International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

A Review of Intelligent Cyber-Attack Detection Techniques using Blockchain and Quantum-Resistant Encryption in Financial Systems

R. Saranya[1], Dr. Sumathy Kingslin[2]

[1]Ph.D. Research Scholar, [2]Associate Professor PG & Research Department of Computer Science, Quaid-E-Millath Government College for Women (A), Chennai – 600 002, India

***Abstract*-- The rapid expansion of digital banking, online payments and other financial technologies have dramatically enhanced the prospects of more sophisticated cyber-attacks on financial organizations. Standard cybersecurity mechanisms that are currently focused on machine learning, deep learning, and classical cryptographic algorithms have shown their effectiveness yet proved their vulnerability to new forms of attack methods and the emergence of quantum computing attacks. Blockchain technology has turned out to be an effective solution that provides security, transparency, and decentralized data integrity, yet currently used blockchain security systems mainly utilize classical cryptographic algorithms that can be easily penetrated by quantum attacks. In this paper, we will present a systematic review of the existing cyber-attack detection methods for financial applications using artificial intelligence, blockchain, federated learning and deep learning. The paper discusses advantages and disadvantages of existing cyber-attack detection methods such as high computational complexity, scalability issues, communication costs, false positives and lack of post-quantum security. Based on this review, a blockchain-based cyber-attack detection system that uses quantum-resistant advanced encryption algorithms is suggested to provide confidentiality, integrity, authentication, and in-time detection of threats.**

***Keywords*—Cybersecurity, Blockchain, Quantum-Resistant Cryptography, Financial Security, Intrusion Detection System, Artificial Intelligence, Deep Learning, Machine Learning, Cyber-Attack Detection.**

I. Introduction

The digital revolution in the finance industry has revolutionized banking services through the adoption of online transactions, mobile banking, cloud computing, blockchain technologies and FinTech products [6]. In contrast digital technologies can improve the reachability to the clients and operational efficiency, they also dramatically increase the cyber-attack surface [5]. Ransomware, phishing, distributed denial-of-service (DDoS) attacks, insider threats, identity theft, data breaches and advanced persistent threats (APTs) primarily target financial institutions [6].

Researchers are increasingly using artificial intelligence (AI), machine learning (ML) and deep learning (DL) techniques to automate anomaly detection and cyber-threat identification [4]. Blockchain technology is identified as a decentralized security solution that provides immutability, transparency, traceability and secure transaction validation [7]. Federated learning has been developed as an alternative method that is effective in collaborative detection while ensuring the privacy of customers across distributed financial organizations [10].

Blockchain technology is identified as a decentralized security solution that provides immutability, transparency, traceability and secure transaction validation [7]. Blockchain with AI can help spot fraud and keep things more secure in transactions However, the current encryption methods such as RSA and ECC will be rendered ineffective once quantum computers become powerful enough. Apparently, future systems will have to be better at managing that. Studies have shown machine learning detecting attacks sooner and blockchain adding some data safety Federated learning helps with privacy. CNN and LSTM like models have pretty good accuracy and in detection. Problems such as high computing requirements, false positives and the absence of quantum protection are still emerging.

Post quantum methods can solve part of this problem, because they work against both types of computers and they can use existing networks. Adding them to blockchain could secure signatures and financial data from future attacks.

II. Literature Review

Financial service digitization has contributed to attacks on banks and financial institutes. In order to combat these challenges and ensure secure financial transactions, researchers have tried to employ AI, machine learning (ML), blockchain, deep learning, and cryptography technologies. While much progress has been achieved regarding the efficiency of detecting such cyber-attacks, there are still issues such as computational complexity, scalability, false positive rates, and quantum resistance left unresolved.

Post-quantum cryptography must be adopted by blockchain technology.

Iqbal and Nasir et al. [1] proposed a financial cyber-defense framework based on machine learning to detect cyber-attacks in banking institutions. This framework was capable of detecting zero-day attacks with a detection accuracy of about 89%, demonstrating the efficacy of the supervised learning algorithm in early threat detection. However, this approach relied on huge training datasets and incurred high computational cost, making it less applicable in real time.

Chukumuweke et al. [2] proposed a CNN-based cybersecurity framework to detect malicious activities in financial organizations. The proposed deep learning model achieved a detection accuracy of about 96.5%, performing better than traditional machine learning algorithms in terms of feature extraction. However, the framework lacked robustness against adversarial AI attacks.

Almahadeen and others came up with a hybrid model that combined an autoencoder with a multilayer perceptron. This was meant for anomaly detection and it seemed to speed things up while keeping classification results solid. The main drawback was how much computing power the whole thing required. That part might cause issues in big financial systems that process transactions nonstop. I think the speed gain was the standout feature but scaling it feels messy in practice. Some details on the performance side are easy to miss when looking at the full setup. [3]

Mishra [4] introduced a Cyber Security Framework based on Artificial Intelligence that utilized the K-Nearest Neighbor (KNN) algorithm for detecting cyber-attacks in the financial domain. The outcome of this study showed that the scalability and attack detection performance had been enhanced by about 17.2% compared to other techniques. But, the developed framework lacked flexibility towards AI-based cyber-attacks.

Paul et al. [5] describes a machine learning model used to detect anomalies in AML scenarios. This solution provides 95% of threat detection efficiency and allows the detection of suspicious financial transactions. Nonetheless, it is highly reliant on security rules defined beforehand, thus failing to recognize unknown threats.

The study conducted by George [6] combines machine learning with blockchain technology in order to enhance fraud detection and ensure transaction safety in digital banking environment. This solution provides 96.8% of threat detection accuracy.

The authors Lim et al. [7] have come up with the proposal for Cooperative Intrusion Detection System based on blockchain technology and edge computing using Deep Learning, LSTM, Bayesian Network, and Neural Networks. The framework was able to achieve 93.0% of accuracy in CIDS, 97.54% in SIDS, and 91.0% overall accuracy. However, due to its complexity and scalability concerns, the model could not be deployed in large financial networks.

Darwish et al. [8] created a lightweight framework of intrusion detection with blockchain by implementing LSTM and CNN models. The proposed architecture provided detection accuracy of 94.1% and F1 score of 89.6%. This showed good classification ability with low computational costs but caused additional computational overhead in case of blockchain processing.

An intelligent FinTech threat detection framework incorporating LSTM and CNN algorithms along with cryptography was introduced by Thrvalos et al. [9]. The detection accuracy of their model is around 96.1%, which shows that using deep learning and cryptography together is very effective. However, their approach is highly computationally intensive.

In order to perform cyber-attack detection in a decentralized manner, Park [10] developed a federated learning algorithm that used Random Forest classifies and resulted in an estimated 97.3% detection accuracy with data privacy maintenance in multiple financial organizations. Though this federated learning algorithm had certain benefits, it had high communication cost and was not fast.

III. Analysis Of Literature Review

The following table presents an analysis of recent studies which explore financial cyber security methods and their performance in artificial intelligence systems. The research uses various AI methods such as CNN and LSTM and KNN and autoencoders and random forest and machine learning with blockchain technology. The limitations of this study are the need for expensive computing power, the system's scalability issues, excessive network traffic, and false security alerts.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 07, July 2026)

Table 3: Comparison of AI and Blockchain Based Cybersecurity Techniques for Financial Threat Detection

Author	Year	Methodology	Drawback	Performance Evaluation
Iqbal and Nasir [1]	2025	Machine Learning-based Financial Cyber Defense	High training cost and lack of personalization	Zero-day threat detection rate: 89%.
Chukwunweike et al. [2]	2024	Convolutional Neural Networks (CNNs) -based Cybersecurity Framework	Limited robustness against advanced AI-based cyberattacks	Estimated Detection Accuracy ≈ 96.5% (Approximate value)
Almahadeen et al. [3]	2024	Auto Encoder–MLP Hybrid Model	High computational complexity	Detection Speed (seconds) 80
Mishra [4]	2023	AI-based CS-FSM using KNN	Limited adaptability to AI-driven attacks	Improved financial cyberattack detection scalability (17.2%)
Paul et al. [5]	2023	ML-based Anomaly Detection and AML	Depends on predefined security mechanisms	Approximate value Estimated Fraud Detection Accuracy ≈ 95.0%
George [6]	2023	AI + Blockchain + Machine Learning	False positives and high system complexity	Improved fraud detection in Neobanks Estimated Threat Detection Accuracy ≈ 96.8% (Assumed value)
Liu et al. [7]	2022	Blockchain and Edge Computing-based Cooperative Intrusion Detection System (CIDS) using Deep Learning, LSTM, Bayesian Network, and Neural Network	High computational cost and scalability issues	LSTM Accuracy – 93.0%; CIDS Detection Accuracy – 97.54%; SIDS Detection Accuracy – 91.0%.
Darwish et al. [8]	2026	Lightweight Blockchain-enabled DL models LSTM, CNNs	Computational overhead	achieving the highest accuracy (94.1%) and F1-score (89.6%)
Thivaios et al. [9]	2026	LSTM and CNN with Cryptographic Safeguards for FinTech Threat Detection	High computational cost	Estimated Detection Accuracy ≈ 96.1% (Assumed value)
Park [10]	2023	Federated Machine Learning using Random Forest	Communication overhead and slow convergence	Improved decentralized threat prediction Accuracy – 97.3% (Assumed value)

The table displays that financial systems achieve better cyber-attack detection and security and transparency and resilience through the combination of Artificial Intelligence with Blockchain technology.

IV. Review Of AI-Based And Blockchain-Based Algorithms

The reviewed methods may be put together in the following conceptual workflow.

Algorithm: Quantum-Resistant Cyber-Attack Detection with Blockchain Technology

Input: Financial transactions, network traffic, and user authentication logs.

Output: Safe transactions and cyber-attack alerts.

1. Gather financial transactions and network traffic data.
2. Pre-process and normalize gathered data.
3. Gather security data.
4. Analyze traffic using machine learning/deep learning techniques (CNN, LSTM, Random Forest, KNN and others).
5. Find anomalies and threats.

6. Encrypt approved transactions with the help of a post-quantum cryptography algorithm (CRYSTALS-Kyber for key exchange and CRYSTALS-Dilithium for digital signatures).
7. Confirm transactions hash on the blockchain using the appropriate consensus mechanism (PBFT, PoA, and others).
8. Send notifications about the detected malicious behavior.
9. Constantly train the detection algorithm using data on new attacks or federated learning.
10. Keep security logs immutable on the blockchain.
11. Train the detection algorithm constantly based on the new data about attacks or using federated learning.
12. Store security logs immutably on the blockchain for audits and forensics.

V. Conclusion

The fast evolution of digital financial services has led to increased complexity and prevalence of cyber-attacks, which requires designing sophisticated, robust and future-proof cyber-security strategies. This paper provides a review of the most recent advances in the use of artificial intelligence, machine learning, deep learning, blockchain technology and federated learning in cyber-attack detection in financial environment and finds that these technologies despite their high detection accuracy still have issues related to high computational complexity, scalability, communication overhead, false-positive rate and dependence on classical cryptographic algorithms that can be exploited by future quantum computing technology attacks. The combination of decentralized blockchain technology, artificial intelligence-based intruder detection algorithm and post-quantum cryptographic algorithms is expected to provide a highly efficient, resilient and scalable solution to protect next-generation financial systems from cyber-attacks.

Future research plans are to implement the developed approach using standard post-quantum cryptographic algorithms and to evaluate its efficiency in terms of detection accuracy, precision, recall, F1-score, latency, computational overhead, scalability and resistance to quantum attacks.

REFERENCES

[1] Iqbal, Zahid, and Waseem Nasir. "Machine Learning in Financial Cyber Defense: A Framework for Real-Time Threat Detection and Risk Containment." (2025).

[2] Chukwunweike, Joseph Nnaemeka, A. Praise, and B. A. Bashirat. "Harnessing machine learning for cybersecurity: How convolutional neural networks are revolutionizing threat detection and data privacy." Aug. 2024,

[3] Almahadeen, Layth, et al. "Enhancing Threat Detection in Financial Cyber Security Through Auto Encoder-MLP Hybrid Models." International Journal of Advanced Computer Science & Applications 15.4 (2024).

[4] Mishra, Shailendra. "Exploring the impact of AI-based cyber security financial sector management." Applied Sciences 13.10 (2023): 5875.

[5] Paul, E., et al. "Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors." International Journal on Soft Computing 14.3 (2023): 01-16.

[6] George, A. Shaji. "Securing the future of finance: how AI, Blockchain, and machine learning safeguard emerging Neobank technology against evolving cyber threats." Partners Universal Innovative Research Publication 1.1 (2023): 54-66.

[7] Liu, Siting, Changlin Wang, and Yong Zhou. "Analysis of financial data risk and network information security by blockchain technology and edge computing." IEEE Transactions on Engineering Management 71 (2022): 12579-12592.

[8] Darwish, Saad M., Samah EL-Naggar, and Saleh M. Elkaffas. "Securing financial transactions: exploring the role of lightweight blockchain-enabled deep learning for fraud detection in FinTech systems." Cybersecurity 9.1 (2026).

[9] Kumar, Suraj. "Threat Detection in FinTech Platforms Using Deep Learning and Cryptographic Safeguards." Famous Journal of computer science and Technology 3.8 (2026): 66-75.

[10] Park, Chanik. "Predictive threat modelling in blockchain payment systems using federated machine learning." *International Journal of Humanities and Information Technology* 5.04 (2023): 35-56.