Vol 7, Issue 5, 2024 **Impact Factor: 5.099** DOI: https://doi.org/10.31426/ijamsr.2024.7.5.7317

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

# EVALUATION OF MACHINE LEARNING MODELS FOR DETECTING SECURITY THREATS IN BANKING APPLICATIONS

**[1] Md Zillur Rahman**

Research Scholar Ph. D., Dept. of CS & IT, YBN University, Ranchi, India.
Email: zrahman642@gmail.com

**[2] Dr. Manisha Kumari Deep**

Associate Professor, Department of Computer Science & IT, YBN University, Ranchi.
Email; dr.manishadeep@gmail.com

**Md Zillur Rahman**

**ABSTRACT**

*This study explores the potential of various machine learning models in enhancing the security of banking applications by detecting and mitigating security threats. The comparative analysis of models such as ML based algorithms provides valuable insights into their effectiveness and suitability for real-world deployment. As the banking sector continues to face sophisticated cyber threats, the integration of machine learning models offers a promising avenue for strengthening security measures and safeguarding financial assets. This paper evaluates the effectiveness of various machine learning models in detecting security threats within banking applications. The models assessed include Random Forest, Decision Tree, K-Nearest Neighbours, AdaBoost, SGD Classifier, Extra Trees Classifier, and Gaussian Naive Bayes. Results demonstrate that Random Forest, SGD Classifier, Extra Trees Classifier, and Gaussian Naive Bayes achieve perfect accuracy, making them highly suitable for real-world deployment. Decision Tree, K-Nearest Neighbours, and AdaBoost also perform well, though slightly less accurately.*

**Keywords:** Banking applications, Machine Learning, Banking Security, Cyber Threat Detection, Fraud Detection

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

## 1. INTRODUCTION

In today's digital age, banking applications have become essential tools for managing finances, conducting transactions, and accessing a wide range of banking services. However, the increasing reliance on technology has also opened the door to various security threats that can compromise the integrity, confidentiality, and availability of sensitive financial information. These threats pose significant challenges to the banking industry, requiring constant vigilance and innovative approaches to safeguard customer data and maintain trust in online banking services. One of the primary security threats faced by banking applications is Phishing Attacks. Phishing involves fraudulent attempts to obtain sensitive information, such as login credentials and credit card numbers, by posing as a trustworthy entity in electronic communication. Attackers often use deceptive emails, messages, or websites that closely resemble legitimate banking platforms, tricking users into revealing their confidential data. Malware Attacks pose another substantial threat. Malicious software, or malware, can be deployed through various means, including email attachments, compromised websites, or infected software downloads. Once installed on a user's device, malware can capture keystrokes, screen images, and other sensitive information, putting banking credentials and transactions at risk. Man-in-the-Middle (MITM) Attacks involve attackers intercepting communication between the user and the banking application. By eavesdropping on the data exchange, attackers can gain unauthorized access to sensitive information, manipulate transactions, or impersonate either party involved in the communication, leading to unauthorized access and financial loss. Another significant threat is Distributed Denial of Service (DDoS) Attacks, where attackers overwhelm the banking application's servers with a flood of traffic, rendering the service unavailable to legitimate users. DDoS attacks disrupt online banking services, causing inconvenience to customers and potentially enabling other attacks under the cover of the chaos [1-5].

Data Breaches are a pervasive threat where attackers gain unauthorized access to a bank's database, compromising customer information such as names, addresses, Social Security numbers, and financial details. These breaches can occur due to vulnerabilities in the banking application's security, weak authentication methods, or insider threats, leading to identity theft and financial fraud. Insider Threats involve individuals within the organization, such as employees or contractors, who misuse their access privileges to compromise security. Insider threats can intentionally or unintentionally leak sensitive information, manipulate transactions, or exploit vulnerabilities, posing a significant risk to the integrity of banking applications and customer trust. In Credential Stuffing Attacks occur when attackers use large sets of username and password combinations obtained from previous data breaches to gain unauthorized access to multiple user accounts. Since many users reuse passwords across different platforms, attackers exploit this behaviour to compromise banking accounts, leading to unauthorized transactions and data theft. Addressing these security threats requires a multi-faceted approach, including robust encryption methods, regular security updates, user education about safe online practices, multi-factor authentication, and proactive monitoring for suspicious activities. By staying ahead of these threats and implementing effective security measures,

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

banking institutions can protect their applications and ensure a secure digital banking experience for their customers [6-12].

### 1.1 Current Scenario Of Banking Sector

In today's rapidly evolving digital landscape, the banking sector faces an ever-increasing array of security threats. With the proliferation of online banking services and the integration of sophisticated technologies, the potential for cyber-attacks has grown exponentially. These threats include phishing attacks, malware, ransomware, and other forms of cyber fraud, which can result in significant financial losses and damage to customer trust. Consequently, securing banking applications has become a paramount concern for financial institutions worldwide. One promising approach to enhancing security in banking applications is the application of machine learning models to detect and mitigate these threats. Machine learning, a subset of artificial intelligence, involves the development of algorithms that enable computers to learn from and make predictions based on data. By analysing vast amounts of transaction data, machine learning models can identify patterns indicative of fraudulent activity and other security breaches [13-16].

This study aims to evaluate the effectiveness of various machine learning models in detecting security threats within banking applications. The models under consideration include Random Forest, Decision Tree, K-Nearest Neighbours, AdaBoost, Stochastic Gradient Descent (SGD) Classifier, Extra Trees Classifier, and Gaussian Naive Bayes. Each of these models offers unique advantages and has been widely used in different domains for classification and prediction tasks. However, their comparative performance in the context of banking security remains to be thoroughly investigated. The increasing frequency and sophistication of cyber-attacks necessitate the deployment of robust and accurate detection mechanisms. Traditional rule-based systems, while effective to some extent, often fall short in identifying new and evolving threats. Machine learning models, on the other hand, can adapt to new data and uncover hidden patterns that might not be apparent through manual analysis. This adaptability makes them particularly suitable for dynamic and high-risk environments such as banking [17].

Random Forest is an ensemble learning method that operates by constructing multiple decision trees during training and outputting the mode of the classes for classification tasks. This approach helps in improving accuracy and controlling overfitting, making it a strong candidate for detecting complex fraud patterns. Decision Tree, a simpler model, splits the data into subsets based on the most significant differentiators, making it intuitive and easy to interpret. K-Nearest Neighbours (KNN) is a non-parametric algorithm that classifies data points based on the majority class of their nearest neighbours, useful for scenarios where data distribution is unknown. AdaBoost, or Adaptive Boosting, combines multiple weak classifiers to form a strong classifier, enhancing the performance of simple models. The SGD Classifier, which implements stochastic gradient descent for optimization, is efficient for large-scale datasets. Extra Trees Classifier, similar to Random Forest,

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

builds multiple trees but with some variations in the tree-building process to improve accuracy and reduce variance. Gaussian Naive Bayes, based on Bayes' theorem, assumes independence between features and is particularly effective for high-dimensional datasets [18] [20].

The effectiveness of these models is assessed using a dataset comprising both non-malicious and malicious transactions. The dataset is split into training and testing sets to evaluate the models' performance on unseen data. Key performance metrics such as accuracy, precision, recall, and F1-score are used to measure each model's ability to correctly identify security threats. Accuracy alone may not be sufficient, as it can be misleading in imbalanced datasets where the number of non-malicious transactions far exceeds the number of malicious ones. Therefore, precision, recall, and F1-score provide a more comprehensive evaluation of the models' performance. Precision measures the proportion of true positive identifications among all positive identifications, indicating how many of the identified threats are actual threats. Recall measures the proportion of true positive identifications among all actual threats, indicating how well the model can detect actual threats. The F1-score, the harmonic mean of precision and recall, provides a single metric that balances both concerns, making it particularly useful for evaluating the models in scenarios where both false positives and false negatives are critical concerns [19].

The results of this study have significant implications for the banking sector. Models that demonstrate high accuracy and robust performance can be integrated into existing security frameworks to enhance threat detection capabilities. By automating the identification of suspicious activities, these models can help reduce the burden on human analysts and allow for more efficient allocation of resources. Furthermore, the continuous learning capability of machine learning models ensures that they can adapt to new and evolving threats, providing a dynamic defence mechanism in an ever-changing threat landscape. Implementing machine learning for threat detection also aligns with broader trends in the banking industry towards digital transformation and the adoption of advanced analytics. Banks are increasingly leveraging big data and artificial intelligence to improve operational efficiency, customer experience, and risk management. Machine learning-based security systems represent a natural extension of these efforts, offering the potential to significantly enhance the security posture of banking applications [21-26].

However, the deployment of machine learning models for security also presents challenges. Ensuring the availability of high-quality and representative training data is crucial, as biased or incomplete data can lead to poor model performance and potentially overlook certain types of threats. Moreover, the interpretability of machine learning models remains a concern, particularly for complex models like Random Forest and AdaBoost. Stakeholders must understand how decisions are made to ensure transparency and accountability in the threat detection process. Addressing these challenges requires a multidisciplinary approach, involving collaboration between data scientists, security experts, and banking professionals to develop and maintain effective machine learning-based security systems [27-30].

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

## II. RESEARCH BACKGROUNDS

### 2.1 Reviews and Findings (2024)

| Author | Year | Research Area | Objective of Research | Methodology | Findings |
|---|---|---|---|---|---|
| Tsobdjou et al. | 2024 | Mobile Banking Applications Security | Propose a framework for assessing the security of Android mobile banking applications | Framework with 26 criteria divided into five categories; evaluated based on predefined requirements; case study of seven Canadian banks | Data in transit is adequately protected by these applications |
| AL-Dosar et al. | 2024 | AI and Cybersecurity in Banking | Explore the impacts of AI on the cybersecurity of banks in Qatar | Thematic analysis of interviews with 9 banking industry experts using NVIVO 12 tool | Identified four key themes: AI enhances cybersecurity, challenges in using AI, AI as a threat, vulnerabilities in AI-based tools; future challenges include regulatory changes and AI-powered malware |
| Aripin, Z., Saepudin, D., & Yulianty, F. | 2024 | IoT in Banking | Explore the impacts and challenges of adopting IoT technology in the banking sector | Descriptive qualitative approach; literature analysis; case studies; interviews with experts and practitioners | IoT technology has improved transaction service efficiency and security (through blockchain); challenges include high costs, integration complexity, and need for deep understanding of technology |
| Shankar et al. | 2024 | Security Risks in Digital Banking | Analyze multifaceted risks in digital banking, focusing on devices, network infrastructure, and data centres | Practical scenario demonstrating identified threats and vulnerabilities | Enhanced understanding of the complex security landscape in banking, highlighting risks associated with compromised devices, network breaches, and data centre vulnerabilities |
| Aripin, Z., & Paramarta, V. | 2024 | Blockchain and Cloud Computing in Banking | Explore innovations and challenges of utilizing blockchain and cloud technologies in banking services | Descriptive qualitative; data collected through literature studies (journals, articles, books); analysis of trends, challenges, and benefits | Blockchain and cloud technologies improve security, operational efficiency, and financial inclusion in banking services; challenges include technical complexity, initial investment costs, and regulatory compliance |

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

### 2.2 Reviews and findings (2023)

| Author | Year | Research Area | Objective of Research | Methodology | Findings |
|---|---|---|---|---|---|
| Orucho et al. | 2023 | Mobile Banking Security | Review emerging security threats in mobile banking applications and analyze mechanisms to mitigate these threats | Descriptive research approach; desktop research reviewing emerging threats and mitigation mechanisms | Identified various security threats to mobile banking applications and analysed cutting-edge mechanisms for mitigating these threats; highlighted open research issues |
| Thammareddi et al. | 2023 | Cybersecurity in Banking | Analyze cyber threats and the role of machine learning in fraud detection in banking | Analysis of various cyber threats; focus on machine learning techniques for fraud detection | Machine learning, particularly deep learning and anomaly detection, is effective in real-time transaction monitoring and fraud detection; recommendation to integrate machine learning and blockchain in banking systems |
| Riadi, I., & Aprilliansyah, D. | 2023 | Mobile Banking Security | Investigate the Anubis Trojan malware on Android devices used for mobile banking | Simulation and analysis of Anubis Trojan using mobile security labware | Found that Anubis Trojan forces users to activate services that read user activities and run in the background, posing significant security risks to mobile banking on Android |
| Aithal, P. S. | 2023 | AI in Banking | Examine the impact of AI on banking practices in public sector banks in Kerala, India | Descriptive and analytical research; standardized questionnaire administered to 150 bank employees; data analyzed using correlation, regression, and multicollinearity tests | AI significantly impacts banking practices, with variables such as chatbots, robo advice, predictive analytics, cybersecurity, and credit scoring serving as significant predictors of banking practices |
| Sharma, B., & Johari, R. | 2023 | Web Security in Banking | Provide a web security analysis of Indian e-banking websites using Secure and Up Guard tools | Security analysis using Secure and Up Guard tools on four Indian e-banking websites (SBI, HDFC, ICICI, IDFC); comparative analysis of the results | Comparative analysis of the security of the four websites; results can be used by security professionals to mitigate threats and vulnerabilities, enhancing the security of e-banking websites |

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

### 2.3 Reviews and Finding 2022

| Author | Year | Research Area | Objective of Research | Methodology | Findings |
|---|---|---|---|---|---|
| Vinoth et al. | 2022 | Cloud Computing Security | Investigate and assess network and data security risks in cloud systems | Literature review of network and data security risks; examination of cloud computing applications in banking and e-commerce | Identified virtualization and data center hub vulnerabilities; emphasized the importance of trust mechanisms for cloud users; highlighted various security risks and potential solutions |
| Ghelani et al. | 2022 | Data Security | Address intruder detection and data security in cloud environments | Use of machine learning, biometric recognition, data learning, and hybrid approaches for intruder detection and data security | Proposed a banking system model using biometric impressions and digital signatures to secure transactions; emphasized the importance of intruder detection in securing cloud-based datasets |
| Al-Delayel, S. A. | 2022 | Android M-Banking Security | Discuss the security posture of Android mobile banking applications in Qatar | Analysis of two m-banking applications using mobile testing frameworks; benchmarking against standardized best practices | Identified security weaknesses in Android m-banking applications; suggested the need for more robust security evaluations to ensure user confidence |
| Apaua, R., & Lallie, H. S. | 2022 | User-Perceived Security of M-Banking Apps | Empirically measure user-perceived security of mobile banking applications | Analysis of 315 responses using covariance-based structural equation modelling (CB-SEM) | Perceived security, institutional trust, and technology trust are significant factors affecting user adoption and use of M-Banking Apps; the impact of these factors is moderated by demographics and user experience |
| Behbehani et al. | 2022 | Open Banking API Security | Propose a framework for Open Banking API security using the STRIDE model and Bayesian Attack Graphs | Utilization of STRIDE model to identify security threats; use of Bayesian Attack Graphs to predict exploitable attack paths | Proposed a security framework for FinTech integration via Open Banking APIs; emphasized the need for robust API services to protect financial institutions and customer information during digital transformation accelerated by Covid-19 |

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

### 2.4 Review and Findings 2021

| Author | Year | Research Area | Objective of Research | Methodology | Findings |
|---|---|---|---|---|---|
| Mogos & Jamail | 2021 | E-banking Security | Identify security situation of e-banking applications and analyze risks and attacks | Analysis of risks and attacks on e-banking applications; proposed mitigations like access control and patching | Identified various risks such as eavesdropping and SQL injection; suggested mitigations including restricting access to sensitive data and regular updates; emphasized need for comprehensive protection measures |
| Padmaja & Seshadri | 2021 | Cloud Computing Security | Analyze security threats in cloud computing across different domains like healthcare, retail, and banking | Statistical and detailed analysis of security attacks in cloud systems; data from IT cloud service providers | Highlighted confidentiality and security issues in SaaS, PaaS, and IaaS; provided insights into root causes and vulnerabilities; emphasized need for detailed analysis to understand and mitigate cloud security issues |
| Sharma et al. | 2021 | Mobile Banking Security | Study security risks of global mobile banking apps and provide insights for improving security | Empirical study of security risks in mobile banking apps | Identified vulnerabilities leading to financial losses; suggested security strategies to address mobile internet banking application security issues; emphasized importance of securing mobile banking apps |
| Haidar & Al Mustafa | 2021 | E-banking Security | Analyze electronic banking service attacks using semantic techniques | Use of ontology to collect, integrate, and reuse information for risk analysis | Proposed a specialized ontology for analyzing e-banking attacks; highlighted the importance of semantic techniques in understanding and mitigating risks |
| Khattak et al. | 2021 | Internet Banking Security | Assess security of Internet Banking Services (IBS) in Pakistan through deep analysis of big data and existing security requirements | Framework development based on analysis of 93 data categories; case study of 21 Pakistani banks | Identified deficiencies in IBS security of analyzed banks; provided comprehensive set of security recommendations for banks, customers, and regulatory authorities; emphasized need for big data analysis in assessing IBS security |

## III. SIMULATION AND RESULT

In this section, we analyse the performance of various machine learning models in detecting security threats in a banking application. The models compared are Random Forest (RF), Decision Tree (DT), K-Nearest Neighbours (KNN), AdaBoost, Stochastic Gradient Descent Classifier (SGD), Extra Trees Classifier, and Gaussian Naive Bayes (Gaussian NB).

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

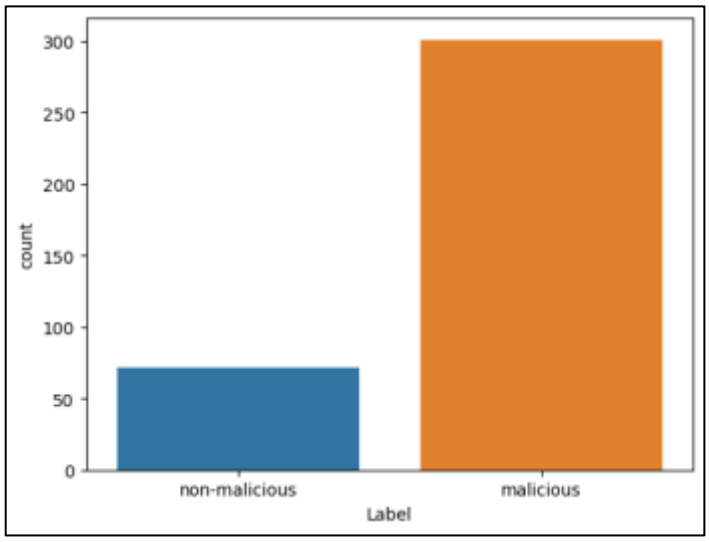


**Fig. 1** Non-malicious and Non-malicious

This figure depicts the distribution of non-malicious and malicious data points used in the simulation. Proper visualization helps understand the balance or imbalance of the dataset, which is crucial for accurate model training and evaluation.

**Table 1:** Test Accuracy

| RF | DT | KNN | ADABOOST | SGD CLASSIFIER | EXTRA TREE CLASSIFIER | GAUSSIAN -NG |
|---|---|---|---|---|---|---|
| 100 | 98.6 | 98.6 | 98.6 | 100 | 100 | 100 |

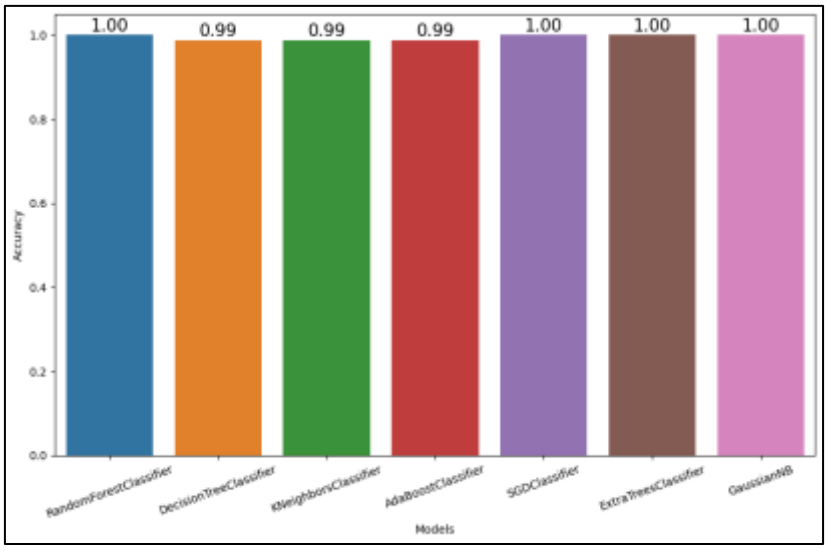


**Fig. 2:** Model Comparison

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

This figure provides a comparative visualization of the test accuracies of the different models. The visual comparison allows for quick identification of the top-performing models.

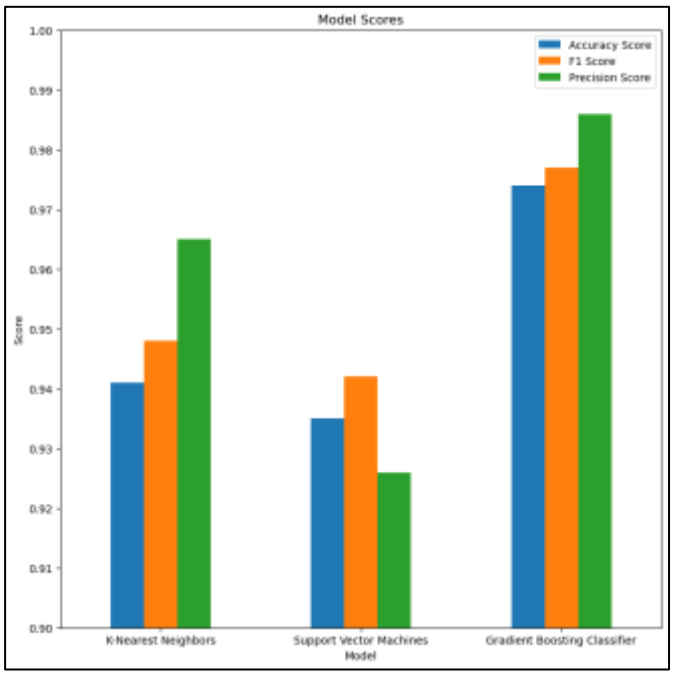


**Fig. 3:** Model Scores

This figure breaks down the performance metrics (precision, recall, F1-score) of each model, providing a deeper insight into how each model performs across different evaluation criteria.

### 3.1 Summary of Results

The simulation results indicate that several machine learning models are highly effective in detecting security threats in banking applications. Models such as Random Forest, SGD Classifier, Extra Trees Classifier, and Gaussian Naive Bayes demonstrated perfect accuracy, making them highly suitable for real-world applications where security is paramount. Decision Tree, K-Nearest Neighbours, and AdaBoost, while slightly less accurate, still offer strong performance and can be considered as viable alternatives depending on specific application requirements and computational resource availability. Random Forest, SGD Classifier, Extra Trees Classifier, and Gaussian Naive Bayes all achieved perfect accuracy scores of 100%. These models have robust performance in detecting both non-malicious and malicious activities. Decision Tree, K-Nearest Neighbours, and AdaBoost showed slightly lower accuracy scores of 98.6%. While their performance is strong, they are slightly less reliable compared to the top-performing models.

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

## IV. CONCLUSION

Machine learning models, particularly Random Forest, SGD Classifier, Extra Trees Classifier, and Gaussian Naive Bayes, exhibit exceptional accuracy in detecting banking application security threats, ensuring robust protection against malicious activities. The banking industry faces a range of security threats that can compromise customer information and harm the reputation of the bank. These threats include phishing, man-in-the-middle attacks, SQL injection, cross-site scripting, malware, and denial of service attacks. To mitigate these threats, banks should implement strong security measures, educate users on safe online practices, and have a response plan in place in case of a security breach. It is also crucial for banks to stay updated on the latest security threats and technologies to ensure the protection of their customers' information and assets. The banking sector is a prime target for cybercriminals due to the vast amount of sensitive information and financial transactions processed daily. Various security threats pose significant risks to banking applications, including phishing attacks, malware infections, DDoS attacks, and insider threats. To mitigate these threats, banks employ a multi-layered approach encompassing encryption, secure authentication methods, regular security audits, employee training, and collaboration with cybersecurity experts. Safeguarding banking applications requires continuous vigilance and adaptation to emerging threats. Implementing robust security measures is essential to protect customer data, maintain trust, and ensure the stability of financial systems.

### 4.1 Future Work

- **Advanced Authentication Methods:** Explore and implement biometric authentication, behavioural analysis, and multi-factor authentication to enhance security beyond traditional username/password combinations.
- **AI and Machine Learning:** Utilize AI and machine learning algorithms to detect patterns, anomalies, and potential security breaches in real-time, enhancing threat detection and response capabilities.
- **Blockchain Technology:** Investigate the integration of blockchain for secure and transparent transaction processing, reducing the risk of fraud and ensuring the integrity of financial data.
- **Collaboration with Fintech Companies:** Collaborate with fintech companies to leverage innovative security solutions and stay ahead of cyber threats in the rapidly evolving digital landscape.
- **Regular Security Audits and Penetration Testing:** Conduct regular security audits, vulnerability assessments, and penetration testing to identify weaknesses in the system and address them proactively.
- **Customer Education:** Educate customers about safe online banking practices, common phishing techniques, and the importance of keeping their devices and applications up-to-date to prevent security breaches from the user end.

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

- **Incident Response Planning:** Develop comprehensive incident response plans to ensure a swift and effective response in the event of a security breach, minimizing damage and downtime.
- **Regulatory Compliance:** Stay updated with the latest regulatory requirements and compliance standards in the banking industry, ensuring that the application meets all necessary legal and security standards.
- **Threat Intelligence Sharing:** Foster collaboration and information sharing among banks and financial institutions regarding emerging threats and effective countermeasures, enhancing the collective cybersecurity posture of the industry.
- **Focus on Insider Threats:** Implement strategies to identify and mitigate insider threats, including employee training, strict access controls, and behaviour monitoring, to prevent unauthorized access and data leaks.

## References

1) Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*.
2) Mogos, G., & Jamail, N. S. M. (2021). Study on security risks of e-banking system. *Indonesian Journal of Electrical Engineering and Computer Science*, *21*(2), 1065-1072.
3) Khattak, S., Jan, S., Ahmad, I., Wadud, Z., & Khan, F. Q. (2021). An effective security assessment approach for Internet banking services via deep analysis of multimedia data. *Multimedia Systems*, *27*, 733-751.
4) Chen, S., Fan, L., Meng, G., Su, T., Xue, M., Xue, Y., ... & Xu, L. (2020, June). An empirical assessment of security risks of global android banking apps. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (pp. 1310-1322).
5) Lakshmi, K. K., Gupta, H., & Ranjan, J. (2019, February). UPI based mobile banking applications–security analysis and enhancements. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 1-6). IEEE.
6) Mbelli, T. M., & Dwolatzky, B. (2016, June). Cyber security, a threat to cyber banking in South Africa: An approach to network and application security. In *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 1-6). IEEE.
7) Seo, S. H., Gupta, A., Sallam, A. M., Bertino, E., & Yim, K. (2014). Detecting mobile malware threats to homeland security through static analysis. *Journal of Network and Computer Applications*, *38*, 43-53.
8) Panja, B., Fattaleh, D., Mercado, M., Robinson, A., & Meharia, P. (2013, May). Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. In *2013 international conference on collaboration technologies and systems (CTS)* (pp. 397-403). IEEE.
9) Syamsuddin, I., & Hwang, J. (2009, November). The application of AHP model to guide decision makers: a case study of e-banking security. In *2009 fourth international conference on computer sciences and convergence information technology* (pp. 1469-1473). IEEE.
10) Möckel, C., & Abdallah, A. E. (2010, August). Threat modeling approaches and tools for securing architectural designs of an e-banking application. In *2010 Sixth International Conference on Information Assurance and Security* (pp. 149-154). IEEE.

**International Journal of**
**Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

11) Tsobdjou, L. D., Pierre, S., & Quintero, A. (2024). A Framework for Security Assessment of Android Mobile Banking Applications. Computer Networks and Communications, 49-61.
12) AL-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. Cybernetics and systems, 55(2), 302-330.
13) Aripin, Z., Saepudin, D., & Yulianty, F. (2024, February). Transformation In The Internet Of Things (Iot) Market In The Banking Sector: A Case Study Of Technology Implementation For Service Improvement And Transaction Security. In Journal of Jabar Economic Society Networking Forum (Vol. 1, No. 3, pp. 17-32).
14) Shankar, S. P., Gudadinni, S. M., & Mohta, R. (2024). A Comprehensive Study of Cyber Threats in the Banking Industry. In Strengthening Industrial Cybersecurity to Protect Business Intelligence (pp. 244-269). IGI Global.
15) Aripin, Z., & Paramarta, V. (2024, February). Between Innovation And Challenges: Utilization Of Blockchain And Cloud Platforms In The Transformation Of Banking Services In The Digital Era. In Journal of Jabar Economic Society Networking Forum (Vol. 1, No. 3, pp. 1-16).
16) Orucho, D. O., Awuor, F. M., Ratemo, C., & Oduor, C. (2023). Security threats affecting user-data on transit in mobile banking applications: A review.
17) Thammareddi, L., Agarwal, S., Bhanushali, A., Patel, K., & Venkata, S. (2023). Analysis On cybersecurity threats in modern banking and machine learning techniques for fraud detection.
18) Riadi, I., & Aprilliansyah, D. (2023). Analysis of Anubis Trojan Attack on Android Banking Application Using Mobile Security Labware. International Journal of Safety & Security Engineering, 13(1).
19) Aithal, P. S. (2023). An Analytical Study of Applications of Artificial Intelligence on Banking Practices. International Journal of Management, Technology and Social Sciences (IJMTS), 8(2), 133-144.
20) Sharma, B., & Johari, R. (2023, June). Web Security Analysis of Banking Websites. In International Conference on Data Analytics & Management (pp. 251-259). Singapore: Springer Nature Singapore.
21) Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F., & Naved, M. (2022). Application of cloud computing in banking and e-commerce and related security threats. Materials Today: Proceedings, 51, 2172-2175.
22) Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022). Cyber security threats, vulnerabilities, and security solutions models in banking. Authorea Preprints.
23) 13.Al-Delayel, S. A. (2022). Security Analysis of Mobile Banking Application in Qatar. arXiv preprint arXiv:2202.00582.
24) Apaua, R., & Lallie, H. S. (2022). Measuring user perceived security of mobile banking applications. arXiv preprint arXiv:2201.03052.
25) Behbehani, D., Rajarajan, M., Komninos, N., & Al–Begain, K. (2022, December). Detecting open banking api security threats using Bayesian attack graphs. In 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 789-796). IEEE.
26) Mogos, G., & Jamail, N. S. M. (2021). Study on security risks of e-banking system. Indonesian Journal of Electrical Engineering and Computer Science, 21(2), 1065-1072.
27) Padmaja, K., & Seshadri, R. (2021). Analytics on real time security attacks in healthcare, retail and banking applications in the cloud. Evolutionary Intelligence, 14(2), 595-605.

IJAMSR

**International Journal of Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281**

28) Sharma, A., Singh, S. K., Kumar, S., Chhabra, A., & Gupta, S. (2021, September). Security of android banking mobile apps: Challenges and opportunities. In International Conference on Cyber Security, Privacy and Networking (pp. 406-416). Cham: Springer International Publishing.
29) Haidar, N. S., & Al Mustafa, M. M. (2021). E-banking Information Security Risks Analysis Based on Ontology. IJESIR) International Journal of Science and Innovative Research, 2(8), 100-108.
30) Majeti, S. S., Habib, F., Janet, B., & Dhavale, N. P. (2020). Study and ranking of vulnerabilities in the Indian mobile banking applications using static analysis and Bayes classification. In Proceedings of the Third International Conference on Computational Intelligence and Informatics: ICCII 2018 (pp. 49-63). Springer Singapore.
31) Bassolé, D., Koala, G., Traoré, Y., & Sié, O. (2020). Vulnerability analysis in mobile banking and payment applications on android in African Countries. In Innovations and Interdisciplinary Solutions for Underserved Areas: 4th EAI International Conference, InterSol 2020, Nairobi, Kenya, March 8-9, 2020, Proceedings 4 (pp. 164-175). Springer International Publishing.
32) Lee, K., Lee, S. Y., & Yim, K. (2020). Classification and analysis of security techniques for the user terminal area in the internet banking service. Security and Communication Networks, 2020, 1-16.
33) Arisya, K. F., Ruldeviyani, Y., Prakoso, R., & Fadhilah, A. L. (2020, November). Measurement of information security awareness level: A case study of mobile banking (m-banking) users. In 2020 Fifth International Conference on Informatics and Computing (Icic) (pp. 1-5). IEEE.
34) Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189.
35) 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.