ISSN: 2182-2069 / E-ISSN: 2182-2077

Revolutionizing Mobile Banking System: Novel ML-Based Approach for Securing Cloud Data

Dr. Meenal R. Kale[1*], Dr. Itikela Shyam Sundar[2], Dr. Bhuvana Jayabalan[3], Dr. Bineet Desai[4], Dr. Akash Kumar Bhagat[5], and Dr. Sachin S. Pund[6]

[1*]Assistant Professor, Department of Humanities, Ycce, India. meenalycce@gmail.com, https://orcid.org/0000-0002-1623-2012

[2]Associate Professor, College of Business and Economics, Department of Accounting and Finance, Assosa University, Ethiopia. drishyam@asu.edu.et, https://orcid.org/0009-0003-1847-5151

[3]Associate Professor, Department of Computer Science and Information Technology, Jain (Deemed to Be University), Bangalore, Karnataka, India. j.bhuvana@jainuniversity.ac.in, https://orcid.org/0000-0002-8372-6311

[4]Professor, Department of Isme, Atlas Skilltech University, Mumbai, Maharashtra, India. bineet.desai@atlasuniversity.edu.in, https://orcid.org/0009-0008-7664-225x

[5]Assistant Professor, Department of Computer Science & IT, Arka Jain University, Jamshedpur, Jharkhand, India. akash.b@arkajainuniversity.ac.in, https://orcid.org/0000-0001-8717-764x

[6]Assistant Professor, Mechanical Engineering, Ramdeobaba University, Rbu, Nagpur, Maharashtra, India. pundss@rknec.edu, https://orcid.org/0000-0002-5616-2469

Received: November 22, 2024; Revised: January 04, 2025; Accepted: January 25, 2025; Published: February 28, 2025

Abstract

The mobile banking system allows consumers to access financial services through mobile phones. It includes services like money transfers, account balance checks and bill payments. Robust data security methods, including encryption and multi-factor authentication, secure user information while preserving the confidentiality and integrity of financial transactions, therefore increasing confidence in the system. In this research, we intend to develop an innovative novel machine learning (ML)-based approach for securing cloud data in mobile banking systems. The cloud computing risk management paradigm enhances financial security. To improve consumer services and banking experiences while maintaining information security, this study explains how mobile cloud architecture might be implemented. This article addressed several difficulties associated with mobile banking, including processing speed and storage capacity, by concentrating on cloud-based risk management for banking systems. We proposed versatile Adaptive Boosting (V-AdaBoost) to improve effectiveness in learning by selecting characteristics and training bank individuals. We implemented our suggested approach in Python software. The performance assessment step employs various metrics to assess the efficacy of the suggested prediction model. We performed a comparative study with other existing methods and the results demonstrate that the suggested model performed better than other conventional methods for securing cloud data in mobile banking systems.

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 170-181.
DOI: *10.58346/JISIS.2025.I1.011*

*Corresponding author: Assistant Professor, Department of Humanities, Ycce, India.

Keywords: Mobile Banking System, Machine Learning (ML), Versatile Adaptive Boosting (V-AdaBoost), Cloud Data, Security.

1 Introduction

Mobile phone interaction is gaining popularity in the corporate world. Nowadays, it is common to utilize a lot of SIM cards for devices and phones. The development allowed customers to easily access their mobile banking products (Karjaluoto et al., 2019). Mobile banking initially developed from secure online banking (Ho et al., 2020), which had Internet banking as its fundamental feature. Other than electronic mobile banking (M-B), money transfers provide a variety of services comparable to those available in traditional bank facilities. Mobile banking has a bright future in developing nations (Prastya et al., 2015). Banks implement security measures such as computerized device (Hrytsyna et al., 2019) endorsements, extortion, program assurance techniques, exchange monitoring, anti-tax evasion and secret key tokens detection frameworks as part of their specialized foundation. These tools and frameworks enhance bank security while meeting administrative requirements for customer information security (Weippl et al., 2011; Ojaghloo & Jannesary, 2015). Banking and financial companies offer products and services online through ATMs located in remote places, eliminating the need for consumers to visit physical facilities (Pakurár et al. 2019). Adaptability will be required (Gayarathi et al., 2018).

These services are accessible without visiting the bank's physical location. These artifacts are accessible over the internet. This enables banks to improve operational efficiency by delivering services faster, lowering branch costs, employing fewer staff, providing comprehensive assistance, offering faster options and focusing on client needs to provide personalized services. Countries that are developing to become more reliant on mobile services for a variety of functions (Hinson et al., 2019). A mobile banking service offers financial services such as money transfers, paying bills, and support for customers. Mobile banking services allow for money transactions on mobile phones (Singh and Srivastava 2020). It may be used remotely at any time and from any location using mobile gadgets. Mobile banking is accessible all day and night. Mobile banking is seen as more dependable compared to banking online (Sathyanarayana & Laxmana Rao, 2024).

Mobile phone banking functions include account messages, alerts about security, support for customers, account balance updates, and bill payments via mobile client and commerce applications. Mobile financial service allows for easy access to customer service (Bojjagani et al., 2023). Mobile phones offer the necessary graphical user interface for basic mobile payment technologies. These applications offer speedier and more dependable services in rural locations than conventional or online banking options. Client apps and components of the server can provide full functionality with robust authentication and modification (Al-Zubaidie et al., 2019). Mobile phone applications for clients are designed to meet market expectations. Mobile phone applications for clients employ phones to contact websites to conduct transactions in banks. The technology provides powerful verification (Tsai and Su 2021). Developing programs that work on several mobile phone models requires careful consideration of both software and hardware compatibility.

The objective of this endeavor is to provide a creative V-AdaBoost technique for securing cloud-based information in the form of mobile banking, hence improving financial safety and trust among consumers through improved services (Zendehboudi et al., 2018). Section 2 provides information on the related work. Section 3 discusses the online banking system and its software architecture, as well as the conceptual architecture and cloud risk administration approach for the banking system, and mobile cloud structures to offer safety for online financial systems. Section 4 presents the research results and comments. Findings are offered in the last parts.

2 Related Work

The study of (Butt et al., 2020) outlined Cloud computing (CC) safety concerns and explored diverse machine learning approaches. They examined multiple strategies, including supervised, unsupervised, and semi-supervised learning, assessing their efficiency and suggesting future research paths for secure CC models.

Researchers (Wang et al., 2021) devised a machine learning-driven intrusion detection system for diverse client-based portable clouds. Their approach, adaptable to client network requirements, eliminates the need for rule adjustments. It comprised multi-layer traffic filtering and decision-based Virtual Machine (VM) deployment, demonstrating high efficiency in intrusion detection through tests.

The author of (Tseng et al., 2021) analyzed the use of the dissemination of idea theory to create a "smart product service system (SPSS)" system for the banking sector. That developed a hierarchical SPSS model with seven traits and 22 criteria to improve papers and drive operating initiatives. Causal connected between features were established using a hybrid fuzzy Survey and evaluation laboratory technique and fuzzy decision-making test, emphasizing relevant aspects such as institutional digital platform operation, compression and e-knowledge management.

Investigation of (Nawrocki et al., 2019) evaluated the possibility of applying ML and the code offloading process in the mobile phone cloud computing concept, which might allow the use of services to be improved, among other issues on mobile devices. Reducing the level of work necessary from developers because identical code executed on a mobile gadget and in the clouds. According to the test results, mobile devices perform the best. The author of (Nguyen et al., 2019) proposed a revolutionary Electronic Health Records (EHR)-sharing infrastructure that blends blockchain with the anonymous "interplanetary file system (IPFS)" on a mobile cloud-based system. Also, they created an effective authorization method that uses smart contracts to facilitate safe EHR exchange across various patients and healthcare providers. The system assessment and safety analysis show improved performance when relative to previous sharing of data methods (Sreevidya & Supriya, 2024; Hrunyk, 2018).

The study of (Carbo-Valverde et al., 2020) assessed bank clients' digitalization progress through a large-scale financial study and ML techniques. They examined factors influencing customers' digitalization, decision sequences and potential associations. Findings suggested banks should categorize clients based on preferences and provide personalized online services to address digital evolution effectively.

3 Methodology

3.1 Internet-Based Banking Network

Clients can access their accounts using personal banking sites, enabling online banking. Customers can conduct financial activities electronically using the Internet. This digital payment method enables users to conduct payment orders, balance inquiries, bill payments and slow down payments through the website of a bank from any place in the world. To begin, the bank consumer must register on their official website. Customers can conduct financial transactions electronically using the Internet. For authentication on the website of the bank, customers have to generate a user account name and password.

3.2 Architecture of Software

The software architecture establishes a foundational connection among components and connectors, which focus on system development. The architectural design of software attempts to satisfy specific quality criteria for a system that uses software. During the implementation of the system, particular settings are taken into account. The banking system prioritizes qualitative traits for performance. Confidentiality and dependability are essential as both bank personnel and consumers use the same platform to conduct transactions.

3.3 Bank System's Conceptual Architecture

The conceptual architecture explains an arrangement utilizing its principles and capabilities.

The banking method's conceptual design encompasses three distinct levels. The first level covers bank kinds, transactional types and different ways of operation. The second level defines the three types of banks: international, national, and local. The Level 3 transactions may occur place in numerous locations (e.g., mobile, online, or local bank branches) and techniques (online transfer, check, or cash).

3.4 Model for Cloud Risk Management

Methods for risk management have been implemented for systems of information in IT projects. We recommend a risk management strategy as a cost-effective way to maintain project quality and interoperability. It increases the likelihood that a software project will be successful. The cloud computing risk management paradigm has the potential to improve the financial system's security.

3.5 Recommend Cloud Risk Safety Framework for Mobile Phone Banking Systems

Researchers proposed a cloud-based framework for risk management. The framework consists of five main components: Cloud deployment services, cloud mobility and banking apps, risk management operations, cloud security services and cloud service operations. IaaS is the most widely utilized cloud service paradigm. This section covers the resources of computers, including Computers, whether real or simulated, encompass virtual machines, storage components, network components and servers.

V-AdaBoost is an adaptive behavior iterative method. The algorithm chooses key characteristics from a large candidate collection and creates a weak predictor for each one. The weaker trainees are united to form a stronger group. This approach assigns a weight to each training sample based on its likelihood of being picked by an algorithm for its training set. Incorrect classification results in increased weight. This strategy allows the V-AdaBoost algorithm to focus on training difficult data. The V-AdaBoost method has limitations such as a sluggish pace of training and dependence on. This study is looking to improve the V-AdaBoost method.

The trained sample set $(w_1 z_1), (w_2, z_2), \cdots (w_m, z_m) w_j \in w$, and the classification signal $z_j \in z$ are used. In equation $z = \{0,1\}$, $z = 0$ represents instances of negativity (non-face), whereas $z = 1$ represents positive examples. The total amount of samples used for training is denoted by "m". $x_{s,j}$ represents the error in the weights in j th sample for the sth cycle. Initializing weight, when $z_1 = 0$, $x_{s,j} = {}^{1}/_{(2n)}$ and when $z_j = 1, x_{1,s} = {}^{1}/_{(2k)}$ The variables n and J represent the total amount of non-face examples and face examples, correspondingly.

For $s = 1, \cdots, S$; The weight was normalized ; $x_{s,j} = x_{s,j} \,/\, \left[\sum_{i=1}^{m} x_{s,j}\right]$, For each feature, i, trains its weak classifier $g_i(w, e, o, \theta)$ to determine the threshold θ_j and the offset p_i , so it could obtain the minimum value of the d function (Eq. (1))

$$\varepsilon_i = \sum_{j=1}^{m} x_{s-i} \mid h_i(w_j) - z_j| \tag{1}$$

After determining the weak categories in the second step, choose the weak predictor g that has the lowest error rate ε_s. The fourth step of this workout, set the weight increase threshold. To modify the resultant weight, use $GX_s = \left(\sum_{i=1}^{m} x_{s,i}\right) / m$ in (Eq. (2)).

$$\begin{cases} \frac{x_{s,i}\beta_s}{Y_s} & if\ g_s(w_j) = z_1 \\ \frac{x_{s,i}\beta_s^{-1}}{Y_s} & if\ g_s(w_j) \neq z_1, x_{s,i} \leq Gx_s \\ \frac{x_{s,i}\beta_s}{Y_s} & if\ g_s(w_j) \neq z_j x_{s,i} > Gx_s \end{cases} \tag{2}$$

Where $\beta_s = {}^{\varepsilon_s}/_{(1-\varepsilon_s)}$, y, is the factor to make $\sum_{i=1}^{m} x_{s,i} = 1$, and GX_s is the weight update threshold for this training. The final powerful classifier is (Eq. (3)):

$$d(w) = \begin{cases} 1 \ \sum_{s=1}^{S} \alpha_s, g_s(w) \geq \frac{1}{2} \ \sum_{s=1}^{S} \alpha_s \ \alpha_s = lo\, g\, \frac{1}{\beta_s} \\ 0 \qquad else \end{cases} \tag{3}$$

The technique increases the total weight of an object if it is incorrectly recognized and its current weight (x) is less than GX during this portion of the cycle. Besides, it should be lowered. This method ensures that even if tough samples are incorrectly classified throughout a cycle, their overall weight is not significantly raised. This can reduce classifier deterioration. Training speed is influenced by several parameters, including algorithm, set of training data size and feature.

For receiving optimal detection outcomes, the number of training sets should not be lowered. Instead, we can reduce the number of features.

3.6 Mobile Cloud Infrastructure for the Online Banking System

The infrastructural layer, that is cloud computing has three different delivery techniques; these are SaaS, IaaS, and PaaS. Platform as a Service is used to construct programs that could be used commercially. IaaS is a service that provides computer, network and storage resources. Based on the cloud architecture provides secure open-source cloud and secure internet services. Client, the transaction, wire and relationship with the client's data are among the data connection layer's different categories. Hadoop may be used to manage operational data. Created at lower prices with less work than standard data technology. Hadoop-based systems use predictive algorithms to store data for extended periods. Massive computations can be completed quickly. The API and UX layer enable smooth online banking and mobile payment transactions. In figure 1 shows the A Mobile Cloud Framework for Online Financial Systems below.

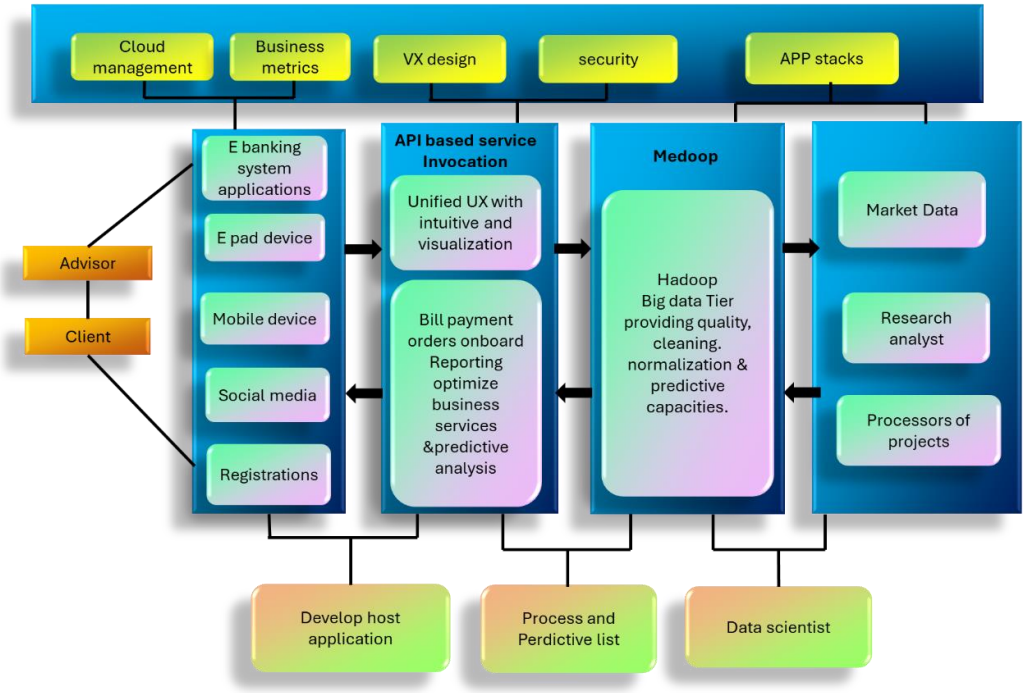

Figure 1: A Mobile Cloud Framework for Online Financial Systems

Banking Information Security Management Services and cloud infrastructure for banks and financial institutions should be inside the country's legislation. Clients accessing cloud foundations are located far away. Clients that manage cloud-based services might disseminate data to optimize cost-effectiveness. However, these customers require supervision from someone with access to the entire structure. Consumers may change over time, leading to different approaches to the structure and knowledge. Banking operations are evaluated for addressing information privacy and security concerns. Forensic capability and secure data destruction.

4 Result

Our technique was developed in Python (v 3.11) on Windows 10. The system is powered by an Intel Core i5 CPU and a high-performance graphics card, making capable of handling complex machine-learning tasks. Consumers might access these services using mobile banking. Mobile phone banking systems are either extremely or moderately secure. We should consider the security of the PIN. The Table 1 describes somebody's PIN outside of the requisite authorization. 50% of the participants believe that accessing someone's PIN without verification is too difficult. That provides information on mobile transfer protection, while Figure 2-A provides a visual illustration.

Table 1: Safety when Using Mobile Transfers

Difficulty Levels of Respondents	Safety of PIN	Percentage
Total number of respondents	56	100
Advanced security	30	53.6
Basic security	20	35.7
Undefined security	4	7.1
Robust security	2	3.6

The illustration in Figure 2-B depicts the PIN/Percentage safety features. Table 2 presents a pattern investigation into mobile phone clients in banking. Table 3 shows growth evaluations for mobile banking users.

Table 2: Another User has Access to the User's PIN

Difficulty Levels of Respondents	Safety of PIN	Percentage
Total number of respondents	55	100
Extremely challenging	10	23.24
Highly demanding	9	20.92
Simple	5	11.61
Effortless	13	30.21
Moderate	6	13.99

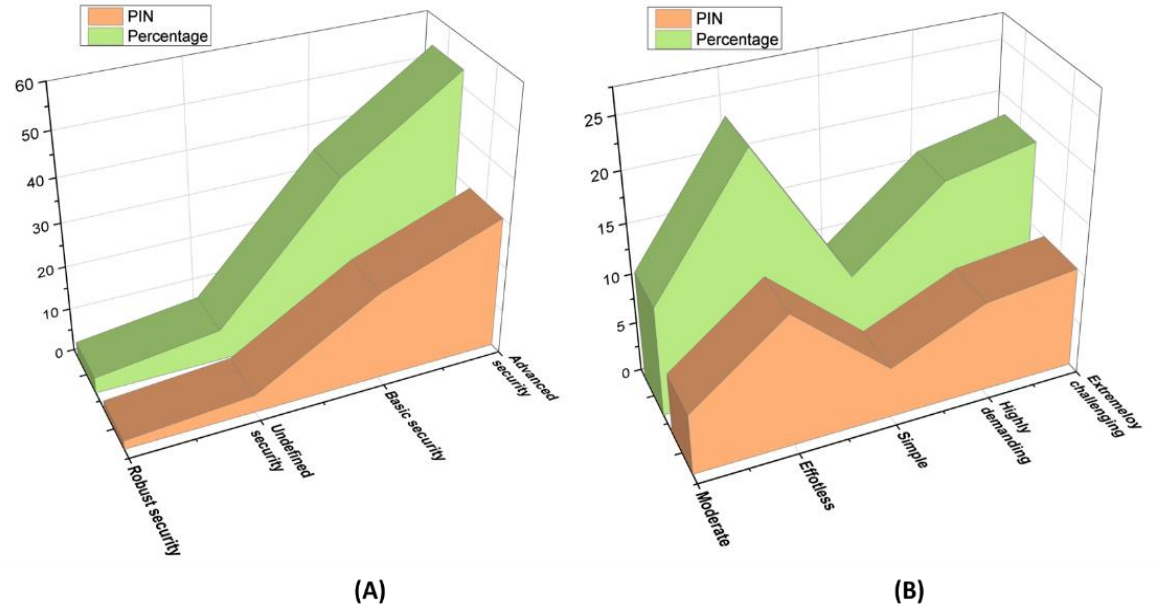

Figure 2: Security Analysis: A) Mobile Transfers & B) PIN/Percentage Features

Table 3: Growth Evaluations for Mobile Banking Users

Projected users	Existing users	Growth percentage	Projected user percentage	Predicted growth rate
115900	504000	88.12	608000	99.56

The efficiency of the recommended approach (V-AdaBoost) was evaluated using characteristics such as accuracy, precision, f1-score and compared to current methods. The study's measurements are conducted using ML methods “Random Forest (RF)”, “K-Nearest Neighbors (KNN)”, and “Support Vector Machine (SVM)” are examples of ML approaches (Kumar 2022).

Accuracy: The fraction of cases properly categorized out of all those assessed. It indicates the prediction model's overall accuracy in classifying secure transactions in the mobile banking system. Figure 3 illustrates the accuracy, showcasing our suggested strategy's 94.22% superiority over existing methods.

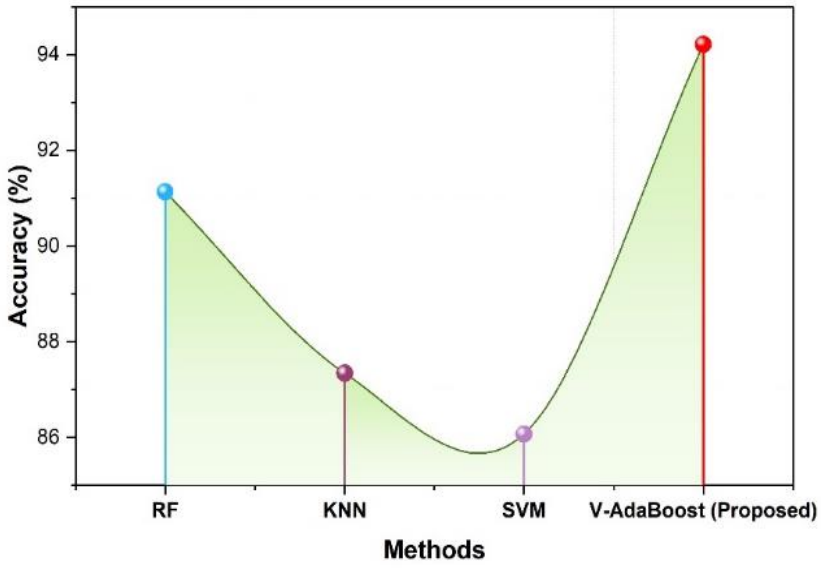

Figure 3: Accuracy

Precision: The ratio of predicted positive occurrences to total anticipated positive instances indicates the system's accuracy in making positive predictions about safe transactions in mobile banking. Figure 4 displays precision, demonstrating our proposed technique's 94% superiority over current methods.

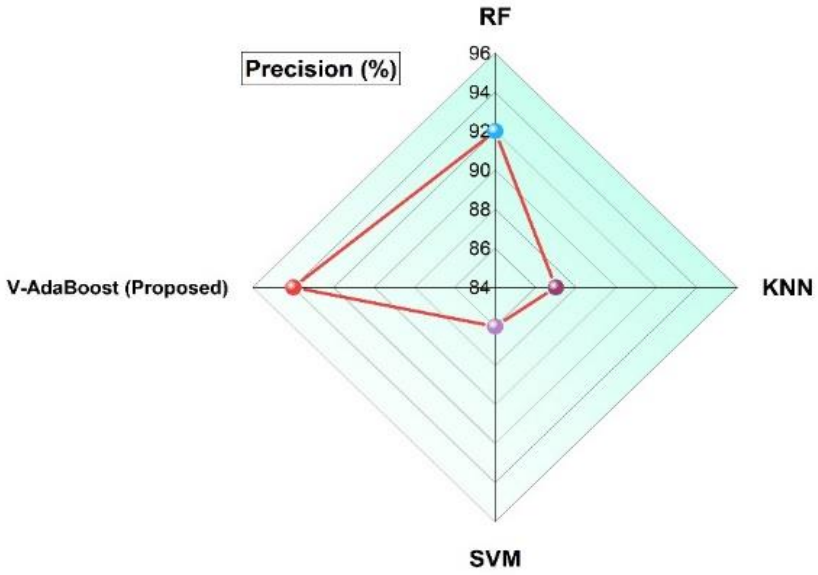

Figure 4: Precision

F1-score: A metric that strikes a balance between accuracy and memory. It represents the model's accuracy in detecting safe transactions while taking into both false positives and false negatives in the mobile banking system's security assessment. Figure 5 displays the f1-score, demonstrating our suggested strategy's 97% superiority over existing techniques.

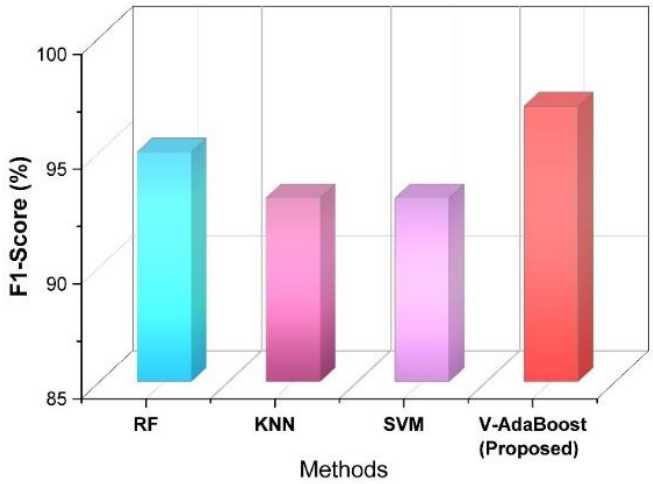

Figure 5: F1-Score

5 Conclusion

Mobile payments are seen as a significant development in India's financial sector. PIN secrecy is an important aspect of mobile payment security. During the implementation phase, significant challenges arise. Nowadays, individuals mostly use mobile phones for everyday services. It is simple to use and offers secure financial services. The system operates quickly, although there are certain issues with the present remedy. The present paper describes a mobile cloud framework for banking systems, allowing users to access mobile banking services anytime and anywhere through cloud-based servers using their mobile devices. The cloud computing risk model is used to assess risks associated with data storage on cloud servers. This paper presents findings from a descriptive study of a mobile phone financial service using the V-AdaBoost method. In modern times, people mostly use mobile phones to perform transactions. It is simple to use and offers protected payment services. This technique may gain popularity in industrialized countries. The system operates quickly, although there are currently issues with the mending process. In comparison with existing solutions, our proposed plan for safeguarding mobile banking transactions outperforms them, as far as of accuracy (94.22%), precision (94 %), and F1-score (97%). It will demonstrate the benefits of our method for strengthening the security of mobile banking systems. A limitation is the narrow focus on ML-based security, potentially overlooking broader techniques and real-world implementation beyond predictive effectiveness. Future research might explore further ML-based safety enhancements for mobile phone banking, aiming to improve user experience while ensuring comprehensive data protection.

References

[1] Al-Zubaidie, M., Zhang, Z., & Zhang, J. (2019). RAMHU: A new robust lightweight scheme for mutual users authentication in healthcare applications. *Security and Communication Networks*, *2019*(1), 3263902. https://doi.org/10.1155/2019/3263902.

[2] Bojjagani, S., Sastry, V. N., Chen, C. M., Kumari, S., & Khan, M. K. (2023). Systematic survey of mobile payments, protocols, and security infrastructure. *Journal of Ambient Intelligence and Humanized Computing*, *14*(1), 609-654. https://doi.org/10.1007/s12652-021-03316-4.

[3] Butt, U. A., Mehmood, M., Shah, S. B. H., Amin, R., Shaukat, M. W., Raza, S. M., ... & Piran, M. J. (2020). A review of machine learning algorithms for cloud computing security. *Electronics*, *9*(9), 1379. https://doi.org/10.3390/electronics9091379.

[4] Carbo-Valverde, S., Cuadros-Solas, P., & Rodríguez-Fernández, F. (2020). A machine learning approach to the digitalization of bank customers: Evidence from random and causal forests. *Plos one*, *15*(10), e0240362. https://doi.org/10.1371/journal.pone.0240362.

[5] Gayarathi, R., Hema, T., Iswarya, K., Kiruthika, E., & Boomidevi, R. (2018). Automatic Baby Cradle. *International Journal of Advances in Engineering and Emerging Technology, 9*(2), 19–23.

[6] Hinson, R., Lensink, R., & Mueller, A. (2019). Transforming agribusiness in developing countries: SDGs and the role of FinTech. *Current Opinion in Environmental Sustainability*, *41*, 1-9. https://doi.org/10.1016/j.cosust.2019.07.002

[7] Ho, J. C., Wu, C. G., Lee, C. S., & Pham, T. T. T. (2020). Factors affecting the behavioral intention to adopt mobile banking: An international comparison. *Technology in Society*, *63*, 101360. https://doi.org/10.1016/j.techsoc.2020.101360.

[8] Hrunyk, I. (2018). Computer technology applications and the data protection concept. *International Journal of Communication and Computer Technologies, 6*(1), 12-15.

[9] Hrytsyna, O., Yakubiv, V., Pavlikha, N., Shmatkovska, T., Tsymbaliuk, I., Marcus, O., & Brodska, I. (2019). Development of electronic banking: A case study of Ukraine. http://doi.org/10.9770/jesi.2019.7.1(17)

[10] Karjaluoto, H., Shaikh, A. A., Saarijärvi, H., & Saraniemi, S. (2019). How perceived value drives the use of mobile financial services apps. *International Journal of Information Management*, *47*, 252-261. https://doi.org/10.1016/j.ijinfomgt.2018.08.014.

[11] Kumar, V. (2022). Adoption of Mobile Payment Systems during COVID-19 in India. *Journal of Pharmaceutical Negative Results*, *13*. https://doi.org/10.47750/pnr.2022.13.S01.09

[12] Nawrocki, P., Sniezynski, B., & Slojewski, H. (2019). Adaptable mobile cloud computing environment with code transfer based on machine learning. *Pervasive and Mobile Computing*, *57*, 49-63. https://doi.org/10.1016/j.pmcj.2019.05.001.

[13] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019). Blockchain for secure ehrs sharing of mobile cloud based e-health systems. *IEEE access*, *7*, 66792-66806. https://doi.org/10.1109/ACCESS.2019.2917555

[14] Ojaghloo, M., & Jannesary, A. (2015). Investigate all attacks on Mobile Wireless Networks and Finding security solutions. *International Academic Journal of Innovative Research, 2*(2), 17–27.

[15] Pakurár, M., Haddad, H., Nagy, J., Popp, J., & Oláh, J. (2019). The service quality dimensions that affect customer satisfaction in the Jordanian banking sector. *Sustainability*, *11*(4), 1113. https://doi.org/10.3390/su11041113

[16] Prastya, I. Y., Putranti, I. R., Yuniningsih, T., & Priyadi, B. P. (2025). Sustainability of Co-Production in Waste Management: Exploring Waste Banks and TPS3R in Semarang City. *Acta Innovations*, 1-12. https://doi.org/10.62441/actainnovations.vi.400

[17] Sathyanarayana, N., & Laxmana Rao, G. (2024). Evaluating the Impact of NPA Dynamics in Selected Indian Banks: A Fifteen-Year Comparative Study. *Indian Journal of Information Sources and Services, 14*(3), 123–132. https://doi.org/10.51983/ijiss-2024.14.3.17

[18] Singh, S., & Srivastava, R. K. (2020). Understanding the intention to use mobile banking by existing online banking customers: an empirical study. *Journal of Financial Services Marketing*, *25*(3), 86-96. https://doi.org/10.1057/s41264-020-00074-w

[19] Sreevidya, B., & Supriya, D. M. (2024). Malicious nodes detection and avoidance using trust-based routing in critical data handling wireless sensor network applications. *Journal of Internet Services and Information Security, 14*(3), 226-244. https://doi.org/10.58346/JISIS.2024.I3.013.

[20] Tsai, C. H., & Su, P. C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. *Information systems and e-business management*, *19*(1), 77-105. https://doi.org/10.1007/s10257-020-00481-5
[21] Tseng, M. L., Bui, T. D., Lan, S., Lim, M. K., & Mashud, A. H. M. (2021). Smart product service system hierarchical model in banking industry under uncertainties. *International Journal of Production Economics*, *240*, 108244. https://doi.org/10.1016/j.ijpe.2021.108244
[22] Wang, F., Yang, N., Shakeel, P. M., & Saravanan, V. (2024). Machine learning for mobile network payment security evaluation system. *Transactions on Emerging Telecommunications Technologies*, *35*(4), e4226. https://doi.org/10.1002/ett.4226
[23] Weippl, E.R., Tjoa, A.M., & Pernul, G. (2011). Guest Editorial: Advances in Applied Security. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2*(4), 1-3.
[24] Zendehboudi, M., Azimpour, J., & Gorginpour, H. (2014). Offering a Method for Ensuring Data Storage Security in the Cloud Network by Using Kerberos Algorithm. *International Academic Journal of Science and Engineering, 1*(2), 75–81.

Authors Biography

Dr. Meenal R. Kale is an Assistant Professor in the Department of Humanities at Yeshwantrao Chavan College of Engineering (YCCE), India. Her research interests include interdisciplinary studies in humanities, language and communication, cultural studies, and educational methodologies. Actively engaged in teaching, mentoring, and research, Dr. Kale has contributed to reputed journals, conferences, and various academic projects aimed at enhancing educational practices. Dedicated to academic excellence and innovative research, she continues to make valuable contributions to her field.

Dr. Itikela Shyam Sundar is an Associate Professor in the Department of Accounting and Finance at the College of Business and Economics, Assosa University, Ethiopia. His research interests include financial management, corporate finance, accounting principles, investment analysis, and economic policy. Actively engaged in teaching, mentoring, and research, Dr. Sundar has published papers in reputed journals, presented at national and international conferences, and contributed to various academic and industry-oriented projects. Committed to academic excellence and financial research, he continues to make significant contributions to his field.

Dr. Bhuvana Jayabalan is an Associate Professor in the Department of Computer Science and Information Technology at Jain (Deemed-to-Be University), Bangalore, Karnataka, India. Her research interests include artificial intelligence, machine learning, data analytics, cybersecurity, and cloud computing. Actively involved in teaching, mentoring, and conducting innovative research, Dr. Jayabalan has published research papers in reputed journals, presented at national and international conferences, and contributed to various academic projects. Committed to academic excellence and technological advancements, she continues to make significant contributions to her field.

Dr. Bineet Desai is a Professor in the Department of ISME at ATLAS Skilltech University, Mumbai, Maharashtra, India. His research interests include business management, entrepreneurship, innovation, leadership, and strategic management. Actively involved in teaching, research, and mentoring, Dr. Desai has published research papers in reputed journals, presented at national and international conferences, and contributed to various industry-oriented projects. With a commitment to academic excellence and promoting innovative practices in management education, he continues to make impactful contributions to his field.

Dr. Akash Kumar Bhagat is an Assistant Professor in the Department of Computer Science & IT at ARKA JAIN University, Jamshedpur, Jharkhand, India. His research interests include artificial intelligence, machine learning, data science, cybersecurity, and cloud computing. Actively involved in teaching, mentoring, and research, Dr. Bhagat has published papers in reputed journals, presented at national and international conferences, and contributed to various academic and industry-oriented projects. Dedicated to academic excellence and technological advancements, he continues to make valuable contributions to his field.

Dr. Sachin S. Pund is an Assistant Professor in the Department of Mechanical Engineering at Ramdeobaba University (RBU), Nagpur, Maharashtra, India. His research interests include thermal engineering, fluid mechanics, advanced manufacturing processes, and automation systems. Actively involved in teaching, mentoring, and research, Dr. Pund has published research papers in reputed journals, presented at national and international conferences, and contributed to various engineering projects. Committed to academic excellence and innovation in mechanical engineering, he continues to make valuable contributions to his field.