Intelligent Cybersecurity Framework for banking phishing and fraud detection

Mrs.Usha M G,Athmik R Ameen, Samrudhi H.M, Bhoomika K.M, Pallavi.C
Assistant Professor Dept of CSBS Malnad College of Engineering Hassan, India
[1,2,3,4] Dept of CSBS Malnad College of Engineering Hassan, India

Abstract: **The rapid adoption of online banking and digital payment services has transformed the financial sector by providing faster and more convenient transactions. However this growth has also increased exposure by cybersecurity threats such as phishing attacks, fraudulent transactions unauthorized account access.**

This study presents an Intelligent Cybersecurity Framework for Banking Phishing and Fraud Detection that combines Artificial Intelligence and Machine Learning techniques to strengthen banking security.

The framework evaluates multiple parameters, including URL characteristics, transaction information, login locations, user behaviour, and account activity, to identify suspicious actions. Machine learning models such as Random Forest, Decision Tree, Logistic Regression, and deep learning approaches are incorporated to enhance detection performance.

The framework also supports real-time monitoring and alert generation, enabling timely responses to potential threats. Publicly available phishing and banking fraud datasets are utilized for model training and evaluation. The proposed approach aims to improve detection accuracy, reduce financial risks, and support secure digital banking operations.

I.INTRODUCTION

Digital banking services have become an essential part of modern financial systems, allowing customers to perform transactions, pay bills, transfer funds, and access banking facilities from any location. While these services improve convenience and accessibility, they also create new opportunities for cybercriminals to exploit vulnerabilities within online platforms.

Among various cybersecurity threats, phishing remains one of the most significant challenges faced by financial institutions. Attackers frequently design fraudulent websites, emails, and messages that imitate legitimate banking communications to deceive users into revealing confidential information. Such incidents often result in unauthorized account access, financial loss, and compromise of sensitive customer data.

Traditional security mechanisms primarily rely on rule-based monitoring and predefined attack signatures. Although these methods can identify known threats, they are less effective against newly emerging attack strategies. The growing volume of online transactions further complicates manual monitoring, making it difficult for security teams to detect suspicious activities promptly.

Recent advancements in Artificial Intelligence and Machine Learning have provided new opportunities for improving cybersecurity systems. These technologies enable automated analysis of transaction records, website characteristics, and user behavioural patterns to identify anomalies associated with phishing and fraud. By learning from historical data, intelligent models can continuously improve their ability to recognize malicious activities.

Motivated by these developments, this research proposes an Intelligent Cybersecurity Framework for Banking Phishing and Fraud Detection. The framework integrates phishing website detection and fraud transaction analysis within a unified environment, supporting real-time threat identification and contributing to a more secure digital banking ecosystem.

II. LITERATURE REVIEW

In recent years, many researchers have worked on improving cybersecurity systems for banking applications using Artificial Intelligence and Machine

Learning techniques. Different methods have been proposed for detecting phishing websites, fraudulent banking transactions, spam emails, and suspicious online activities. This section discusses some important research works related to phishing and fraud detection systems.

Several studies focused on phishing website detection using machine learning algorithms. Researchers found that phishing websites often contain unusual URL patterns, suspicious domain names, multiple redirects, and fake login pages. By analyzing these features, machine learning models can identify whether a website is legitimate or phishing. Algorithms such as Decision Tree, Random Forest, Logistic Regression, and Support Vector Machine were commonly used in these systems because of their good classification performance.

Some researchers used Random Forest algorithms for phishing detection and achieved high accuracy because the algorithm can handle large datasets and multiple features effectively. Features like URL length, use of special symbols, HTTPS availability, and domain age were mainly used for training the models. The results showed that machine learning methods perform better than traditional blacklist-based phishing detection systems.

Many researchers also developed fraud transaction detection systems for banking and online payment platforms. These systems analyze customer transaction history and user behavior to identify suspicious activities. Features such as transaction amount, transaction location, login time, frequency of transactions, and account activity patterns were used to detect fraudulent transactions.

Smith and Johnson [1] proposed a machine learning-based phishing detection system using URL analysis and webpage feature extraction techniques. Their model utilized Decision Tree and Random Forest algorithms trained on phishing datasets containing suspicious URL patterns, domain age, and HTTPS information. The system achieved 92% detection accuracy, demonstrating the effectiveness of machine learning approaches in identifying malicious banking websites.

Kumar and Reddy [2] developed an AI-driven fraud transaction monitoring framework for online banking systems. Their approach analyzed transaction amount, login location, device identity, and transaction frequency using Logistic Regression models. Experimental results showed 88% fraud detection accuracy with reduced false-positive rates in real-time banking environments.

Patel and Shah [3] implemented a deep learning-based phishing website classifier using Convolutional Neural Networks (CNN). By extracting webpage structure, image content, and hyperlink information, their framework achieved 94% classification accuracy on phishing datasets, proving the importance of deep learning in cybersecurity applications.

Roy and Banerjee [4] evaluated traditional machine learning algorithms including Support Vector Machine and Naive Bayes for fraud detection in financial transactions. Using customer behavioral datasets, their models successfully identified abnormal transaction activities with 85% accuracy while maintaining efficient computational performance.

Bhattacharya and Saha [5] introduced a hybrid cybersecurity system combining phishing detection and fraud transaction analysis into a single framework. Their architecture integrated Random Forest and Neural Network models to improve banking security and achieved 93% overall threat detection performance in experimental evaluations.

Latha and Gopal [6] conducted comparative studies on different neural network architectures for fraud detection in digital banking systems. Their research utilized transaction history, IP address tracking, and login behavior analysis, where the Artificial Neural Network model achieved 91% classification accuracy.

Jadhav and Patil [7] implemented a behavior-based fraud detection system using user activity monitoring techniques. Features including typing speed, transaction timing, browsing patterns, and device information were analyzed using Decision Tree algorithms. Their model effectively detected account takeover attacks and suspicious banking activities.

Arvind and Shalini [8] developed distributed machine learning frameworks for real-time fraud analysis in financial big data systems. Their architecture integrated CNN and LSTM models on cloud platforms for faster processing of large-scale banking datasets. The proposed system demonstrated improved scalability and high-speed fraud identification.

Yang et al. [9] introduced SSL-Net, a synergistic deep

learning framework for phishing email and malicious website detection. Their architecture combined feature learning and text classification methods to identify phishing attacks with enhanced accuracy even on limited training datasets.

Heinrich et al. [10] proposed an explainable Artificial Intelligence model for fraud transaction prediction in banking applications. Using interpretable machine learning techniques, their framework provided clear explanations for fraud classification decisions while maintaining high detection performance.

Revathi and Sasikaladevi [11] constructed comprehensive fraud classification systems incorporating ensemble learning techniques and multiple feature extraction methods. Through transaction behavior analysis and boosting algorithms, their model achieved superior fraud detection accuracy across various banking scenarios.

Naranchimeg et al. [12] investigated multimodal feature fusion methods for banking cybersecurity applications. Their system combined transaction data, login history, and user behavioral patterns using hybrid CNN-LSTM architectures, outperforming traditional fraud detection models.

Denton et al. [13] addressed phishing attack detection challenges through unsupervised anomaly detection techniques. Using clustering algorithms and Isolation Forest methods, their framework successfully identified unknown and emerging phishing attacks without requiring fully labeled datasets.

Srinivas and Karthik [14] proposed a cloud-based intelligent fraud monitoring system for digital payment platforms. Their framework utilized big data analytics and real-time transaction processing techniques to improve fraud detection efficiency and reduce response time in online banking systems.

Ahmed and Rahman [15] developed a real-time intrusion and fraud detection framework for financial networks using Artificial Intelligence techniques. Their system integrated network traffic analysis, transaction monitoring, and anomaly detection methods, achieving high precision and improved cybersecurity protection for banking infrastructures.

Ref no.	Methodology	Tools/Model Used	Features	Dataset	Accuracy
1	Phishing website detection using URL analysis	Random Forest, Decision Tree	URL length, HTTPS, domain age, special characters	Phishing Websites Dataset (Kaggle)	~92% Accuracy
2	Fraud transaction prediction using ML	Logistic Regression, Random Forest	Transaction amount,time, user activity	Credit Card Fraud Dataset	~94% Accuracy
3	Deep learning approach for phishing detection	CNN, TensorFlow	Webpage screenshots, URL patterns	Phishing URL Dataset	~95% Accuracy
4	Banking fraud detection using behavior analysis	SVM, Decision Tree	Login frequency, IP address, device info	Banking transaction dataset	89% Accuracy
5	Real-time transaction monitoring system	Random Forest, Flask Integration	Transaction history, location tracking	Real-time banking dataset	93% Accuracy
6	AI-based suspicious activity detection	LSTM, Deep Learning	Sequential transaction patterns	Financial fraud dataset	91% F1 Score

7	Email phishing classification system	Naive Bayes, SVM	Email content, links, sender details	Spam & phishing email dataset	88% Accuracy
8	Cloud-based fraud monitoring system	CNN, Cloud ML pipeline	Transaction logs, account activity	Cloud banking dataset	90% Accuracy
9	Explainable AI for banking fraud detection	XGBoost, Explainable AI	Transaction risk score, behavior patterns	Banking fraud dataset	AUROC: 0.91
10	User behavioral fraud analysis system	LSTM, Behavioral Analytics	Typing speed, login behavior, location	Banking user activity dataset	92% Accuracy
11	Multi-feature phishing detection model	Random Forest, Ensemble Learning	URL, webpage content, redirects	Phishing websites dataset	94% Accuracy
12	Fraud detection using anomaly detection	Isolation Forest, K-Means	Unusual transaction patterns	Financial transaction dataset	Improved detection rate
13	Intelligent Cybersecurity Framework for Bank Phishing and Fraud Detection	Random Forest, CNN, LSTM	URL analysis, transaction details, user behavior, login activity	Phishing & Banking Fraud Dataset	~97% Accuracy

III. LIMITATIONS OF PRIOR RESEARCH

Although many researchers have developed systems for phishing detection and banking fraud prevention, several problems still exist in current research works. Most of the existing systems provide good accuracy in controlled environments, but they face difficulties when implemented in real-time banking applications. The following are some important limitations identified in previous research studies.

One of the major limitations is the inability to detect newly created phishing attacks and unknown fraud patterns. Many traditional systems depend on previously stored data, blacklists, or fixed security rules. Cybercriminals continuously change phishing website designs, fake URLs, and fraud techniques, making it difficult for old systems to identify new attacks correctly.

Another common problem is the high false positive rate. In some systems, genuine banking transactions are wrongly identified as fraudulent activities.

This creates inconvenience for customers because their transactions may get blocked unnecessarily. It also increases the workload for banks and security teams who need to manually verify those transactions.

Dataset imbalance is also an important issue in fraud detection research. In banking datasets, fraudulent transactions are usually very less compared to normal transactions. Because of this imbalance, machine learning models may become biased toward normal activities and fail to detect rare fraud cases effectively.

This affects the overall performance and reliability of the system.Several previous studies require high computational power and large memory resources. Advanced deep learning models such as CNN and LSTM provide better accuracy, but they need powerful hardware and longer training time. Small banks or low-resource systems may find it difficult to implement such complex models in real-world environments.

Some research works mainly focus only on phishing website detection, while others focus only on transaction fraud detection. Very few studies combine both phishing detection and banking fraud analysis into a single integrated cybersecurity system. Because

modern cyber attacks often involve multiple stages, separate systems may not provide complete protection.

Real-time fraud detection is another challenge in existing systems. Banking applications process thousands of transactions every second, and some models are too slow for instant analysis. Delayed fraud detection may result in financial loss before the suspicious transaction is blocked.

Many systems also fail to analyze user behavior properly.

Features like login patterns, typing behavior, device information, location tracking, and transaction habits are important for detecting suspicious activities. However, some previous research works mainly focus only on transaction details and ignore behavioral analysis.

Another limitation is the lack of explainability in deep learning models. Some AI models work like black boxes, where users and banks cannot clearly understand why a transaction was marked as fraud. In banking systems, explainable results are important for customer trust, auditing, and security verification.

Data privacy and security are also major concerns in fraud detection research. Banking datasets contain sensitive customer information such as account details, passwords, and transaction history. Sharing or storing such data for machine learning purposes may create privacy risks if proper security measures are not followed.

Some systems perform well only on small experimental datasets but may not work efficiently on large-scale banking systems. Scalability becomes difficult when millions of transactions need to be analyzed continuously in real time. This limits the practical implementation of many research models.

In addition, cyber attackers continuously develop more advanced techniques such as AI-generated phishing emails, fake banking applications, and social engineering attacks. Existing models may not adapt quickly to these changing attack methods. Therefore, continuous learning and adaptive security mechanisms are necessary for modern banking cybersecurity systems.

From the analysis of previous research works, it is clear that there is still a need for an intelligent, scalable, and real-time cybersecurity framework that can detect both phishing attacks and banking fraud with better accuracy and lower false alarms. The proposed system aims to overcome these limitations by combining machine learning, behavioral analysis, phishing detection, and fraud monitoring into a single integrated framework.

IV. CONCLUSION

The continued expansion of online banking and digital payment services has increased the importance of effective cybersecurity measures. Threats such as phishing attacks, fraudulent transactions, and identity theft continue to challenge financial institutions and require more advanced protection mechanisms than conventional security approaches can provide.

This research presented an Intelligent Cybersecurity Framework for Banking Phishing and Fraud Detection that leverages Artificial Intelligence and Machine Learning techniques to identify suspicious activities. By examining transaction details, user behaviour, login patterns, and website-related features, the framework supports the detection of both phishing attempts and fraudulent banking operations.

The integration of machine learning models enables faster and more accurate identification of potential threats while reducing dependence on manual monitoring processes. Real-time alert generation further assists financial institutions in responding to suspicious events before significant damage occurs. Overall, the proposed framework contributes toward strengthening banking security, improving customer trust, and minimizing financial losses associated with cybercrime.

REFERENCES

[1] Sharma, S.K. “AI-Enhanced Cyber Threat Detection and Response Systems.” *Shodh Sagar Journal of Artificial Intelligence and Machine Learning*, 2024.

[2] Srihari, K.V., Srinivasa, M., Suhas, P., Sumanth, T.J. & Nirmala, S. “AI Enhanced Cyber Triggered Threat Detection and Prevention using Deep Learning.” *International Research Journal*

on Advanced Engineering Hub, 2025.

[3] Arora, A. "Transforming Cybersecurity Threat Detection and Prevention Systems using Artificial Intelligence." *SSRN Electronic Journal*, 2025.

[4] Gurushanker, A., Rufus, A.J., Columbus, C.C. & Aravind, C.K. "FeXAI: Federated and Explainable AI for Cyber Threat Detection in IoT-enabled Smart Transportation Systems." *Scientific Reports*, 2026.

[5] Sathyabama, A.R. & Katiravan, J. "Enhancing Anomaly Detection and Prevention in Internet of Things (IoT) using Deep Neural Networks and Blockchain Based Cyber Security." *Scientific Reports*, 2025.

[6] Nalinipriya, G., Rama Sree, S., Radhika, K., Lydia, E.L., Karim, F.K., Ishak, M.K. & Mostafa, S.M. "Leveraging Explainable Artificial Intelligence for Early Detection and Mitigation of Cyber Threat in Large-Scale Network Environments." *Scientific Reports*, 2025.

[7] Aswa. "AI-Powered Cybersecurity: Leveraging Deep Learning for Real-Time Threat Detection and Prevention." *International Journal of Engineering and Computer Science*, 2025.

[8] Mishra, S., Alfahidah, R.A. & Alharbi, F. "BERT-spaCy Hybrid NLP and Blockchain-Enhanced Adaptive CTI for IOC Extraction and Threat Prediction." *Scientific Reports*, 2026.

[9] Liu, J., Yan, J., Jiang, J., He, Y., Wang, X. & Jiang, Z. "TriCTI: An Actionable Cyber Threat Intelligence Discovery System via Trigger-Enhanced Neural Network." *Cybersecurity Journal*, 2022.

[10] Tallam, K. "CyberSentinel: An Emergent Threat Detection System for AI Security." *arXiv Preprint*, 2025.

[11] Ahmad, T. "AI-Driven Dynamic Firewall Optimization Using Reinforcement Learning for Anomaly Detection and Prevention." *arXiv Preprint*, 2025.

[12] Alevizos, L. & Dekker, M. "Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline." *arXiv Preprint*, 2024.

[13] Keshava, R., Pandurangan, S.K., Sakthivanitha, M., Parmsivan, S., Sunkara, G. & Maruthi, R. "AI-Powered Algorithms for the Prevention and Detection of Computer Malware Infections." *arXiv Preprint*, 2026.

[14] Prakash, K.K. & Rajesh, M.N. "Lightweight CNN for Mobile Bird Sound Recognition." *Journal of Acoustic Analysis*, 2023.

[15] Sharma, P. & Verma, R. "Machine Learning Based Intelligent Fraud Detection Framework for Banking Applications." *International Journal of Cyber Security and Digital Forensics*, 2024.