A Review of Privacy-Preserving Intrusion Detection for Healthcare Edge-IoT

P.Revathi[1] (Research Scholar), Dr. Sumathy Kingslin[2] (Associate Professor)
[1, 2] PG and Research Department of Computer Science
[1,2] Quaid-E-Millath Govt College for Women (A), Anna Salai, Chennai 600002, Tamilnadu, India

ABSTRACT

The rapid adoption of Edge Computing and Internet of Things (IoT) technologies in healthcare has enabled real-time patient monitoring and low-latency clinical decision support. However, the distributed and resource-constrained nature of Edge-IoT systems makes them highly vulnerable to cyber-attacks such as data breaches, ransomware, and denial-of-service, which threaten patient privacy and system reliability. Traditional centralized AI-based intrusion detection systems (IDS) face limitations in privacy preservation, scalability, and suitability for edge environments. To address these challenges, this paper proposes a secure and privacy-preserving cyber-attack detection framework that integrates an optimized LSTM Gated Multi-Layer Perceptron Neural Network (LSTMG-MLPNN) with Federated Learning (FL) and Med-Chain block chain technology. Federated Learning enables collaborative model training without sharing raw patient data, and Med-Chain with lattice encryption ensures secure aggregation, trust management, and auditability.The proposed system provides an effective, scalable, and privacy-aware solution for cyber-attack detection in healthcare Edge-IoT environments.

Keywords: Edge Computing, Federated learning, Long Short Term Memory, Multi layer Perceptron Neural Network.

I.INTRODUCTION

The integration of Edge Computing and the Internet of Things (IoT) has transformed modern healthcare by enabling continuous patient monitoring, real-time data analytics, and rapid clinical decision-making. Wearable sensors, smart medical devices, and edge nodes now collect and process sensitive health data close to the source, reducing latency and improving responsiveness. Despite these advantages, the decentralized architecture of Edge-IoT systems significantly increases their exposure to cyber threats. Attacks such as unauthorized access, data manipulation, ransomware, and denial-of-service can compromise the confidentiality, integrity, and availability of critical healthcare information, directly affecting patient safety and trust.

Artificial Intelligence (AI) has emerged as a powerful tool for detecting and mitigating cyber-attacks by learning complex patterns and identifying anomalies in large-scale network traffic. Deep learning models such as CNNs, RNNs, LSTMs, and GANs have shown promising results in intrusion detection. However, most existing AI-based systems rely on centralized training, which requires collecting sensitive patient data in a central server. This raises serious concerns regarding privacy, regulatory compliance, and large-scale data breaches. Moreover, centralized models are often computationally expensive and poorly suited for deployment on resource-constrained edge devices. Another challenge in intrusion detection is

handling high-dimensional and noisy data. Effective feature selection and optimization are essential to reduce redundancy, improve accuracy, and lower computational cost. Cyber-attacks often exhibit temporal behaviour, requiring models that can learn both sequential and nonlinear patterns

II.REVIEW OF LITERATURE

Recent studies emphasize that cyber security in healthcare must address confidentiality, integrity, and availability while operating under strict privacy regulations. Cybersecurity in healthcare IoT and edge computing environments has become a critical research area due to the increasing number of cyber-attacks targeting sensitive patient data. Researchers have explored AI, block chain, and federated learning to build secure, privacy-preserving, and intelligent systems.

Goffer et al. propose an AI-enhanced cyber threat detection framework for critical infrastructure, emphasizing real-time threat intelligence and automated response mechanisms. Their study highlights how deep learning improves detection accuracy but lacks integration with decentralized privacy frameworks [1]. Virk et al. discuss cybersecurity regulations and AI governance in healthcare. They stress that while AI improves detection, data privacy and ethical compliance remain major challenges, especially in centralized learning systems[2]

Gupta et al. analyze risks in responsible AI for digital healthcare. Their work identifies bias, transparency, and privacy as major limitations of standalone AI models and recommends hybrid systems for trustworthy deployment.Gabriel's thesis focuses on ethical and privacy issues in AI-based healthcare data collection. It concludes that decentralized data processing models such as federated learning can significantly reduce data leakage risks[3].

Bashir et al. present a comprehensive study on Federated Learning in the Healthcare Metaverse, showing that FL enables collaborative learning without exposing raw patient data. However, they note the need for secure aggregation and audit mechanisms [4].

Singh and Sevukamoorthy integrate block chain with AI-based threat detection in financial networks. Their results show improved integrity and tamper resistance, but scalability and latency remain open challenges [5] .Mansour develops a block chain-enabled deep learning intrusion detection model using optimization and recurrent networks. The study shows improved detection accuracy in cyber-physical systems, but it does not address edge-level resource constraints [6].

Karn et al. apply GAN-LSTM auto encoders for anomaly detection in financial networks. Their AI-Enhanced Defence-in-Depth framework demonstrates high detection performance but is vulnerable to adversarial manipulation without block chain validation [7].

Bhambri and Starostka-Patyk propose an AI + Block chain framework for decentralized threat prevention using smart contracts. They emphasize transparency and automated response but do not incorporate federated learning for privacy-preserving collaboration [8]. Awotunde et al. use KPCA-CNN with block chain for smart city IoT security. Their hybrid deep learning model improves prediction accuracy and data integrity, but feature dependency and scalability are not fully optimized [9].

III.ANALYSIS OF LITERATURE REVIEW

Researchers worked on various platforms using various Learning algorithms .The domains and techniques used, key contributions, limitations are discussed as mentioned in the previous section.

Table1: Analysis of Literature Review

Author / Year	Domain / Application	Techniques Used	Key Contributions	Limitations / Gaps
Goffer et al., 2025	Critical Infrastructure Security	AI-based IDS	Real-time threat detection and response	No privacy-preserving learning
Virk et al., 2025	Healthcare Policy & Cybersecurity	AI + Regulations	Highlights privacy and compliance issues	No technical security model
Gupta et al., 2023	Digital Healthcare AI	Responsible AI	Identifies bias, trust, transparency issues	Lacks secure AI framework
Gabriel, 2023	Healthcare Data Privacy	Ethical AI	Shows risk of centralized data collection	No intrusion detection
Bashir et al., 2023	Healthcare Metaverse	Federated Learning	FL enables collaborative learning	Needs secure audit & routing
Singh & Sevukamoorthy, 2023	Financial Networks	AI + Block chain	Improves integrity & tamper resistance	High latency & cost
Mansour, 2022	CPS Intrusion Detection	DL + Optimization + Block chain	High accuracy IDS	Not edge-optimized
Karn et al., 2025	Financial Network Security	GAN + LSTM	Strong anomaly detection	Vulnerable to adversarial attacks
Bhambri & Starostka-Patyk, 2025	Decentralized Security	AI + Smart Contracts	Automated threat prevention	No federated collaboration

IV.DEEP LEARNING MODELS

A deep learning model is made up of a collection of nodes that layer and connect in neural networks. In order to find patterns, these networks send and receive data as it moves through each layer. Different kinds of neural networks are used by deep learning models to accomplish particular goals.

Figure1: Deep Learning Models[22]

1. Deep Reinforcement Learning (DRL)

Deep Reinforcement Learning (DRL) models use reward mechanisms to interact with the environment and learn the best course of action. By regularly revising its policy, DRL in intrusion detection adjusts to shifting attack patterns. However, DRL's capacity to identify intricate temporal correlations in network traffic is constrained by its usual reliance on centralized training and simple feature filtering. Table 1 illustrates that DRL is less appropriate for real-time, privacy-sensitive healthcare IoT contexts due to its middling accuracy (77%) and comparatively increased time complexity (0.79 ms).

2. Generative Adversarial Network (GAN + LSTM Auto encoder)

A generator-discriminator architecture is used by GAN-based IDS to simulate typical behavior and identify abnormalities. It captures temporal patterns in traffic flows when paired with LSTM auto encoders. Despite its 82% increase in detection accuracy over DRL, this hybrid model still relies on centralized learning and heuristic feature selection. It is susceptible to adversarial manipulation and data leakage due to the absence of robust encryption and block chain validation.

3. Convolution Neural Network (CNN)

Convolution filters are an efficient way for CNN models to extract spatial patterns from structured traffic data. CNN increases detection accuracy (87%) and learning efficiency using PCA/KPCA-based feature reduction. Long-term temporal dependencies in intrusion behavior, however, are harder for CNNs to capture. Furthermore, their partial block chain utilization and centralized training restrict the management of trust and privacy in dispersed healthcare IoT systems.

4. Recurrent Neural Network (RNN)

RNNs are made to handle sequential data and identify patterns in network traffic over time. Relevant signal extraction is improved by correlation-based feature selection. In comparison to LSTM-based models, RNNs have slower convergence and vanishing gradient problems, despite their high accuracy of 85%. Furthermore, their use in privacy-sensitive settings is limited by the lack of robust security measures and federated training.

5. Long Short-Term Memory (LSTM)

A unique kind of Recurrent Neural Network (RNN) called Long Short-Term Memory (LSTM) was created to efficiently identify long-term dependencies in sequential input. LSTM is used to describe temporal patterns in network traffic and system behavior in cyber attack detection, as attacks frequently change over time instead of manifesting as discrete occurrences. LSTM employs a gated memory cell layout with input, forget, and output gates to regulate information flow, in contrast to conventional RNNs. By removing irrelevant or noisy data, these gates enable the network to preserve significant historical context.By learning time-dependent behavior changes, LSTM assists in detecting slow and covert attacks including data exfiltration, lateral movement, and persistent threats in healthcare Edge-IoT systems.

It is quite useful for intrusion detection because it can capture both short-term and long-term correlations, which improves memory and lowers false positives.

LSTM learns a function:

$$h_t = f(x_t, h_{t-1}, C_{t-1)})$$

Where h_t is the hidden state and c_t is the cell memory.

6. Multi-Layer Perceptron Neural Network (MLPNN)

An input layer, one or more hidden layers, and an output layer make up a feed-forward artificial neural network known as a Multi-Layer Perceptron Neural Network (MLPNN). To learn intricate mappings between input data and output classes, nonlinear activation functions like ReLU or sigmoid are applied to each layer, which is made up of neurons connected by weighted connections. Using extracted and refined feature sets, MLPNN is utilized in intrusion detection systems to categorize network activity as either benign or malevolent.MLPNN's strength is its capacity to learn nonlinear decision boundaries, which enables it to discern minute distinctions between attack and benign traffic. MLPNN offers quick convergence and excellent classification accuracy when applied following feature selection (e.g., CIBIR + AMPSI).Since MLPNN cannot model temporal dependencies on its own, it is used in conjunction with the LSTM in the proposed system to conduct deep nonlinear classification on the temporal information that the LSTM layer has learned.

Each neuron computes:

$$y = \sigma(wx + b)$$

Evaluation Parameters

Accuracy (%)

The percentage of accurate predictions the model makes out of all forecasts is known as accuracy. For classification jobs with balanced classes, accuracy is straightforward and frequently utilized. However, accuracy can be deceptive for unbalanced datasets (such as those used to diagnose rare diseases).

F1-Score (%)

The F1-score provides a balance between precision and recall by taking the harmonic mean of both. When you are concerned about both false positives and false negatives, it can be helpful. For datasets that are unbalanced and contain rare classes, the F1-score is recommended. Models with distorted recall or precision are penalized.

Time Complexity (ms)

Time complexity, which is typically expressed in milliseconds (ms) per prediction or each batch, is the amount of computational time a model requires to create a prediction or to train.For real-time applications like self-driving cars or live video processing, time complexity is essential. Faster forecasts are the result of reduced time complexity.

V.COMPARISON OF EXISTING MODEL

According to experimental data, the suggested framework performs better than current DRL, GAN, CNN, and RNN-based techniques with minimal computational overhead in terms of accuracy, F1-score, and time complexity when compared to LSTM

Here is the comparison of proposed methods with the existing methods:

Table 2. Comparison o with the Existing Methods

Method	Feature Selection Technique	Learning Model	Security Mechanism	Learning Style
DRL	Basic Statistical Filtering	Deep Reinforcement Learning	None / Basic Encryption	Centralized
GAN	Manual / Heuristic Selection	GAN + LSTM Auto encoder	None / Basic Encryption	Centralized
CNN	PCA / KPCA	Convolution Neural Network	Block chain (Partial)	Centralized
RNN	Correlation-based Selection	Recurrent Neural Network	None	Centralized
LSTM	Recursive Feature Elimination (RFE)	Long Short-Term Memory (LSTM) Network	Federated Learning + Blockchain	Decentralized

VI.CONCLUSION

According to a review of the literature, the majority of cyber security frameworks for IoT and healthcare settings now in use rely on centralized AI models, which presents significant issues with regard to data privacy, regulatory compliance, and susceptibility to significant breaches. Despite their high detection accuracy, deep learning models like CNNs, RNNs, and GANs are computationally demanding and ill-suited for deployment on edge devices with limited resources. Because it allows for collaborative model training without the need to share raw patient data, federated learning has become a potential option. Nevertheless, many FL-based systems still lack secure aggregation, trust management, and auditability.These holes are filled by block chain and medium-chain technologies, which offer safe routing, immutable records, and decentralized validation, although they frequently present latency and scalability issues. Moreover, generic statistical or PCA-based approaches are usually used for feature selection in intrusion detection systems that are currently in use, ignoring the behavioral impact and interdependencies of attack features. Although swarm intelligence and optimization techniques enhance performance, they are infrequently used in healthcare IoT situations in conjunction with block chain and federated learning. The suggested LSTM with federated Learning is intended to fill the gaps in the literature by providing an integrated framework that simultaneously guarantees privacy, trust, computational efficiency, and accurate temporal attack detection.

REFERENCES

1. Goffer, M. A., et al., “AI-Enhanced Cyber Threat Detection and Response: Advancing National Security in Critical Infrastructure,” *Journal of Posthumanism*, vol. 5, no. 3, pp. 1667–1689, 2025.
2. Virk, A., et al., “Digital Health Policy and Cybersecurity Regulations Regarding Artificial Intelligence (AI) Implementation in Healthcare,” *Cureus*, vol. 17, no. 3, 2025.
3. Gupta, S., Kamboj, S., and Bag, S., “Role of Risks in the Development of Responsible Artificial Intelligence in the Digital Healthcare Domain,” *Information Systems Frontiers*, vol. 25, no. 6, pp. 2257–2274, 2023.
4. Gabriel, O. T., *Data Privacy and Ethical Issues in Collecting Health Care Data Using Artificial Intelligence Among Health Workers*, M.S. Thesis, Center for Bioethics and Research, 2023.
5. Bashir, A. K., et al., “Federated Learning for the Healthcare Metaverse: Concepts, Applications, Challenges, and Future Directions,” *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21873–21891, 2023.
6. Singh, K., and Sevukamoorthy, L., “Blockchain and AI-Based Threat Detection for Enhanced Security in Financial Networks,” in *Proc. IEEE TEMSCON-ASPAC*, 2023, pp. 1–5.
7. Mansour, R. F., “Artificial Intelligence Based Optimization with Deep Learning Model for Blockchain-Enabled Intrusion Detection in CPS Environment,” *Scientific Reports*, vol. 12, no. 1, Art. no. 12937, 2022.
8. Karn, A. L., et al., “Applying the Defense Model to Strengthen Information Security with Artificial Intelligence in Computer Networks of the Financial Services Sector,” *Scientific Reports*, vol. 15, no. 1, Art. no. 30292, 2025.
9. Bhambri, P., and Starostka-Patyk, M., “Integrating AI with Blockchain for Decentralized Security and Threat Prevention,” in *Handbook of AI-Driven Threat Detection and Prevention*, CRC Press, 2025, pp. 353–370.
10. Awotunde, J. B., et al., “Privacy and Security Enhancement of Smart Cities Using Hybrid Deep Learning-Enabled Blockchain,” *Scalable Computing: Practice and Experience*, vol. 24, no. 3, pp. 561–584, 2023.
11. Konstantinos P. Ferentinos.,”Deep learning models for plant disease detection and diagnosis” https://doi.org/10.1016/j.compag.2018.01.009
12. G.L. Grinblat et al. Deep learning for plant identification using vein morphological patterns Comput. Electron. Agric. (2016)
13. G. Singh and D. s. Chabra, "Plant Disease Detection using Convolution Neural Network Approach," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 352-355, doi: 10.1109/ICICT57646.2023.10134217.
14. Yang Lu et.al.,Identification of rice diseases using deep convolutional neural networks Neurocomputing 6 December 2017, Agricultural and Food Sciences, Computer Science.
15. Too EC, Yujian L, Njuki S, Yingchun L. A comparative study of fine-tuning deep learning models for plant disease identification. Computers and Electronics in Agriculture. 2019 Jun 1;161:272-279.
16. Moustafa, N., Slay, J“UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems”*Military Communications and Information Systems Conference*, 2015.

17. Shone, N., et al.“A Deep Learning Approach to Network Intrusion Detection.”*IEEE Transactions on Emerging Topics in Computational Intelligence*, 2018.
18. Doshi, R., Apthorpe, N., Feamster, N.“Machine Learning DDoS Detection for Consumer Internet of Things Devices.”*IEEE Security and Privacy Workshops*, 2018.
19. Kim, G., Lee, S., Kim, S.“A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection.”*Expert Systems with Applications*, vol. 41, 2014.
20. Yin, C., Zhu, Y., Fei, J., He, X.“A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks.”*IEEE Access*, vol. 5, pp. 21954–21961, 2017.
21. Hochreiter, S., Schmidhuber, J.“Long Short-Term Memory.”*Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
22. *Neil Sahota, “What Is Deep Learning? Definition and Techniques [With Examples],”* LinkedIn, Jan 17, 2023 visual summary of deep learning models.