

A Review of Intelligent Cyber-Attack Detection Techniques for Smart Healthcare using Explainable AI, Federated Learning and Block chain

P. Revathi¹, Dr. Sumathy Kingslin²

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

Abstract— The Internet of Medical Things (IoMT), wearable technology, cloud computing, smart healthcare, and electronic health records have all grown quickly, greatly enhancing healthcare services but opening the door for increasingly complex cyberattacks on healthcare systems. Current cybersecurity techniques based on blockchain, federated learning, deep learning, artificial intelligence, and machine learning have proven successful in identifying criminal activity and safeguarding private medical data. Nevertheless, there are still drawbacks with current methods, including high computational complexity, scalability problems, communication cost, false positives, limited explainability, privacy hazards, and hurdles in identifying emerging cyberattacks. Data integrity, authentication, transparency, traceability, and secure healthcare data sharing are all made possible by block chain technology, which has become a powerful decentralized security mechanism. Federated learning lessens the requirement for dispersed enterprises to share sensitive healthcare data while also promoting cooperative cyberattack detection. This work offers a comprehensive analysis of current cybersecurity methods for IoMT and smart healthcare settings that make use of blockchain, federated learning, deep learning, artificial intelligence, and machine learning. In addition to identifying significant research gaps in the areas of attack detection, feature reduction, interpretability, privacy, authentication, integrity, trust, and scalability, the article examines the benefits and drawbacks of current methods. The study emphasizes the necessity of adaptable, explainable, privacy-preserving, scalable, and computationally efficient cybersecurity solutions for next-generation smart healthcare environments based on the examined literature. **Keywords**— Smart Healthcare, Internet of Medical Things (IoMT), Cybersecurity, Block chain, Artificial Intelligence, Machine Learning, Deep Learning, Federated Learning, Intrusion Detection, Cyber-Attack Detection, Healthcare Data Security.

I. INTRODUCTION

To deliver dynamic healthcare services, smart healthcare combines wearable technology, cloud computing, artificial intelligence (AI), IoT-enabled medical devices, electronic health records, and intelligent communication systems.

Although deep learning has made it easier to analyze complicated healthcare data and make predictive decisions, cybersecurity exposure has also increased due to greater connectivity between medical equipment, healthcare servers, and communication networks. Because cyber breaches can impact both the provision of vital services and private patient data, healthcare facilities are especially sensitive.

The use of wearable technology, cloud computing, Internet of Medical Things (IoMT), electronic health records, and intelligent healthcare applications, the quick growth of smart healthcare has revolutionized medical services [1]. While these technologies enhance clinical decision-making, data exchange, patient monitoring, and healthcare accessibility, they also greatly expand the cybersecurity attack surface of healthcare systems [2]. Cyberthreats that can affect linked medical equipment and healthcare networks include ransomware, malware, distributed denial-of-service (DDoS) attacks, unauthorized access, data injection, phishing, insider attacks, and data breaches [5]. In IoMT contexts, researchers are progressively automating anomaly detection, intrusion detection, and cyberattack identification thru the use of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) approaches [6]. Data integrity, authentication, transparency, traceability, and safe healthcare transactions are all made possible by block chain technology, which has become a decentralized security mechanism [12]. Federated learning has also been investigated as a way for dispersed healthcare institutions to collaborate on learning without directly exchanging sensitive patient data while maintaining privacy [3]. AI-based methods that have shown promise in identifying fraudulent activity and healthcare network intrusions include ANN, Random Forest, KNN, ensemble learning, DRNN, and Transformer models [14]. Healthcare data security and reliable information sharing can be further strengthened by combining blockchain technology with artificial learning.



High computing needs, false positives, communication cost, scalability, limited explainability, privacy hazards, malicious model modifications, and difficulties in identifying evolving cyberattacks are some of the issues that still plague current techniques.

II. LITERATURE REVIEW

Healthcare systems are now more vulnerable to cyberattacks due to the quick uptake of wearable technology, cloud computing, Internet of Medical Things (IoMT), electronic health records, and smart healthcare applications. Researchers have increasingly used artificial intelligence (AI), machine learning (ML), deep learning (DL), block chain, federated learning, and cryptography techniques to address these issues and safeguard private health information.

Kilincer et al. [6] used an optimized Multilayer Perceptron (MLP) and Recursive Feature Elimination with Regressor to develop an automated cybersecurity attack detection method for healthcare systems. Effective feature selection and attack detection for IoMT scenarios were demonstrated by the method.

Kumar [7] used an ensemble classifier to create a real-time framework for detecting healthcare cyberattacks. The capacity to detect malicious activity was enhanced by the use of numerous classifiers; however, the multi-classifier architecture added processing complexity, which may make real-time deployment in big healthcare networks difficult.

Chidambaranathan and Geetha [8] looked into a block chain-based method for detecting attacks on electronic healthcare data that is enabled by deep learning. Their research showed that deep learning and blockchain can improve attack detection and healthcare data security. However, combining blockchain protocols with computationally demanding deep learning models may result in higher processing and communication demands.

A Security-of-Things intrusion detection system for smart healthcare settings was created by Iwendi et al. [9]. The method emphasized the significance of intrusion detection

for IoT-enabled healthcare systems, but generalized attack detection is still difficult due to the heterogeneous nature of IoMT devices and constantly shifting network behavior.

Using Particle Swarm Optimization (PSO), Deep Recurrent Neural Networks (DRNN), and machine learning methods, Saheed and Arowolo [10] examined an effective cyberattack detection strategy for IoMT environments. The study's detection accuracy of almost 99.76% shows how well feature optimization and deep recurrent learning work together.

A Security-of-Things intrusion detection system for smart healthcare settings was created by Iwendi et al. [9]. The method emphasized the significance of intrusion detection for IoT-enabled healthcare systems, but generalized attack detection is still difficult due to the heterogeneous nature of IoMT devices and constantly shifting network behavior.

Using Particle Swarm Optimization (PSO), Deep Recurrent Neural Networks (DRNN), and machine learning methods, Saheed and Arowolo [10] examined an effective cyberattack detection strategy for IoMT environments. The study's detection accuracy of almost 99.76% shows how well feature optimization and deep recurrent learning work together..

III. ANALYSIS OF LITERATURE REVIEW

An analysis of recent research on cybersecurity techniques for smart healthcare systems utilizing blockchain, federated learning, deep learning, machine learning, and artificial intelligence is shown in the following table. For cyberattack detection, intrusion detection, authentication, privacy preservation, and secure healthcare data sharing, the reviewed research uses a variety of techniques, including MLP, ensemble learning, deep recurrent neural networks, LightGBM, Transformer, ANN, Decision Tree, Random Forest, KNN, blockchain, smart contracts, and federated learning. The experiments show encouraging results in identifying harmful activity and enhancing the security of healthcare data.

TABLE 1: REVIEW OF AI- AND BLOCKCHAIN-BASED SECURITY APPROACHES FOR SMART HEALTHCARE

Author	Year	Technique	Major limitation	Reported contribution
Kilincer et al. [6]	2023	Regressor + optimized MLP	High computational complexity	IoMT attack detection; adaptive feature selection needed
Kumar [7]	2022	Ensemble classifier	Multi-stage/processing complexity	Real-time healthcare attack detection
Chidambaranathan & Geetha [8]	2024	Deep learning + blockchain	Resource and processing requirements	Blockchain-assisted healthcare attack detection
Iwendi et al. [9]	2021	Security-of-Things IDS	Detection scope and deployment constraints	IoT/IoMT intrusion detection
Saheed & Arowolo [10]	2021	RNN + ML	Feature optimization and deep processing cost	99.76% reported accuracy
Wazid et al. [11]	2022	Blockchain ransomware security	Primarily ransomware-focused	Tamper-resistant healthcare protection
Datta & Namasudra [12]	2024	Blockchain + smart contract	Cryptographic communication overhead	Secure EMR transactions
Ghourabi [13]	2022	LightGBM + Transformer	Multiple-model computational complexity	Healthcare intrusion/malware detection
Sundas et al. [14]	2022	ANN, DT, RF, KNN	Moderate detection performance	91% detection success; 90% F1
Wazid et al. [15]	2023	Ensemble ML	High computational complexity	Multi-attack intrusion detection

The main research gaps found in the examined smart healthcare cybersecurity studies are compiled in the following table. It draws attention to current security strategies, their noted shortcomings, and the research avenues suggested by the literature study.

TABLE 2: MAJOR RESEARCH GAPS IDENTIFIED FROM THE REVIEWED STUDIES

Security requirement	Common approach	Observed limitation	Integrated direction
Attack detection	ML/DL/ensemble models	False positives; changing attacks	Spatial-temporal and adaptive learning
Feature reduction	RFE, GA, PSO	Optimization overhead	DQHHO-based multi-objective selection
Interpretability	AI/DL models	Black-box decisions	XAI within EHNFTN
Privacy	Federated learning	Malicious model updates	Authenticated and blockchain-validated FL
Authentication	Blockchain	Partial security coverage	ECC signatures + certificate validation

IV. REVIEW OF AI-BASED AND BLOCKCHAIN-BASED ALGORITHMS

A conceptual process built from the original paper can be used to illustrate the reviewed methodologies. Instead of presenting the workflow as a newly proposed method, it is offered here as a review synthesis.

Algorithm: Secure Federated Healthcare Workflow and Integrated Intelligent Cyber-Attack Detection

Input includes node IDs, model updates, IoMT network traffic, healthcare communication logs, and local healthcare data.

Classification of cyberattacks, comprehensible security judgments, verified nodes, a reliable global model, and unchangeable security records are the results.

1. Gather statistics on healthcare communication and heterogeneous IoMT network traffic.
2. Pre-process the data by eliminating temporal abnormalities, redundant packets, missing values, and communication noise.
3. Create a model of temporal and spatial communication dependencies.
4. Reduce dimensionality and redundancy by optimizing the learned feature representation.
5. Categorize cyberattacks.
6. Verify the digital signatures and certificates of participating healthcare nodes.
7. Create local federated model updates and store raw healthcare data at regional organizations.
8. Updates to the local model should be encrypted and sent to a permissioned blockchain.
9. Use smart contracts to confirm transaction legitimacy, integrity, and access permissions.
10. Verify updates and reject submissions that have been tampered with or are not permitted.
11. Combine local model parameters that have been verified and agreed by consensus to create a global model.
12. Redistribute the global model for the subsequent federated-learning cycle and permanently record the aggregate result.

V. CONCLUSION

The examined research shows that blockchain, federated learning, deep learning, artificial intelligence, and machine learning offer viable ways to improve cybersecurity in smart healthcare systems.

Numerous methods have been effectively used for cyberattack detection, intrusion detection, authentication, privacy preservation, and secure healthcare data exchange, including MLP, ensemble learning, RNN, ANN, Decision Tree, Random Forest, KNN, blockchain, smart contracts, and federated learning. Research demonstrates that blockchain improves data integrity, decentralization, authentication, and traceability, federated learning facilitates privacy-preserving collaborative learning, and AI-based methods can boost the identification of criminal activity. High computing needs, scalability, communication overhead, false positives, limited explainability, privacy hazards, and detection of emerging cyberattacks are among the outstanding issues. In order to provide complete protection for diverse IoMT and smart healthcare environments, future research should concentrate on creating effective, scalable, adaptable, explainable, and privacy-preserving cybersecurity solutions.

REFERENCES

- [1] Lv, Zhihan, et al. "Deep learning-based smart predictive evaluation for interactive multimedia-enabled smart healthcare." *ACM Transactions on Multimedia Computing, Communications, and Applications* 18.1s (2022): 1-20.
- [2] Bhosale, Karuna S., Maria Nenova, and Georgi Iliev. "A study of cyber attacks: In the healthcare sector." *IEEE*, 2021.
- [3] Rahman, Anichur, et al. "Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues." *Cluster Computing* 26.4 (2023): 2271-2311.
- [4] Chakraborty, Chinmay, et al. "Intelligent AI-based healthcare cyber security system using multi-source transfer learning method." *ACM Transactions on Sensor Networks* (2023).
- [5] Alrowais, Fadwa, et al. "Cyber attack detection in healthcare data using cyber-physical system with optimized algorithm." *Computers and Electrical Engineering* 108 (2023): 108636.
- [6] Kilincer, Ilhan Firat, et al. "Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization." *Biocybernetics and Biomedical Engineering* 43.1 (2023): 30-41.
- [7] Kumar, CNS Vinoth. "A real time health care cyber attack detection using ensemble classifier." *Computers and Electrical Engineering* 101 (2022): 108043.
- [8] Chidambaramanathan, S., and R. Geetha. "Deep learning enabled blockchain based electronic healthcare data attack detection for smart health systems." *Measurement: Sensors* 31 (2024): 100959.
- [9] Iwendu, Celestine, et al. "Security of things intrusion detection system for smart healthcare." *Electronics* 10.12 (2021): 1375.
- [10] Saheed, Yakub Kayode, and Micheal Olaolu Arowolo. "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms." *IEEE Access* 9 (2021): 161546-161554.
- [11] Wazid, Mohammad, Ashok Kumar Das, and Sachin Shetty. "BSFR-SH: Blockchain-enabled security framework against ransomware attacks for smart healthcare." *IEEE Transactions on Consumer Electronics* 69.1 (2022): 18-28.



International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 08, August 2026)

- [12] Datta, Sagnik, and Suyel Namasudra. "Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing." *IEEE Transactions on Consumer Electronics* 70.1 (2024): 4026-4036.
- [13] Ghourabi, Abdallah. "A security model based on lightgbm and transformer to protect healthcare systems from cyberattacks." *IEEE Access* 10 (2022): 48890-48903.
- [14] Sundas, Amit, et al. "HealthGuard: An intelligent healthcare system security framework based on machine learning." *Sustainability* 14.19 (2022): 11934.
- [15] Wazid, Mohammad, et al. "An ensemble-based machine learning-envisioned intrusion detection in industry 5.0-driven healthcare applications." *IEEE Transactions on Consumer Electronics* 70.1 (2023): 1903-1912.