Despite the availability of mobile banking systems, only 40% of users in Sri Lanka utilize them, primarily due to security concerns [13]. Factors influencing customers' behavioral intention to use mobile banking services in Sri Lanka include Perceived Trust (PT) and Perceived Compatibility (PC), with PT being identified as the strongest influencer [14]. Additionally, a study on Sri Lankan mobile banking apps revealed that unstable versions after updates, poor customer service, and functional errors contribute to customer dissatisfaction, impacting app ratings [4]. Furthermore, a broader study on banking apps highlighted numerous vulnerabilities in such applications, emphasizing the need for enhanced security measures and effective vulnerability detection tools to address these issues [15].

The objective of this study is to evaluate security vulnerabilities in Sri Lankan mobile banking applications, assess existing security measures, and benchmark them against industry standards. By identifying common issues, the study aims to provide actionable recommendations for enhancing app security. The paper is organized into several sections: it begins with an introduction to the importance of mobile banking in Sri Lanka and the role of application security in protecting user data. It then reviews related works on global security issues, specific challenges in Sri Lankan applications, and key security frameworks and measures. The methodology section details the research approach, data collection methods, and analysis techniques used in the study. Following this, the analysis and findings section presents the results of evaluating 17 mobile banking applications, highlighting identified vulnerabilities and their implications. The discussion section compares these findings with best practices, explores challenges in mobile banking security, and assesses the impact on the banking sector. Finally, the conclusion summarizes the key findings, discusses their significance, and outlines future research directions to improve mobile banking security in Sri Lanka.

II. Related Work

A. *Common security issues faced by mobile banking applications*

Research indicates that common security issues in mobile banking applications include information leakage, cryptography vulnerabilities, insecure SSL implementation, and poor code quality. Specific vulnerabilities such as wrong default permissions, cleartext storage of sensitive information, and the use of weak cryptographic algorithms are frequently identified [16][17][18]. Threats from malware and unauthorized access to personal and financial data arise from lapses in mobile security, highlight the need for robust security measures [19][20]. Additionally, outdated app versions and third-party libraries are vulnerable, emphasizing the importance of regular updates and patches to mitigate vulnerabilities [18]. In Sri Lanka, challenges such as poor communication of mobile banking services and lack of value-added propositions limit broader adoption, necessitating solutions to improve security, usability, and trustworthiness [1].

B. *The key security frameworks and standards for mobile banking applications*

Key Security frameworks for mobile banking include a comprehensive 26-criteria framework for Android banking applications, covering device security and cryptographic requirements [25]. Additionally, a mobile banking customer security model has been assessed as technically trustworthy [26]. Threat mapping and behavioral biometrics, such as touch dynamics, are employed for proactive threat mitigation and secure user authentication [19][27]. Furthermore, a blockchain-based framework incorporating multi-level authentication and two-factor authentication (2FA) has been suggested to enhance security in privacy-sensitive banking applications [28].

C. *Common security measures employed by banks to protect mobile applications*

Banks employ several critical security measures to ensure the safety of mobile applications such as certificate pinning to prevent man-in-the-middle (MITM) attacks [16], multi-level authentication, and 2FA for secure transactions [29]. Existing measures like hashing, role-based authentication, and preventing SQL injection ensure the Confidentiality, Integrity, and Availability (CIA) triad [30]. Additionally, secure coding practices, strong encryption algorithms, and proper storage for sensitive data mitigate vulnerabilities [16][20]. Banks also rely on encryption protocols managed by trusted servers, ensuring secure communication across different device applications while isolating roles within a defined security perimeter [31].

D. *The Role of User Education and Emerging Technologies*

Additionally, user education and awareness are vital in reducing security threats. Educating users about potential risks and safe practices can significantly mitigate behavior-driven vulnerabilities [19][24]. Emerging technologies like AI/ML and blockchain offer advanced security enhancements, though their integration requires balancing security measures with user convenience to avoid disrupting the overall experience [12][28][30]. These innovations, coupled with informed user behavior, are critical for strengthening security and promoting the adoption of mobile banking services.

Research must address regulatory changes and develop effective educational programs to improve user behavior and security awareness [22][23]. Additionally, regional-specific studies can address vulnerabilities unique to Sri Lanka, considering local cultural, technological, and economic factors [1][3]. Emerging technologies like AI/ML and blockchain offer advanced solutions for threat detection and secure transactions. Designing user-friendly security solutions, enabled by emerging technologies, present significant opportunities for innovation [12][28][31].

III. Methodology

This section outlines the research methodology employed in assessing the security vulnerabilities of mobile banking applications in Sri Lanka. The study adopted a quantitative approach, utilizing static analysis tools to evaluate the security levels of 17 banking and digital wallet apps. The applications analyzed include those from both government and private sector banks, ensuring comprehensive coverage of nearly all mobile banking applications available in Sri Lanka. The applications analyzed include those from both government and private sector banks. The primary objective was to identify common security issues and assess the overall security posture of these apps. For ethical reasons, code names (e.g., B1, B2) were used instead of actual app names.

A. *Research Approach*

The research followed a quantitative approach, focusing on the systematic measurement and statistical analysis of data collected from the applications. This approach was selected to provide an objective assessment of the security vulnerabilities present in the apps. By leveraging quantitative methods, the study aimed to derive statistically significant conclusions that could inform stakeholders about prevalent security issues in mobile banking applications.

B. *Data Collection*

The data collection process involved downloading the latest versions of the 17 banking and digital wallet apps directly from the Google Play Store. Only Android applications were considered for this study due to the widespread use of Android devices in Sri Lanka. This selection ensures the relevance and applicability of the findings to the most commonly used platform in the region, thus enhancing the impact of the study.

C. *Tools and Techniques*

Static analysis tools were employed, with the Mobile Security Framework (MobSF) being the primary tool utilized. MobSF, a widely recognized framework for assessing mobile application security, offers comprehensive analytical capabilities that were leveraged in this study.

D. Analysis Process

The analysis process was systematically structured to ensure a thorough evaluation of the mobile banking applications. Initially, the selected applications were downloaded from the Google Play Store, ensuring that the latest versions were analyzed. Each app was then subjected to static analysis using the Mobile Security Framework (MobSF). This static analysis encompassed several critical security aspects, including data encryption, secure storage, and application permissions, providing a comprehensive assessment of the app's security features. The results were carefully recorded in a specific structure to make sure that they could later be codified based on the applications' compliance with the rules. Moreover, a MobSF 100-point scoring system was proposed that should allow for the quantification of the applications' security quality.

In the case of the performed analysis, several static tools were used, which, however, were centered around the Mobile Security Framework. This is a relatively random tool that was chosen for the research because of its complexity. Thus, the analysis involved:

First, Code analysis involves the careful examination of the app's source code to identify relatively common and critical vulnerabilities, such as hard-coded keys, improper encryption, and data leakage. Thus, the analysis was supposed to render the basic weaknesses in the design of the applications.

Second, Permission analysis aims to arrive at a better understanding of the applications' design process by bringing to the fore unnecessary and dangerous permissions that the application requests. Thus, this part of the analysis is supposed to reveal potential threats to the users' privacy.

Third, Security configurations, such as SSL/TLS, and secure storage. The analysis of these factors was supposed to determine whether the apps live up to the best security practices. The role of the Mobile Security Framework can be defined by the fact that it is effective in detecting a broad range of different vulnerabilities. Moreover, it, unlike some other static analysis tools, does not rely on sources and products it must have in its main base, allowing for a more independent and broad analysis of the applications. Finally, in the framework of the performed research, the tools were used based on their accepting non-proprietary access to the code base.

Given the requirements of ethical standards, the research used the practice where the apps' names are replaced with "B1" and "B2". This practice was used to prevent public access to sensitive information regarding the flaws of specific applications.

E. Limitations and Future Work

The study provides valuable insights into the security vulnerabilities of Sri Lankan mobile banking applications, but it has certain limitations. First, the analysis was limited to static analysis using the Mobile Security Framework (MobSF), which does not capture runtime vulnerabilities or dynamic threats. Future research should integrate dynamic analysis for a more comprehensive assessment. Second, the study focused exclusively on Android applications, leaving iOS and other platforms unexplored. Expanding the scope to include iOS applications would provide a more comprehensive understanding of cross-platform security challenges. Third, the analysis was based on the app versions available at the time of the study, and newer versions may have different security postures. Longitudinal studies tracking security improvements over time would offer more robust insights. Finally, the study did not consider user behavior or security awareness, which are critical factors in mitigating risks. Future research should explore the impact of user education programs on improving security practices.

Future work should focus on several key areas. First, combining static and dynamic analysis techniques will provide a more holistic evaluation of mobile banking applications. Second, developing real-time monitoring tools to detect and mitigate emerging threats is essential for enhancing security. Third, pilot studies on user behavior and the effectiveness of educational initiatives can help identify gaps in security awareness. Fourth, expanding research to include iOS applications and other platforms will address cross-platform security challenges. Finally, exploring the impact of regulatory changes on mobile banking security and assessing compliance measures will provide valuable insights for policymakers and financial institutions.

IV. ANALYSIS AND FINDINGS

A. Vulnerability Identification

As the analysis of 17 mobile banking applications showed, many different security vulnerabilities could be defined in their functioning. Thus, security vulnerabilities encountered can be categorized into compliant and non-compliant. The key vulnerabilities include insecure data transmission, insecure data storage, poor encryption passing, lack of runtime integrity verification, and poor UI pass. Hence, the analysis of these applications revealed that online banking applications keep transmitting sensitive data without proper encryption protection as MITM attacks can decipher the data within the shortest period passing. It may be explained by the fact that many applications keep storing sensitive data in plaintext in internal storage, external storage, log files, and cache files, which makes it easy for an attacker to access and mode if the mobile device is compromised. The mobile applications were found to use outdated and weak encryption means, such as ECB mode and hardcoded keys frequently. Furthermore, most apps fail to use secure random values for their random IVs in CBC encryption. Besides, there are no runtime integrity verification checks in most apps, continuous uses. Poor UI pass is another significant problem as many applications have no method to turn off UI screenshots and no method to handle UI security.

B. Assessment of Security Measures

The presented applications have been assessed as to whether the implemented security measures are effective at protecting user data and ensuring the integrity of applications. The method of assessment has been based on how properly the encryption has been used, the means of data protection have been implemented, and the authentication and access control measures have been employed. It is evident that most applications use some form of encryption, yet the quality and ways of its implementation vary widely. It is generally important for the safety of sensitive data that it be encrypted both at rest and in use, yet this requirement has not been met in the majority of applications. The appropriateness of data protection means has also been explored, including using SharedPreferences in private mode. The assessment has revealed that not all applications follow best practices in this regard. Lastly, the means of access identification and control have been explored, with the samples including limiting the number of attempts at login and limiting the access of the administrative method. The respective assessment has shown that these measures are also applied variably.

C. Security Level Determination

The assessment of the overall security level of each application was made based on the quantity and severity of vulnerabilities found. The identified features are classified into three risk levels according to MobSF: Low Risk, Medium Risk, and High Risk. The assessment was made using the scoring system based on the number of running compliant and non-compliant features of applications. Low-risk applications were found to possess a large number of existing compliant features and a small number of critical outstanding vulnerabilities, indicating a relatively strong security posture. Medium-risk applications had fewer compliant security features than low-risk ones and exhibited a moderate level of vulnerabilities. All other applications, with a high number of critical vulnerabilities and poor compliance with security norms, were classified as high-risk.

V. Discussion

A. Challenges in Mobile Banking Security

The analysis also highlights several common challenges associated with securing the mobile banking application. The rapid development cycle often requires shortcuts in security implementation, with developers focusing on delivering functionality and user experience over security measures which can lead to major vulnerabilities. The complexity of mobile ecosystems which includes different devices, operating systems, and their versions makes it difficult to maintain consistent security for all users. Depending on the device, and often on the software version, a mobile banking application may offer different levels of security. On top of that, the behavior of a user and their security awareness make it difficult to maintain security. Users' limited knowledge of best security practices, such as recognizing phishing attempts or using secure networks, may make even properly implemented security measures ineffective. Another important challenge to maintain security is the rapidly changing nature of the threat. Currently, new types of attacks directed at mobile banking applications, such as malware, phishing, or social engineering, are being developed, and maintaining up-to-date security requires implementing protection that can no longer be secure. Smaller banks and financial institutions may not have the resources or expertise needed to implement proper security and may rely on outdated systems and ineffective practices. Overall, properly implementing effective measures could help to improve the security of mobile banking applications through multiple channels and defend the data delivered through mobile banking against potential threats that could damage institutions and lead to user losses.

B. Comparison with Best Practices and Industry Standards

According to the performed analysis, there is a considerable deviation from established security best practices and industry standards. In particular, the OWASP Mobile Security Testing Guide recommends using a strong encryption algorithm, such as AES with CBC mode, and secure initialization vectors for the protection of the data at rest and in transit. However, most applications used old or insecure methods, such as the ECB mode or hard-coded keys. Similarly, the industry standard is to keep the data stored securely, encrypted, and not in plaintext, but this is not being followed as evidenced by the number of applications that implemented this method (Fig.1). Additionally, many comprehensive security features, including integrity checks, secure generation of random numbers, and proper session management are standard for a secure mobile application, mainly when combined with multiple levels of communication security. However, in most cases, these features were either inadequately implemented or not implemented at all.

C. Implications of Findings

The static analysis of 17 mobile banking applications revealed that all applications contain several severe vulnerabilities (Table I) that compromise data security. One major issue is improper data handling, such as storing sensitive client information in plaintext or implementing inadequate security measures (Fig. 2). This is critical because many other vulnerabilities may become significant only when an attacker gains access to this information. If an attacker obtains it, they can easily retrieve the client's data. At the same time, multiple offensive security scenarios exist where sensitive information is extremely valuable. In the case of a data breach, this may cause severe privacy violations, identity theft, unauthorized fund withdrawals, or even fraudulent credit applications using the victim's data. Another vulnerability is the weak encryption used. While AES-128 is considered secure, attackers may still breach it relatively quickly. The lack of proper encryption for data transmission may lead to a MITM attack, allowing an adversary to interfere with data transmission. Crypto tokens and the server certificate should not be compromised, as their breach

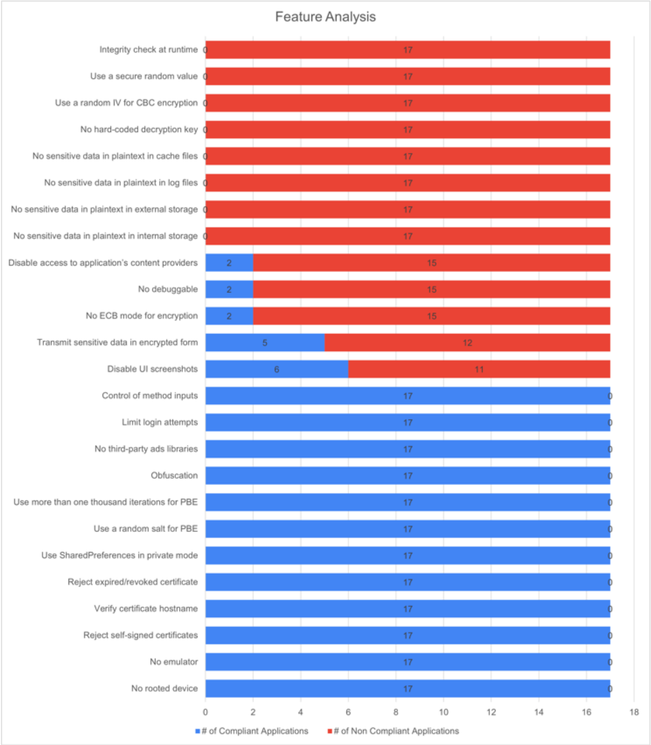

Fig. 1. Feature Compliance Analysis: A comparison of compliant and non-compliant mobile banking applications based on key security features.

Table I. Security Assessment Table: Detailed compliance analysis of mobile banking applications across various security criteria, with an overall risk rating and score for each application.

Criteria	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16	B17
No rooted device	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
No emulator	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reject self-signed certificates	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Verify certificate hostname	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reject expired/revoked certificate	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Transmit sensitive data in encrypted form	✗	✓	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
No sensitive data in plaintext in internal storage	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
No sensitive data in plaintext in external storage	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
No sensitive data in plaintext in log files	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
No sensitive data in plaintext in cache files	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Use SharedPreferences in private mode	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
No hard-coded decryption key	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
No ECB mode for encryption	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Use a random IV for CBC encryption	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Use a random salt for PBE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Use more than one thousand iterations for PBE	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Use a secure random value	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Disable UI screenshots	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✓	✗	✗	✗	✗	✓	✓
Obfuscation	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
No debuggable	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
No third-party ads libraries	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Limit login attempts	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Integrity check at runtime	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Disable access to application’s content providers	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Control of method inputs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Overall Security Assessment By MobSF(Risk Level)	Medium	Medium	Medium	Medium	Medium	Low	Low	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium	Medium
Score out of 100 by MobSF	46	57	48	47	54	67	65	49	46	58	47	43	52	47	40	46	47

allows attackers to hijack the connection between a user and a bank. This, in turn, may enable uncontrolled transactions or access to sensitive financial data. Finally, the absence of runtime integrity checks and the presence of a debuggable flag indicate that the application is accessible by any client and is not fully secured. This could result in unintended execution, behavior manipulation, injection of malicious code, or unauthorized access. Trust-destroying threats may reduce app compatibility or severely damage the reputation of financial institutions.

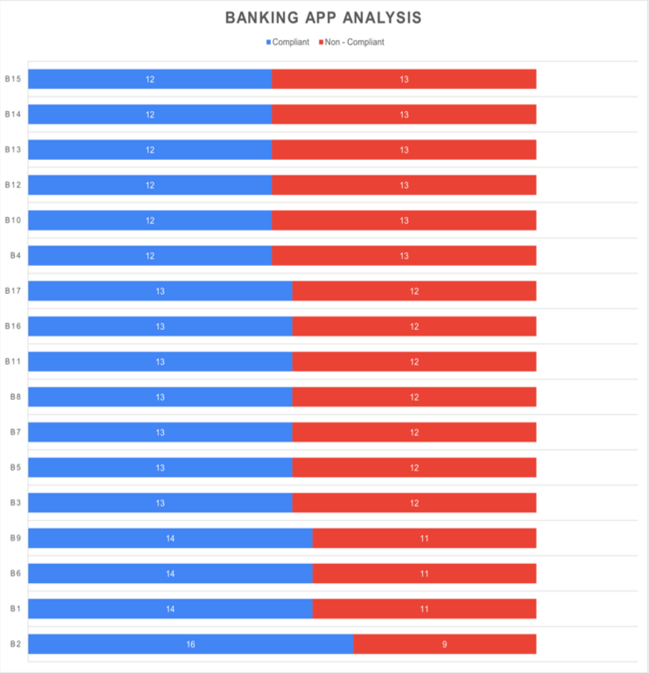

Fig. 2. Application Compliance Analysis: A bar chart illustrating the count of compliant and non-compliant security features for each analyzed mobile banking application.

VI. Conclusion

The comprehensive evaluation of 17 mobile banking applications in Sri Lanka revealed notable security vulnerabilities across various dimensions. The analysis indicated widespread non-compliance with fundamental security practices, including inadequate encryption of sensitive data, insufficient session management, and poor coding practices. Identified vulnerabilities comprised the use of weak encryption methods such as ECB mode and hard-coded keys, the storage of sensitive information in plaintext, and a lack of runtime integrity checks. The security assessment classified most applications as medium risk, with a few rated as low risk, but none as high risk. This classification suggests an awareness of security needs, yet highlights significant areas requiring improvement. The improper handling of sensitive data, combined with inadequate protection mechanisms, poses a substantial risk to user information, potentially exposing it to data breaches, identity theft, and unauthorized transactions.

The identified vulnerabilities carry critical implications for both the banking sector and its clientele. The erosion of customer trust is a significant concern, as these vulnerabilities can undermine confidence in mobile banking services. Trust is a fundamental element of financial services, and exposure of such security weaknesses may lead to reduced adoption rates, customer dissatisfaction, and potential reputational damage for the banks involved. Additionally, the lack of robust security measures may attract regulatory scrutiny and potential penalties for non-compliance with data protection laws and industry standards. Financial institutions could also face legal liabilities in the event of data breaches. Furthermore, banks that neglect security may experience a competitive disadvantage, as customers are likely to prefer institutions that offer stronger security assurances and better protection of their financial information.

The findings of this study underscore several areas for further research and development. Combining dynamic and static analysis can provide a comprehensive evaluation of mobile banking applications by identifying runtime vulnerabilities related to network communication and user interactions. Future research should focus on developing dynamic monitoring tools to detect and mitigate real-time threats in mobile banking applications. Additionally, pilot studies on user behavior can assess the effectiveness of educational initiatives and identify gaps in security awareness. Expanding research to include iOS applications and conducting longitudinal studies to monitor security improvements over time will provide a more holistic understanding of mobile banking security. Addressing cross-platform security challenges, particularly for Android and iOS, is essential to ensure consistent security measures and address device-specific vulnerabilities. By tackling these challenges, banks can strengthen the security of Sri Lankan mobile banking applications, safeguard customer data, uphold trust, and ensure the secure delivery of digital financial services.

REFERENCES

[1] S. Ruwini and G. Pushpika, "Communication and Adoption of Mobile Banking Services in Sri Lanka," Asian Journal of Economics Business and Accounting, vol. 24, no. 3, pp. 147-156, Feb. 2024, doi: 10.9734/ajeba/2024/v24i31248.

[2] U. A. Jayaweera, "Analyzing the effectiveness of Mobile Banking on Customer Satisfaction; A survey on the XYZ Bank PLC with specific reference to branch Thalawathugoda, Sri Lanka," International Journal of Scientific and Research Publications, vol. 12, no. 11, pp. 83-90, Nov. 2022, doi: 10.29322/ijsrp.12.11.2022.p13111.

[3] A. N. Jayasinghe and Amila. S. Withanaarachchi, User Experience in Mobile Banking Applications in Sri Lanka: A Systematic Literature Review. 2024, pp. 264-269. doi: 10.1109/icarc61713.2024.10499765.

[4] M. S. Sally, "Why are consumers dissatisfied? A text mining approach on Sri Lankan mobile banking apps," International Journal of Intelligent Computing and Cybernetics, vol. 16, no. 4, pp. 727-744, May 2023, doi: 10.1108/ijicc-02-2023-0027.

[5] S. Subasinghe, S. Mirihagalla, T. Welivitage, and L. Gunathilake, "Public Intention towards Mobile Money Transactions in Sri Lanka," KDU International Research Conference 2020, Oct. 2020, [Online]. Available: http://ir.kdu.ac.lk/handle/345/3054

[6] N. J. Dewasiri, K. S. S. N. Karunarathna, M. S. H. Rathnasiri, K. Sood, and A. Saini, "The Role of Health-Related Perceptions on Mobile Payment Adoption: Evidence from the Mobile Banking Industry in Sri Lanka," in Contemporary studies in economic and financial analysis, 2023, pp. 67-86, doi: 10.1108/s1569-37592023000111c004.

[7] S. De Mel, C. McIntosh, K. Sheth, and C. Woodruff, "Can Mobile-Linked Bank Accounts Bolster Savings? Evidence from a Randomized Controlled Trial in Sri Lanka," The Review of Economics and Statistics, vol. 104, no. 2, pp. 306-320, Aug. 2020, doi: 10.1162/rest_a_00956.

[8] P. Rawat and S. Sharma, "KEY DRIVERS AND CHALLENGES FOR THE ADOPTION OF MOBILE BANKING APPLICATION," International Journal of Global Research Innovations & Technology (IJGRIT)., vol. 02, no. 03, pp. 65-73, Sep. 2024, doi: 10.62823/ijgrit/02.03.6841.

[9] M. Rabbani, J. D. Wijaya, R. S. Kusuma, W. B. P. Purba, and R. M. Tajib, "Digital Payments in Indonesia: Understanding the Effect of Application Security on User Trust," Indonesian Journal of Computer Science, vol. 12, no. 5, Oct. 2023, doi: 10.33022/ijcs.v12i5.3426.

[10] S. Lad, "Application and data security patterns," in Apress eBooks, 2022, pp. 111-133. doi: 10.1007/978-1-4842-8936-5_5.

[11] A. Pant, "Importance of Data Security and Privacy Compliance," International Journal for Research in Applied Science and Engineer- ing Technology, vol. 11, no. 11, pp. 1561-1565, Nov. 2023, doi: 10.22214/ijraset.2023.56862.

[12] "Siddhartha Dutta Inventions, Patents and Patent Applications - Justia Patents Search." https://patents.justia.com/inventor/siddhartha-dutta

[13] L. C. Senanayake, "Evaluating security provisions in banking software systems," 2019. [Online]. Available: https://openrepository.aut.ac.nz/handle/10292/12911.

[14] S. S. Nawaz and F. B. M. Yamin, "Sri Lankan customers' behavioural intention to use mobile banking: a structural equation modelling approach," Journal of Information Systems & Information Technology (JISIT), Jan. 2018, [Online]. Available: http://192.248.66.13/handle/123456789/3018

[15] S. Chen et al., Are mobile banking apps secure? what can be improved? 2018. doi: 10.1145/3236024.3275523.

[16] E. E. Archibong, B. U.-A. Stephen, and P. Asuquo, "Analysis of cybersecurity vulnerabilities in mobile payment applications," Archives of Advanced Engineering Science, Jun. 2024, doi: 10.47852/bonviewaaes42022595.

[17] A. Sharma, S. K. Singh, S. Kumar, A. Chhabra, and S. Gupta, "Security of Android Banking Mobile apps: challenges and opportunities," in Lecture notes in networks and systems, 2023, pp. 406-416. doi: 10.1007/978-3-031-22018-0_39.

[18] S. Chen et al., An Empirical assessment of security risks of global Android Banking apps. 2020, pp. 1310-1322. doi: 10.1145/3377811.3380417.

[19] A. Chattopadhyay and D. Sripada, "Security analysis and threat modelling of mobile banking applications," 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), Jul. 2023.

[20] V. K. Malviya, P. Phan, Y. N. Tun, A. Ching, and L. K. Shar, "An industrial practice for securing Android apps in the banking domain," 2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE), pp. 1870-1875, Sep. 2023.

[21] S. Dandeniya, "EXPANDING FINANCIAL SERVICES FRONTIER AND MOBILE BANKING IN SRI LANKA," 26th Anniversary Convention 2014, Commercial Bank of Ceylon PLC, Jan. 01, 2014. [Online]. Available: http://www.apbsrilanka.org/articales/26_ann_2014/25_26th_Sunari_Dandeniya.pdf

[22] C. M. Suwandaarachchi, S. Bahri, and A. Fauzi, "Collaborative regulatory development in Sri Lankan Mobile Money Sector for financial inclusion.," Pacific Asia Conference on Information Systems, p. 153, Jan. 2018, [Online]. Available: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1152&context=pacis2018

[23] L. C. Senanayake, "Evaluating security provisions in banking software systems," 2019. [Online]. Available: https://openrepository.aut.ac.nz/handle/10292/12911

[24] B. A. L. Madhushani, "Challenges in mobile application testing: Sri Lankan Perspective - ProQuest." https://www.proquest.com/openview/317d6726c20b127e568ada484e8b0845/1?pq-origsite=gscholar&cbl=2032622

[25] L. D. Tsobdjou, S. Pierre, and A. Quintero, "A Framework for Security Assessment of Android Mobile Banking Applications," Computer Networks and Communications, Mar. 2024, pp.49-61.

[26] N. Rawat, D. Bordoloi, and A. Dumka, Framework for the Provision of User Felt Protected Mobile Banking Services. 2022, pp. 5-9. doi: 10.1109/icfirtp56122.2022.10059415.

[27] P. P. M. A. B. Estrela, R. De Oliveira Albuquerque, D. M. Amaral, W. F. Giozza, and R. T. De Sousa J√∫nior, "A Framework for Continuous Authentication Based on Touch Dynamics Biometrics for Mobile Bank- ing Applications," Sensors, vol. 21, no. 12, p. 4212, Jun. 2021.

[28] J. B. Awotunde, R. O. Ogundokun, S. Misra, E. A. Adeniyi, and M. M. Sharma, "Blockchain-Based framework for secure transaction in mobile banking platform," in Advances in intelligent systems and computing, 2021, pp. 525-534. doi: 10.1007/978-3-030-73050-5_53.

[29] J. B. Awotunde, C. Chakraborty, and S. O. Folorunso, "A secured transaction based on blockchain architecture in mobile banking platform," International Journal of Internet Technology and Secured Transactions, vol. 12, no. 4, p. 287, Jan. 2022, doi: 10.1504/ijitst.2022.124470.

[30] V. P. Bhosale, P. G. Naik, S. B. Desai, and P. Patekar, "Secure QR code transactions using mobile banking app," in Lecture notes in networks and systems, 2023, pp. 35-46. doi: 10.1007/978-981-99-0838-7_4.

[31] H. A. Moen and V. Erik, "Secure mobile platform," Jul. 2019. [Online]. Available: https://search.patentstyret.no/tidende/patent/2019/patenttidende-nr28-2019.pdf.