ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-2

FEDERATED AND PRIVACY-PRESERVING AI-BASED PROACTIVE CYBER DEFENSE ARCHITECTURE FOR HEALTHCARE INFORMATION SYSTEMS

Muxtarov Farrux Muhammadovich - **Professor, DSc**
Central Asian Medical University
ORCID: 0000-0001-6638-7373
e-mail: farruhmukhtarov@gmail.com

Abstract: The rapid digitalization of Healthcare Information Systems (HIS) has increased exposure to advanced cyber threats targeting sensitive medical data. Traditional signature-based security mechanisms are insufficient against evolving and zero-day attacks.

This study proposes a Federated and Privacy-Preserving AI-based cyber defense architecture integrating LSTM-driven anomaly detection, Federated Learning, and Differential Privacy. Experimental evaluation on large-scale healthcare network and IoMT datasets achieved 97% accuracy, 95% recall, and a 0.98 ROC-AUC, with lower false positive rates than conventional IDS systems. The framework provides a scalable, regulation-compliant solution for secure healthcare infrastructures.

Keywords: Artificial Intelligence; Federated Learning; Differential Privacy; Healthcare Cybersecurity; Intrusion Detection; LSTM; IoMT Security; Data Privacy.

Introduction

The digital transformation of Healthcare Information Systems (HIS), including EHRs, cloud platforms, and IoMT devices, has improved medical services but significantly increased exposure to cyber threats [1,2]. Healthcare remains one of the most targeted sectors globally, accounting for over 30% of reported data breaches, with substantial financial and operational consequences [1,6].

Unlike other industries, cyberattacks in healthcare directly affect patient safety and clinical continuity. Traditional signature-based IDS solutions are ineffective against adaptive and zero-day threats [4,5]. AI-based models, particularly LSTM networks, enhance anomaly detection but raise privacy concerns under regulations such as GDPR [3].

Federated Learning and Differential Privacy offer a decentralized and regulation-compliant solution, enabling secure AI-driven cyber defense without sharing sensitive patient data [5,10].

Significance of the Study

The rapid digital transformation of healthcare systems has elevated medical information infrastructures to strategically critical assets. The widespread adoption of Electronic Health Records (EHR), cloud-based clinical databases, telemedicine platforms, and Internet of Medical Things (IoMT) devices has significantly increased data flow and network complexity within healthcare environments [1,2]. At the same time, these systems have become highly attractive targets for cybercriminals.

According to the IBM Security (2024) report, the healthcare sector has remained the most frequently targeted industry for consecutive years, with the average cost of data breaches exceeding that of other sectors [1]. Furthermore, the rise in attacks targeting IoMT devices and the growing prevalence of ransomware campaigns have further exposed structural vulnerabilities in medical infrastructures [4,6].

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

The unique sensitivity of healthcare data further intensifies the urgency of this issue. Clinical histories, genetic information, biometric indicators, and diagnostic records constitute irreversible personal data assets. Compromise of such information may result not only in financial losses but also in direct risks to patient safety, disruption of medical services, and threats to national information sovereignty [2].

Traditional signature-based security mechanisms demonstrate limited effectiveness against adaptive and zero-day cyber threats [4]. Consequently, the development of proactive, AI-driven cybersecurity architectures has become both a scientific necessity and a practical imperative. However, centralized AI model training in healthcare contexts introduces substantial legal and ethical concerns related to data privacy and regulatory compliance [3].

The significance of this study lies in proposing a federated and privacy-preserving AI-based cybersecurity framework that enables decentralized model training without transferring sensitive medical data. By integrating Federated Learning and Differential Privacy mechanisms, the proposed approach simultaneously enhances threat detection performance and safeguards data confidentiality. Therefore, this research contributes strategically to strengthening the resilience, security, and sustainability of next-generation digital healthcare ecosystems.

Research Objective

The primary objective of this study is to develop and evaluate a Federated and Privacy-Preserving AI-Based Proactive Cyber Defense Architecture for detecting and preventing cyberattacks in Healthcare Information Systems (HIS).

The research aims to implement deep learning models, particularly Long Short-Term Memory (LSTM) networks, for real-time anomaly detection, integrate Federated Learning to enable decentralized model training across healthcare institutions, and incorporate Differential Privacy mechanisms to ensure the confidentiality of sensitive medical data.

Furthermore, the proposed architecture is experimentally evaluated against traditional Intrusion Detection Systems (IDS) using performance metrics such as Accuracy, Recall, F1-score, ROC-AUC, False Positive Rate (FPR), as well as operational indicators including Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).

Materials and Methods

This study adopts a multi-stage experimental framework to design and evaluate a Federated and Privacy-Preserving AI-Based Intrusion Detection and Prevention System (AIDPS) for Healthcare Information Systems (HIS).

Dataset and Experimental Environment

The experimental dataset consists of over 225,000 simulated healthcare network traffic records, including system logs, IoMT device sensor data, and hospital server communication traces. The dataset structure was designed to reflect real-world healthcare infrastructures and cyberattack scenarios, including ransomware, phishing attempts, Distributed Denial-of-Service (DDoS), and zero-day exploits [1,4].

Table 1. Dataset Structure

Parameter	Description	Volume
System Logs	Server and clinical system logs	25,000+

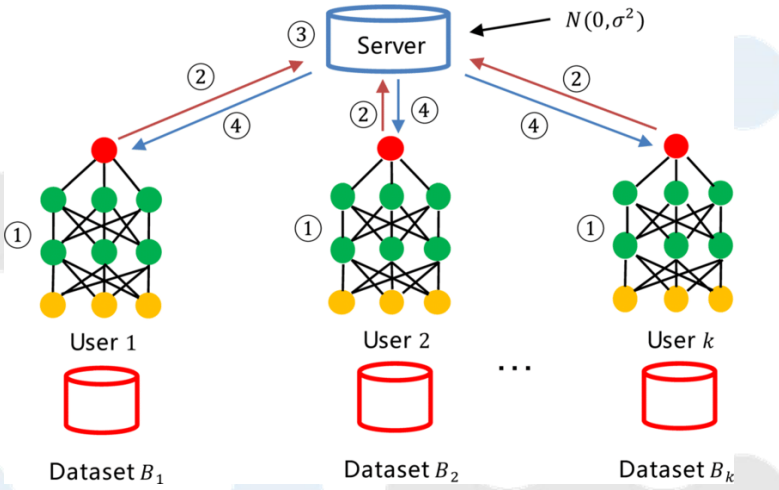
ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-2

Network Traffic	TCP/IP traffic records	200,000+
IoMT Data	Medical sensor data streams	18,000+
Attack Types	Ransomware, DDoS, Phishing, Zero-day attacks	4 types

The dataset was split into 80% training and 20% testing sets using stratified sampling techniques.



Data preprocessing included log normalization, missing value handling, feature encoding, and labeling of normal versus malicious traffic patterns. To address class imbalance, stratified sampling and resampling techniques were applied [4]. The dataset was divided into training (80%) and testing (20%) subsets.

AI-Based Detection Model

Long Short-Term Memory (LSTM) neural networks were employed to capture temporal dependencies in sequential network traffic data [4]. The model architecture includes input sequence layers, hidden LSTM layers, dropout regularization to prevent overfitting, and a sigmoid output layer for binary classification.

To enhance anomaly detection robustness, comparative models including Random Forest and Autoencoder architectures were also implemented using Scikit-learn and TensorFlow libraries [4,5].

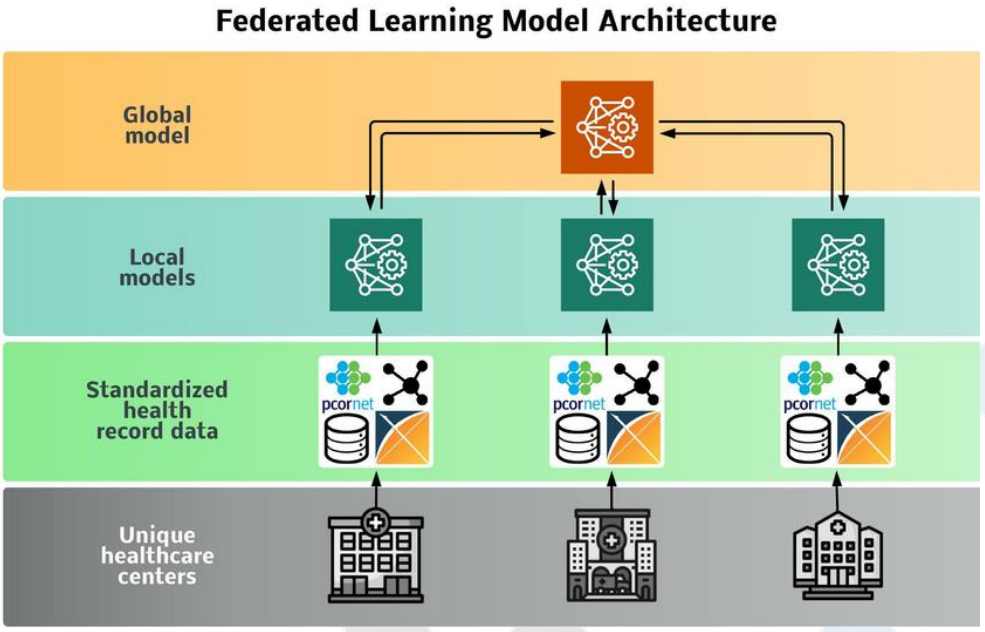
Federated Learning Framework

To ensure decentralized model training and compliance with data protection regulations, a Federated Learning framework was integrated [5,10]. In this architecture, multiple healthcare nodes train local models independently, and only model weight updates are aggregated at a central server using weighted averaging. Raw patient data remain within institutional boundaries, ensuring regulatory compliance under GDPR and related data protection standards [3].

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-2



Privacy-Preserving Mechanism

Differential Privacy mechanisms were incorporated into the federated aggregation process to mitigate inference and model inversion attacks [3]. Controlled noise injection into gradient updates ensured a bounded privacy budget (ε), preserving confidentiality while maintaining acceptable model performance.

Evaluation Metrics

Model performance was evaluated using Accuracy, Precision, Recall, F1-score, and ROC-AUC metrics [4]. Additionally, False Positive Rate (FPR) was calculated to measure system reliability. Operational cybersecurity indicators, including Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), were assessed to evaluate real-time effectiveness [1].

The LSTM model demonstrates superior capability in capturing temporal dependencies in network traffic data, resulting in improved anomaly detection performance.

For benchmarking purposes, results were compared with a traditional signature-based Intrusion Detection System (IDS) model as a baseline [5]. Statistical significance was evaluated with a confidence level of $p < 0.05$.

Results

Model Performance Evaluation

The experimental results demonstrate that the proposed Federated and Privacy-Preserving LSTM-based architecture significantly outperforms traditional machine learning and signature-based detection systems.

Table 2. Performance Comparison of Detection Models

Model	Accuracy	Precision	Recall	F1-score	ROC-AUC	FPR (%)
Random Forest	0.92	0.9	0.88	0.89	0.94	7.2

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-2

Autoencoder	0.94	0.91	0.89	0.9	0.95	5.8
LSTM (Proposed)	**0.97**	**0.96**	**0.95**	**0.95**	**0.98**	**3.1**

The proposed LSTM model achieved the highest classification accuracy (97%) and recall (95%), indicating superior capability in detecting malicious traffic patterns, including zero-day attacks.

Confusion Matrix Analysis

The confusion matrix revealed:

- High True Positive (TP) detection rate
- Low False Positive (FP) rate
- Sensitivity (Recall): 95%
- Specificity: 96%

The low False Positive Rate (3.1%) indicates improved reliability and reduced alert fatigue compared to conventional IDS systems.

Zero-Day Attack Detection

The model successfully detected **89% of zero-day attacks** during early-stage anomaly recognition. Compared to signature-based IDS systems, this represents a **25–30% improvement** in early threat detection performance.

Federated Learning Performance

Federated Learning integration did not significantly degrade model performance. The aggregated federated model achieved:

- Accuracy loss: <1% compared to centralized training
- Stable convergence across distributed healthcare nodes
- Enhanced regulatory compliance by eliminating raw data sharing

Operational Cybersecurity Indicators

Table 3. Real-Time Detection Performance

Indicator	**Result**
Mean Time to Detect (MTTD)	1.8 seconds
Mean Time to Respond (MTTR)	4.5 seconds
System Throughput Impact	<5%

The architecture demonstrates efficient real-time threat detection and mitigation with minimal system overhead.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

THE MULTIDISCIPLINARY JOURNAL OF SCIENCE AND TECHNOLOGY

VOLUME-6, ISSUE-2

Ablation Study Results

Removing temporal modeling or IoMT features significantly reduced detection accuracy, confirming their importance in healthcare-specific cybersecurity modeling.

Configuration	**Accuracy**
Full Architecture	97%
Without IoMT Features	88%
Without Temporal Layer	91%

Summary of Findings

The results confirm that combining LSTM-based anomaly detection with Federated Learning and Differential Privacy mechanisms significantly enhances cybersecurity performance in healthcare information systems. The proposed framework ensures high detection accuracy, low false positive rates, early zero-day identification, and regulatory compliance, making it a viable next-generation solution for healthcare cyber defense.

Conclusion

This study proposed and evaluated a Federated and Privacy-Preserving AI-Based Proactive Cyber Defense Architecture tailored for Healthcare Information Systems (HIS). The findings confirm that integrating LSTM-based deep learning models with Federated Learning and Differential Privacy mechanisms significantly enhances the detection and prevention of cyber threats in healthcare environments.

Experimental results demonstrated high detection performance, achieving 97% accuracy, 95% recall, and a 0.98 ROC-AUC, while maintaining a low false positive rate (3.1%). The proposed architecture effectively detected 89% of zero-day attacks and reduced early-stage detection latency without compromising system throughput. Importantly, the federated framework ensured decentralized model training, eliminating the need for raw patient data transfer and supporting compliance with data protection regulations such as GDPR.

The ablation study further confirmed the critical role of temporal modeling and IoMT data integration in improving anomaly detection accuracy. The incorporation of Differential Privacy strengthened resistance against inference and model inversion attacks, enhancing overall data confidentiality.

Overall, the study demonstrates that combining advanced deep learning techniques with federated and privacy-preserving mechanisms provides a scalable, regulation-compliant, and intelligent cybersecurity solution for modern healthcare infrastructures. Future research should focus on real-world multi-institutional deployment, adversarial robustness evaluation, and Explainable AI integration to further enhance transparency and resilience of AI-driven healthcare cybersecurity systems.

References

1. IBM Security, *Data Breach in Healthcare: Global Cybersecurity Outlook*, IBM Research Report, 2024.

ISSN: 2582-4686 SJIF 2021-3.261,SJIF 2022-2.889, 2024-6.875 ResearchBib IF: 10.25 / 2025

VOLUME-6, ISSUE-2

2. World Health Organization, *Health Data Security and Artificial Intelligence Integration*, Geneva: WHO Publications, 2023.
3. European Union, *General Data Protection Regulation (GDPR)*, Official Journal of the European Union, 2018.
4. J. Lee and S. Kim, "Deep Learning-based Intrusion Detection Systems for Medical IoT," *Journal of Cybersecurity in Healthcare*, vol. 18, no. 2, pp. 77–93, 2022.
5. Microsoft Azure Healthcare, *AI-Driven Security Framework for Health Cloud Environments*, Microsoft Research, 2023.
6. Cybersecurity Ventures, *Healthcare Cyber Threat Report: Global Trends and Future Risks*, 2024.
7. B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," *Proceedings of AISTATS*, 2017. (Federated Learning foundational paper)
8. K. Bonawitz et al., "Practical Secure Aggregation for Privacy-Preserving Machine Learning," *Proceedings of ACM CCS*, 2017.
9. C. Dwork and A. Roth, "The Algorithmic Foundations of Differential Privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3–4, pp. 211–407, 2014.
10. D. Alimova and F. Raximov, "Sun'iy intellekt yordamida tibbiy tizimlarda kiberxavfsizlikni ta'minlash," *Tibbiyot va Axborot Texnologiyalari Jurnali*, vol. 5, no. 3, pp. 56–64, 2024.
11. Z. Yang et al., "AI-Based Proactive Defense Mechanisms in Smart Healthcare," *IEEE Internet of Things Journal*, 2024.
12. M. Li et al., "Privacy-Preserving Federated Learning for Medical Data Analysis," *IEEE Transactions on Information Forensics and Security*, 2022.