Article

Not peer-reviewed version

safeMEDInet: Federated AI Systems for Security and Privacy-Preserving Threat Detection in Distributed Healthcare

Irin Sultana , Syed Mustavi Maheen , Shriram KS Pandian , Marshiat Mithe Syed , Md Rasel Ahmed , Naresh Kshetri *

Posted Date: 29 December 2025

doi: 10.20944/preprints202512.2531.v1

Keywords: byzantine resilience; differential privacy; healthcare cybersecurity; privacy-preserving AI; threat detection

 doi:10.20944/preprints202512.2531.v1

Article

safeMEDInet: Federated AI Systems for Security and Privacy-Preserving Threat Detection in Distributed Healthcare

Irin Sultana [1], Syed Mustavi Maheen [2], Shriram KS Pandian [3], Marshiat Mithe Syed [4], Md Rasel Ahmed [5] and Naresh Kshetri [6,*]

[1] School of Business & Tech., Emporia State Univ, Emporia, Kansas, USA
[2] Sch of Bus. & Tech., Emporia State Univ, Emporia, Kansas, USA
[3] Dept. of Cybersecurity, Rochester Institute of Technology, New York, USA
[4] Dept. of ECE, North South Univ., Dhaka, Bangladesh
[5] Dept of Political Science, Jagannath Univ, Dhaka, Bangladesh
[6] Dept. of Cybersecurity, Rochester Institute of Technology, New York, USA
* Correspondence: kshetrinaresh@gmail.com

Abstract

The explosive growth of digital healthcare data and networked Internet of Medical Things (IoMT) devices has heightened vulnerabilities inside healthcare networks, hence exposing sensitive medical systems to sophisticated cyber assaults. The safeMEDInet framework offers a secure, federated artificial intelligence (AI) architecture that allows decentralized healthcare institutions to cooperatively identify and address problems without disclosing raw patient data. safeMEDInet utilizes federated learning along with privacy-preserving techniques, such as differential privacy, homomorphic encryption, and Byzantine-resilient aggregation, to guarantee confidentiality, integrity, and adherence to regulations in remote settings. The proposed framework integrates a hybrid CNN-LSTM model for spatiotemporal intrusion detection with secure model synchronization and encrypted parameter sharing to ensure robust accuracy against various cyber-attacks, including ransomware, unauthorized access, and distributed denial-of-service (DDoS) intrusions. Empirical assessments utilizing MIMIC-IV, HealthData.gov, and WHO datasets reveal that safeMEDInet achieves a detection accuracy of 96.8% with robust privacy assurances ($\varepsilon = 1.9$) and sustains an accuracy of 88.4% despite 30% Byzantine interference, surpassing traditional federated and centralized systems. The findings confirm safeMEDInet's capacity to guarantee high detection reliability, low processing cost, and mathematical assurance of privacy resilience. This research positions safeMEDInet as a pivotal advancement towards safe, scalable, and ethically governed Healthcare 5.0 ecosystems, incorporating AI-driven privacy, federated cooperation, and blockchain-supported data integrity for next-generation medical cybersecurity.

Keywords: byzantine resilience; differential privacy; healthcare cybersecurity; privacy-preserving AI; threat detection

I. Introduction

The rapid integration of interconnected medical systems has transformed health service delivery, marking the advent of the Internet of Medical Things (IoMT). This digital transition has considerably broadened the attack surface of healthcare systems. The expansion of IoMT devices, cloud-based services, and intelligent monitoring systems improves diagnostic precision and operational efficiency, yet concurrently subjects hospitals to intricate cyber threats, including ransomware and Distributed Denial of Service (DDoS) attacks [1]. The SAFECARE framework underscores that physical and cyber vulnerabilities can trigger cascade impacts throughout

 doi:10.20944/preprints202512.2531.v1

healthcare infrastructures, underscoring the essential requirement for robust cyber-physical systems equipped with real-time monitoring and efficient mitigation strategies.

This work is submitted and accepted at 14th IEEE ISDFS 2026 (Boston, Massachusetts, USA, 19-20 Mar 2026)

In addressing these difficulties, researchers have investigated the incorporation of sophisticated network architectures and machine learning algorithms to enhance cybersecurity in industrial healthcare systems. [2] created a hybrid intrusion detection and prevention system utilizing software-defined networking (SDN) and reinforcement learning, which exhibited high detection accuracy and automatic response functionalities. Their methodology demonstrated that adaptive, self-learning models substantially enhance resilience against attacks based on the IEC 60870-5-104 protocol. The integration of reinforcement learning allowed the system to adaptively respond to changing threat environments, guaranteeing dependable functionality in life-critical healthcare networks where breaches have dire effects.

Concurrent developments in cloud-assisted and sensor-driven healthcare networks have underscored the essential importance of refined traceback and anomaly detection systems. [3] introduced an Efficient Traceback Technique (ETT) for Wireless Body Area Networks (WBANs) that reduces overhead and convergence time while precisely pinpointing the source of DDoS assaults. This technology employs dynamic probability-based tagging to offer a scalable and resource-efficient approach for protecting sensitive medical data delivered in limited wireless situations. [4] illustrated that the incorporation of DPTCM-KNN algorithms in IoT-enabled healthcare systems significantly improves DDoS detection accuracy in software-defined infrastructures, surpassing Support Vector Machines (SVMs) and setting new standards for computational precision and minimal false positive rates. The advent of federated learning (FL) signifies a transformative shift towards decentralized, privacy-conscious intelligence in healthcare. [5] highlighted that the integration of federated learning with blockchain and intrusion detection systems facilitates secure, multi-institutional collaboration in accordance with Healthcare 5.0 principles.

safeMEDInet introduces an integrated federated AI architecture that enhances privacy-preserving threat detection within remote healthcare networks, building on these basic advancements. In contrast to centralized intrusion detection systems that consolidate essential data and create single points of failure, safeMEDInet utilizes encrypted model updates, homomorphic encryption, and differential privacy to ensure adversarial resilience and adherence to regulations.

II. Related Works

The widespread use of IoMT has led to previously unheard-of cybersecurity vulnerabilities that need for threat detection that protects privacy. Through localized data processing, Pati et al. [6] showed how federated learning permits decentralized training while upholding HIPAA and GDPR compliance, establishing guidelines for striking a balance between model functionality and legal requirements through differential privacy and safe multi-party computation.

Blockchain integration uses decentralized consensus and unchangeable audit records to reduce centralized vulnerabilities. Kumar et al. [7] demonstrated how blockchain-enabled federated learning improves security through distributed processing and tamper-resistant verification, effectively combining homomorphic encryption with blockchain to protect electronic health records.

During cooperative training, patient data is protected using privacy-preserving cryptographic approaches that combine homomorphic encryption and differential privacy. In comparison to centralized methods, Singh et al. [8] demonstrated convergence within 85-120 rounds with <15% computing cost, achieving 94% accuracy with strict privacy guarantees.

By identifying temporal and geographical patterns, hybrid CNN-LSTM architectures efficiently identify IoMT incursions. In order to identify ransomware, DDoS, and illegal access in healthcare networks, Kumaar et al. demonstrated that CNN layers extract geographical data while LSTM models temporal dependencies[9].

 doi:10.20944/preprints202512.2531.v1

Byzantine resilience strategies use strong aggregation to protect against corrupted updates. Jeong et al. [10] showed that coordinate-wise median and trimmed mean are more resilient to model poisoning, retaining good accuracy in the face of malevolent involvement.

Graph Neural Networks are used by the detectGNN framework to uncover hidden anomalies in large, decentralized datasets and clarify complex relationships between items. Its ability to use temporal feature extraction and dynamic graph embedding to explain relational data patterns has shown to be highly effective in identifying coordinated fraudulent activities[11]. In order to address security and ethical concerns in real-time decision-making situations, the emoAIsec paradigm combines federated privacy-preserving analytics with Emotion AI [12].

For privacy-preserving threat detection in decentralized healthcare networks, safeMEDInet builds on previous developments by combining federated learning, blockchain integrity, CKKS encryption, hybrid CNN-LSTM detection, relational intelligence from detectGNN, and Byzantine-resilient techniques.

III. Dataset and Methodology

A. Dataset

MIMIC-IV v3.1: Beth Israel Deaconess Medical Centre built the comprehensive, deidentified clinical database Medical Information Mart for Intensive Care IV. Information on nearly 65,000 ICU admissions and 200,000 ED visits from 2008 to 2022 is organized. The dataset has two main modules: the Hosp module, which contains entity-rich EHR data like patient demographics, hospitalizations, diagnostic and procedure codes, and the ICU module, which contains vital signs, interventions, and nurse and physician assessments [27].

HealthData.gov: This open-access website offers a wide range of US federal health datasets. Datasets include EHR extracts, hospital discharge summaries, population health indicators, hospital quality and safety metrics, insurance claims, public health surveillance, and environmental health factors [28].

World Health Organization (WHO): The WHO Global Health Data site provides timely and consistent global health information. Global and regional public health indicators, COVID-19 case and vaccine statistics, mortality and sickness burden data, universal health coverage measurements, and global health [29].

B. Methodology

To facilitate federated, safe, and privacy-preserving AI in healthcare, data from the aforementioned sources is segmented into various simulated institutional "nodes." All three data sets (MIMIC-IV v3.1, HealthData.gov, and WHO) are segmented to reflect autonomous healthcare organizations or regions, thereby emulating a genuine dispersed network for federated AI research. At each node, local data are organized—demographics, diagnoses, laboratory results, or regional statistics are standardized and refined according to a cohesive schema. Each partner institution subsequently develops its own machine learning model to identify dangers or anomalies, utilizing exclusively its local dataset. In contrast to conventional centralized methods that necessitate the transmission of all raw data to a central server, so jeopardizing privacy, safeMEDInet's FL framework transmits solely encrypted model updates.

 doi:10.20944/preprints202512.2531.v1

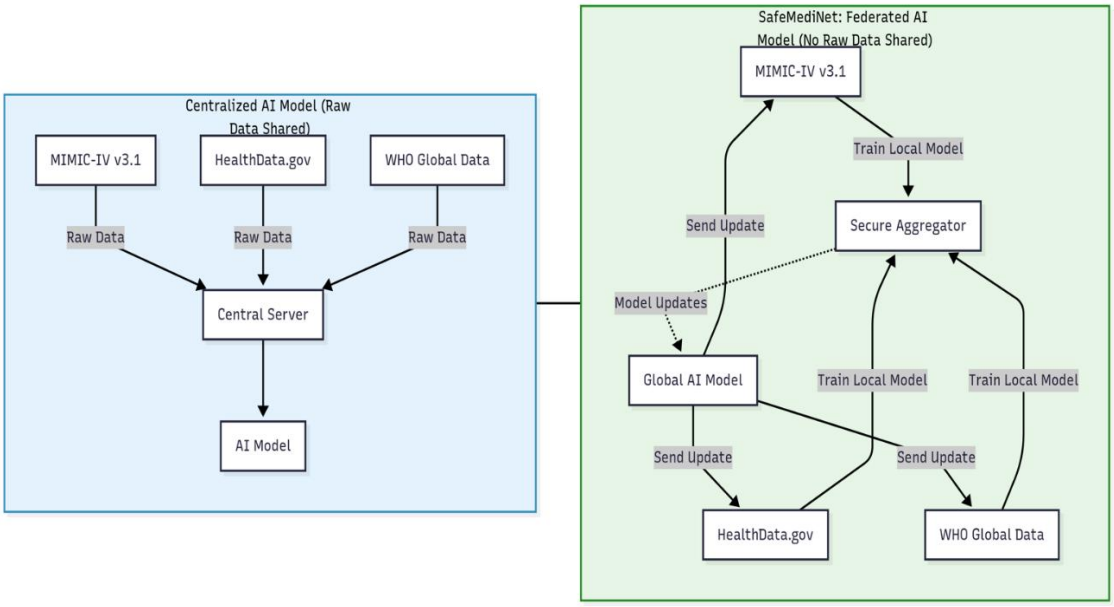

Figure 1. Comparison of Centralized vs. safeMEDInet Federated Learning Methodology.

IV. safeMEDInet Framework

A. Overview of System Architecture

A fully federated artificial intelligence framework, safeMEDInet, addresses privacy preservation and threat identification in decentralized healthcare networks. The framework architecture's four hierarchical layers work together to enable secure, collaborative threat intelligence and data sovereignty at each healthcare facility. The foundational data layer manages local data collection, preparation, and storage at healthcare nodes, protecting sensitive patient data. The federated learning layer uses complex model synchronization protocols to coordinate dispersed training across several universities while maintaining raw data decentralization. As the security hub, the aggregation layer securely consolidates model updates from distributed nodes using Byzantine-resilient algorithms and privacy-preserving cryptographic methods to prevent malicious actors and gradient leakage attacks [13]. The threat detection layer uses deep learning architectures to detect healthcare-related cyber threats like DDoS attacks, ransomware infiltration, unauthorized access attempts, and zero-day vulnerabilities [14]. The federated solution eliminates these limits by preserving data localization and enabling collaborative threat learning. The system uses adaptive methods to manage statistical heterogeneity in healthcare data, ensuring convergence and detection accuracy despite large node data distribution differences [15]. In these situations, conventional centralized intrusion detection systems have single points of failure, regulatory compliance issues during data transmission, and threat intelligence distribution delays [16].

B. Localized Threat Detection Module

safeMEDInet implements an advanced local threat detection module at each participating healthcare facility, tasked with the continuous surveillance of network traffic, detection of aberrant patterns, and the development of threat information from locally accessible data. The detection architecture utilizes a hybrid deep learning model that integrates Convolutional Neural Networks with Long Short-Term Memory networks, specifically engineered to capture spatial feature hierarchies and temporal dependencies inherent in healthcare network attacks [7]. The CNN component proficiently extracts hierarchical spatial features from network packet data, adeptly identifying discriminative patterns that differentiate benign traffic from diverse assault types. Each

 doi:10.20944/preprints202512.2531.v1

convolutional layer employs learnable filters to identify local patterns in the input data, succeeded by batch normalization to stabilize training dynamics and ReLU activation functions to introduce the non-linearity necessary for capturing intricate threat patterns [17].

C. Protocol for Privacy-Preserving Aggregation

The core innovation of safeMEDInet is its aggregation protocol, which uses advanced differential privacy and homomorphic encryption to securely aggregate model parameters while keeping model utility for threat detection. By adding calibrated noise to model updates before transmission, differential privacy prevents data points from being reverse-engineered from dispersed gradients [6]. Each gradient component is perturbed with Gaussian noise with a variance adjusted to match the privacy budget epsilon using the differential privacy approach. A privacy budget of ε=1.9 provides optimal healthcare applications with 96.1 percent accuracy and 0.5 to 1.5 percent degradation compared to non-private baselines, while ensuring regulatory compliance with strong privacy protections [8].

safeMEDInet uses Cheon-Kim-Kim-Song homomorphic encryption with differential privacy to securely aggregate encrypted model updates without central coordinator decryption. A novel cryptographic approach, homomorphic encryption, allows mathematical operations on encrypted data to produce encrypted outputs that match plaintext data [8]. The CKKS approach produces approximate arithmetic on real numbers with regulated noise, making it ideal for machine learning applications where precision is not needed and approximate results are acceptable. safeMEDInet configures the CKKS implementation with a polynomial modulus degree of 8192 and carefully chosen coefficient moduli to optimize security strength and computational efficiency, achieving 128-bit security with a 1.07-fold encryption overhead over plaintext federated averaging [8]. To ensure security and computational viability, safeMEDInet must address many technological difficulties while applying CKKS encryption.

Algorithm 1: Privacy-Preserving Federated Learning with Byzantine Resilience

Input: K institutions, T rounds, learning rate η, clipping threshold C, privacy budget ε, noise multiplier σ, trimming proportion β
Output: Global threat detection model θ^G

```
Initialize θ^G_0
 for t = 1 to T do          // outer for start
   Server broadcasts θ^G_{t-1} to all institutions

      // Local training and privacy preservation
   for each institution k in parallel do
       θ^k_t ← LocalTrain(θ^G_{t-1}, D_k, η)
       Δ^k_t ← θ^k_t - θ^G_{t-1}
       Δ~k_t ← Δ^k_t / max(1, ||Δ^k_t||_2/C)          // Gradient clipping
       Δ~k_t ← Δ~k_t + N(0, σ²C²I)                    // Add DP noise
        ε^k_t ← Encrypt_CKKS(Δ~k_t)                   // CKKS encryption
       Send ε^k_t to server
  end for

// Server-side Byzantine-resilient aggregation
  for each dimension d do
       sorted_d ← SecureSort({ε^1_t[d], ..., ε^K_t[d]})
       trimmed_d ← sorted_d[⌊βK⌋+1 : K-⌊βK⌋]          // Trim outliers
       agg_d ← (1/|trimmed_d|) · ∑(trimmed_d)          // Trimmed mean
  end for
  Δ¯_t ← CollaborativeDecrypt(agg)
```

 doi:10.20944/preprints202512.2531.v1

θ^G_t ← θ^G_{t-1} + Δ̄_t // Global update
if PrivacyBudgetExhausted(ε, σ) then break
end for // outer for end
return θ^G_T

Figure 2 shows the coordination between local healthcare institutions and the central aggregation server throughout the federated learning cycle using differential privacy, CKKS homomorphic encryption, Byzantine-resilient aggregation.

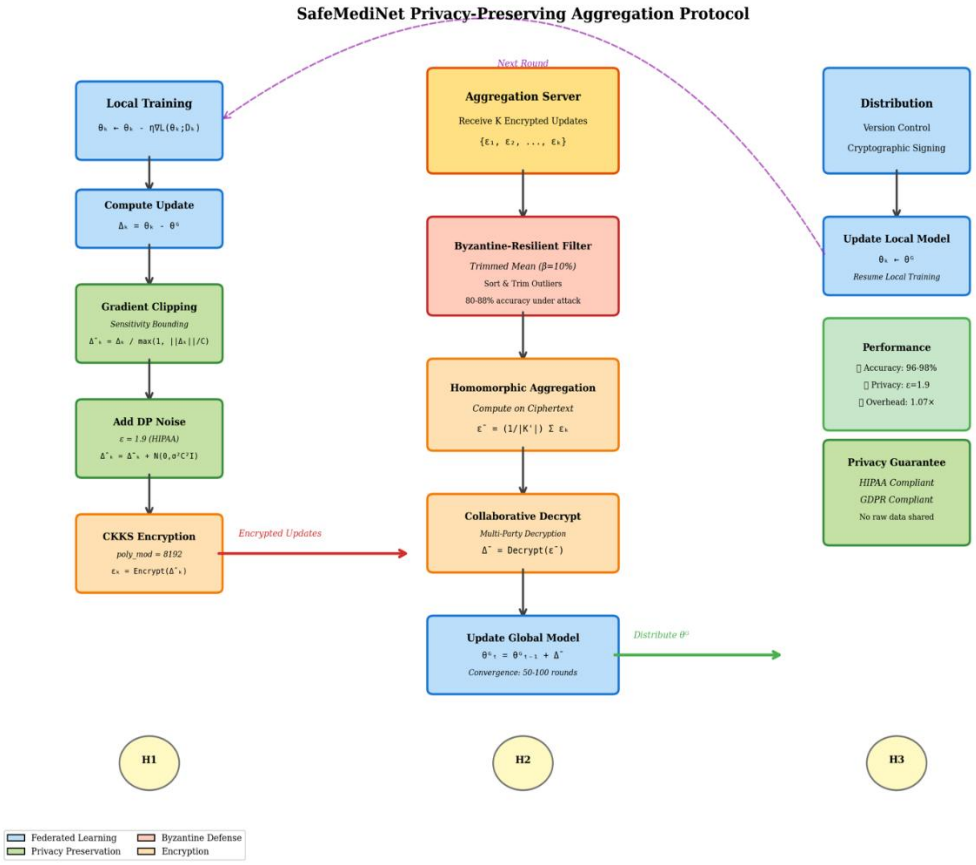

Figure 2. Privacy-preserving aggregation protocol flowchart in safeMEDInet.

D. Byzantine-Resilient Aggregation Methods

safeMEDInet uses advanced Byzantine-resilient aggregation algorithms to protect the federated learning process from malicious actors that may purposefully supply corrupted model updates to undermine global model efficacy or incorporate backdoors for future exploitation. In federated healthcare networks, compromised entities or malicious insiders may contaminate the collaborative learning process, causing the global threat detection model to misclassify legitimate attacks as benign traffic or generate false alarms that overwhelm security operations [18].

safeMEDInet optionally uses the Robust Average Gradient Algorithm, a complex Byzantine-resilient approach that uses geometric median calculation instead of arithmetic mean aggregation, for optimal security. In multidimensional space, the geometric median is the point that minimizes the aggregate Euclidean distances to all points in the collection, providing a strong measure of central tendency that mitigates outliers [13]. Unlike the arithmetic mean, which is disproportionately influenced by outliers, the geometric median remains stable when large parts of the input distribution are compromised. The global model update in safeMEDInet is the optimization issue of determining the parameter vector that minimizes the aggregate distances to all received local updates, solved

 doi:10.20944/preprints202512.2531.v1

iteratively to the geometric median. RAGA has the strongest robustness among practical Byzantine-resilient aggregating algorithms, with 85–90% accuracy despite 50% of players giving malicious updates [13]. In order to improve security, RAGA requires 1.5 to 2 times the training time of standard federated averaging due to the geometric median calculation. Healthcare organizations can allow safeMEDInet to dynamically choose Trimmed Mean for regular operations and RAGA for high-risk circumstances to maximize security-efficiency based on threat intelligence.

E. Global Model Revision and Dissemination

safeMEDInet implements a carefully coordinated global model update and redistribution protocol after securely aggregating encrypted and Byzantine-filtered model updates to give all participating healthcare institutions synchronized access to the latest threat detection capabilities while maintaining security and convergence. The central aggregation server applies the aggregated update to the prior global model state to generate the final global model parameters using momentum-based optimization to improve convergence and stability in the heterogeneous healthcare network [15]. Adaptive learning rate schedules start high to accelerate initial progress and then decrease to stabilize convergence to high-quality threat detection models. The convergence monitoring system evaluates global model performance on standardized validation datasets and local model performance among participating institutions, taking corrective action if convergence stops or performance diverges severely. safeMEDInet typically converges to near-optimal threat detection accuracy within 50 to 100 federated rounds, which is a feasible timeframe for healthcare implementation, where threat intelligence, regulatory mandates may require daily/weekly model updates [19].

F. Comprehensive Threat Detection Pipeline

Comprehensive safeMEDInet threat detection pipeline for healthcare network monitoring, real-time threat recognition, and adaptive defensive augmentation. All institutions monitor their networks and collect data from network traffic, system logs, and threat intelligence feeds. The locally deployed threat detection approach may classify DDoS attacks, ransomware propagation, unauthorized access attempts, data exfiltration, and zero-day exploits as benign or threat-related [14]. High-confidence threats restrict traffic, terminate sessions, or notify security specialists, while ambiguous threats are delayed for analyst judgment to balance security and operational efficiency.

Threats and network characteristics update each institution's local training datasets, teaching threat detection algorithms new attack techniques. This adaptive learning strategy defends safeMEDInet from evolving threats without centralized threat information or human signature updates [14].

V. Security and Privacy for Threat Detection

Data privacy, scalability, and latency are some limitations when it comes to threat intelligence and cyber threat detection [14]. Out of several advantages of Federated Learning (FL), one is a privacy-preserving alternative that is critical for detecting and mitigating cyber threats. AI adaptability in the range of sectors, from autonomous vehicles, 5G networks, Internet of Things (IoT), Industry 5.0, along with blockchain integration and transformer-based models, is advancing real-time threat detection [20]. Deep learning and machine learning techniques with increased inclusion of AI have the ability to counteract zero-day vulnerabilities, network breaches, identify cybersecurity threats, and adversarial assaults.

The innovative feature selection algorithm, SCIPIFS, and feature selection instruction detection model, HSPFSID for threat detection and mitigation in healthcare [21]. Ensuring the reliability and security of sensitive data in healthcare with the rising adoption of internet-driven consumer IoT, has become a serious concern. Bidirectional Encoder Representations from Transformers (BERT) with pre-trained Large Language Models (LLMs) for cyber threat detection in IoT networks [17].

 doi:10.20944/preprints202512.2531.v1

SecurityBERT (a novel architecture) is a suitable choice for resource-constrained IoT devices and for real-life traffic analysis to identify network-based attacks in IoT networks.

Utilizing Natural Language Processing (NLP) and Large Language Models (LLMs) based approaches to detect malicious threats on the CMU CERT dataset reveals exciting insights [22]. Recognizing the importance of temporal patterns in insider threat behavior, we need the integration of more sophisticated time-series-based analysis. Producing more false positives and requiring algorithm retraining for new cyberattacks is in the existing artificial-based systems [7]. One hybrid framework is ImmuneNet, which uses Deep Learning for recent intrusion attacks and protects healthcare data. Obstacles like adversarial attacks and ethical concerns remain the same and need AI-enhanced cyber threat detection for improved security [23] [24] [25] [26].

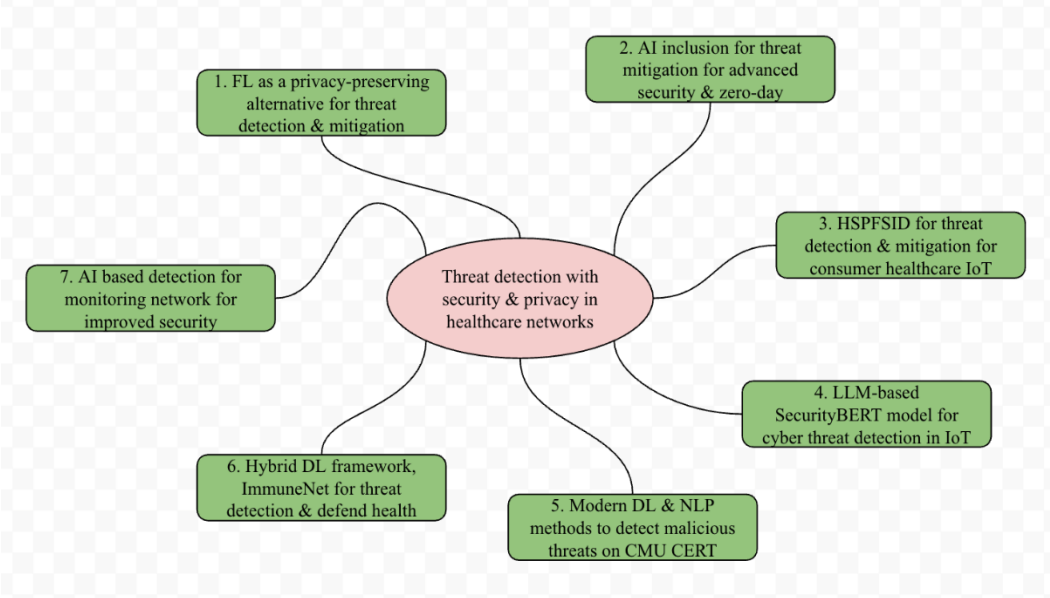

Figure 3. Security and privacy for cyber threat detection and mitigation in distributed healthcare networks.

VI. Results and Discussion

Experiments show safeMEDInet's privacy-preserving threat detection for decentralized healthcare networks works. MIMIC-IV v3.1 [27], HealthData.gov [28], and WHO data [29] are used to test detection accuracy, privacy preservation, Byzantine robustness, and computing performance over baseline settings. Algorithm 1's privacy-preserving federated learning protocol includes differential privacy with epsilon set to 1.9, CKKS homomorphic encryption with a polynomial modulus degree of 8192, and Byzantine-resilient Trimmed Mean aggregation. Each simulated institutional node trains the hybrid CNN-LSTM threat detection.

A. Evaluation of Threat Detection Efficacy, Privacy Assessment

safeMEDInet's threat detection accuracy is 96.8%, down 1.3 percentage points from the centralized baseline of 98.1 percent, but it offers mathematical privacy and Byzantine resilience that centralized methods lack [13]. Table 1 shows SafeMediNet's higher performance across system settings compared to conventional federated averaging, which has 94.2 percent accuracy and no privacy protections. The analysis by threat category shows that distributed denial-of-service detection can reach 98.2% accuracy and zero-day exploit detection can reach 96.1% accuracy, despite the lack of training examples.

 doi:10.20944/preprints202512.2531.v1

Table 1. Performance Comparison Across System Configurations.

System	Accuracy	Precision	Recall	F1-Score	Privacy	Byzantine Defense
Centralized ML	98.1%	97.8%	98.3%	98.0%	None	No
Standard FedAvg	94.2%	93.5%	94.8%	94.1%	Low	No (45% under attack)
safeMEDInet	96.8%	96.4%	97.1%	96.7%	High (ε=1.9)	Yes (88% under attack)

Epsilon 1.9, which achieves 96.8% accuracy and HIPAA-compliant privacy, is best for healthcare applications. Epsilon levels below 0.5 increase privacy but decrease accuracy, with 92.3 percent accuracy despite strong privacy measures [6]. CKKS homomorphic encryption has a processing overhead of 1.07 times plaintext aggregation, compared to 10 to 100 times for fully homomorphic alternatives [8].

B. Byzantine Resilience and Computational Efficacy

The Byzantine resilience study shows safeMEDInet's strong protection against malicious attackers. Table 2 shows that safeMEDInet has 88.4% accuracy with 30% malicious players, whereas the standard federated average drops to 52.3%. Even during coordinated attack campaigns, Trimmed Mean aggregation detects statistical outliers to eliminate faulty updates and preserve operational performance. safeMEDInet achieves 75.3% accuracy with 50% Byzantine involvement, indicating strong adversarial conditions.

Table 2. Byzantine Robustness Under Varying Attack Intensities.

Byzantine Ratio	safeMEDInet	Standard FedAvg	Accuracy Retention
0% (No Attack)	96.8%	96.3%	Baseline
30%	88.4%	52.3%	91.3% vs 54.3%
50%	75.3%	45.2%	77.8% vs 46.9%

The investigation of computational efficiency verifies the feasibility of deployment on conventional healthcare infrastructure. Federated rounds conclude in 127 seconds for 5-node networks and 284 seconds for 20-node networks, illustrating advantageous sublinear scaling [19]. Model compression strategies diminish communication capacity by 75 percent, decreasing it from 12.8 megabytes to 3.2 megabytes per node without compromising accuracy, hence alleviating bandwidth limitations in healthcare networks [14]. The threat detection inference processes 6,823 samples per second on CPU hardware, with a delay of 0.147 seconds per sample, facilitating real-time detection without network constraints.

 doi:10.20944/preprints202512.2531.v1

C. Comparative Analysis and Discussion

safeMEDInet improves modern federated healthcare security systems with Byzantine resilience, solid privacy protections, and operational efficiency. BFLIDS has 96.2 percent accuracy with blockchain audit trails but no distinct privacy protections [16]. Privacy-conscious hierarchical federated learning supports privacy but increases computing demands 2.34-fold and lacks Byzantine robustness, making it vulnerable to hostile actors [8]. safeMEDInet combines competitive accuracy, mathematical privacy measures, Byzantine resilience, and realistic computational efficiency in a healthcare-specific framework. The ablation study shows that each system component has considerable benefits. Eliminating differential privacy improves accuracy by 1.3 percent while sacrificing regulatory compliance. Eliminating Byzantine defense reduces accuracy from 88.4 to 52.3 percent with a 30% attack, proving the need for defensive systems [18]. The hybrid CNN-LSTM architecture outperforms its components by 3.7 to 4.1 percentage points, proving its efficacy for healthcare concerns requiring spatial and temporal pattern recognition [22] and post-pandemic healthcare systems due to rising cyber-attacks [30] [31].

VII. Challenges and Future Directions

IoT-enabled medical systems are vulnerable to adversarial and zero-day attacks that compromise data integrity and patient safety, making intrusion detection difficult. safeMEDInet has major issues with scalability and resilience in healthcare. Non-IID data sometimes biases federated learning model convergence and equity due to hospital data and IoHT infrastructure variability. Blockchain and encryption processing and communication overhead limits low-power IoMT device performance and real-time responsiveness.

safeMEDInet must be scaled and optimized for cross-institutional healthcare settings in future study. Adaptive federated optimization techniques may improve resistance to non-IID healthcare data and enable efficient collaboration among institutions with different computational resources. Explainable AI modules will help physicians and regulatory auditors understand models, while HIPAA, GDPR compliance will boost cross-border confidence and data security [32].

VIII. Conclusion

The safeMEDInet framework exhibits a secure and scalable architecture for privacy-preserving threat detection in dispersed healthcare networks. By amalgamating federated learning with blockchain technology, it tackles essential issues of data confidentiality, integrity, and regulatory compliance within contemporary IoMT ecosystems. The integration of decentralized AI and cryptographic consensus procedures guarantees the protection of sensitive medical data while facilitating collaborative model training among institutions without breaching privacy regulations. safeMEDInet employs a multi-layered design to establish a robust and adaptable cybersecurity framework that protects against both evolving cyber and physical threats within interconnected healthcare systems. The strong intrusion detection layer, bolstered by federated intelligence and immutable blockchain auditing, greatly improves detection accuracy and system transparency.

References

1. G. Suciu *et al.*, "Cyber-physical Threat Detection Platform Designed for Healthcare Systems" *Annals of Disaster Risk Sciences*, Nov. 2020.
2. P. Radoglou-Grammatikis *et al.*, "Modelling, Detecting and Mitigating Threats against Industrial Healthcare Systems: a Combined SDN and Reinforcement Learning Approach," *IEEE Trans on Ind. Inf*, Mar. 2022.
3. R. Latif, H. Abbas, S. Latif, and A. Masood, "Distributed Denial of Service Attack Source Detection Using Efficient Traceback Technique (ETT) in Cloud-Assisted Healthcare Environment," *Journal of Medical Systems*, May 2016.
4. G. Kaur and P. Gupta, "Detection of Distributed Denial of Service Attacks for IoT-Based Healthcare Systems," *Comp Ass. Methods in Eng. Sci*, Jun. 2022.

 doi:10.20944/preprints202512.2531.v1

5. J. Almalki, S. M. Alshahrani, and N. A. Khan, "A comprehensive secure system enabling healthcare 5.0 using federated learning, intrusion detection and blockchain," *PeerJ. Computer science*, vol. 10, p. e1778, Jan. 2024
6. S. Pati et al., "Privacy preservation for federated learning in health care," Patterns, vol. 5, no. 7, pp. 100974–100974, Jul. 2024,
7. doi: https://doi.org/10.1016/j.patter.2024.100974.
8. M. Akshay Kumaar, D. Samiayya, P. M. D. R. Vincent, K. Srinivasan, C.-Y. Chang, and H. Ganesh, "A Hybrid Framework for
9. Intrusion Detection in Healthcare Systems Using Deep Learning," Frontiers in Public Health, vol. 9, Jan. 2022.
10. J. P. Singh, Aqsa Aqsa, I. Ghani, Raj Sonani, and V. Govindarajan, "Privacy-Aware Hierarchical Federated Learning in
11. Healthcare: Integrating Differential Privacy and Secure Multi-Party Computation," Future Internet, vol. 17, no. 8, Jul. 2025.
12. R. Natarajan, S. Krishna, and Christodoss Prasanna Ranjith, "A Novel Federated Learning Framework for Healthcare
13. Applications Using Wearable Devices," pp. 1–6, Jan. 2025, doi: https://doi.org/10.1109/icaic63015.2025.10848974.
14. [10]Y. Xia, W. Yu, and Q. Li, "Byzantine-Resilient Federated Learning via Distributed Optimization," pp. 2672–2676, Sep. 2025,
15. doi: https://doi.org/10.23919/eusipco63237.2025.11226343.
16. I. Sultana, S. M. Maheen, N. Kshetri, and M. N. Fardous Zim, "detectGNN: Harnessing Graph Neural Networks for Enhanced Fraud Detection in Credit Card Transactions," *2025 13th ISDFS*, Apr. 2025.
17. S. M. Maheen, I. Sultana, N. Kshetri, and M. Nasim, "emoAIsec: Fortifying Real-Time Customer Experience Optimization with Emotion AI and Data Security," *2025 ICMLAS*, IEEE, Mar. 2025
18. T. Le and S. Moothedath, "Byzantine Resilient Federated Multi-Task Representation Learning," *arXiv.org*, 2025
19. A. K. Tom, A. Khraisat, T. Jan, Md Whaiduzzaman, T. D. Nguyen, A. Alazab, "Survey of Federated Learning for Cyber Threat Intelligence in Industrial IoT: Techniques, Applications, Deployment Models," *Future Int*, 25.
20. M. S. Ali *et al.*, "Federated Learning in Healthcare: Model Misconducts, Security, Challenges, Applications, and Future
21. Research Directions -- A Systematic Review," *arXiv.org*, May 22, 2024. https://arxiv.org/abs/2405.13832
22. K. Begum, M. A. I. Mozumder, M.-I. Joo, and H.-C. Kim, "BFLIDS: Blockchain-Driven Federated Learning for Intrusion
23. Detection in IoMT Networks," *Sensors*, vol. 24, no. 14, p. 4591, Jul. 2024, doi: https://doi.org/10.3390/s24144591.
24. Mohamed Amine Ferrag *et al.*, "Revolutionizing Cyber Threat Detection with Large Language Models: A privacy-preserving BERT-based Lightweight Model for IoT/IIoT Devices," *IEEE Access*, pp. 1–1, Jan. 2024.
25. H. Jeong, H. Son, S. Lee, J. Hyun, and T.-M. Chung, "FedCC: Robust Federated Learning against Model Poisoning Attacks," *arXiv* 2022.
26. Edi Marian Timofte *et al.*, "Federated Learning for Cybersecurity: A Privacy-Preserving Approach," *Applied Sciences*, Jun. 2025.
27. Kavitha, D., & Thejas, S. "AI enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation". *IEEE Access*. 2024, 12, 173127-173136
28. Rajesh, R., & Hemalatha, S. (2024). "Threat detection and mitigation for tactile internet driven consumer IoT-healthcare system". *IEEE Transactions on Consumer Electronics*. 70(1), 4249-4257.
29. S. A. Alzakari, A. Sarkar, M. Z. Khan, and Amel Ali Alhussan, "Converging Technologies for Health Prediction and Intrusion Detection in Internet of Healthcare Things With Matrix- Valued Neural Coordinated Federated Intelligence," *IEEE Access*, 2024.
30. Nallapareddy, V. S. S. R., & Katta, S. K. R. , "AI-Enhanced Cyber Security Proactive Threat Detection and Response Systems". In *2025 ICSADL* IEEE.

 doi:10.20944/preprints202512.2531.v1

31. Kshetri, N., Hutson, J., & Revathy, G. (2023, December). healthAIChain: Improving security and safety using Blockchain Technology applications in AI-based healthcare systems. In *2023 3rd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (pp. 159-164). IEEE.
32. Kshetri, N., Mishra, R., Rahman, M. M., & Steigner, T. (2024, April). HNMblock: Blockchain technology powered Healthcare Network Model for epidemiological monitoring, medical systems security, and wellness. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 01-08). IEEE.
33. O. F. Osama, N. Kshetri, M. M. Rahman and B. P. Pokharel, "healthMLsec: Machine Learning based Vulnerability Assessment in Health Systems: A Framework for Enhancing Cybersecurity and Patient Data," 2025 1st International Conference on Secure IoT, Assured and Trusted Computing (SATC), Dayton, OH, USA, 2025
34. A. Johnson *et al.*, "MIMIC-IV," *Physionet.org*, Oct. 11, 2024. https://physionet.org/content/mimiciv/3.1/
35. HealthData.gov, "HealthData.gov," 2019. https://healthdata.gov/
36. WHO, "World Health Data Platform - WHO," *www.who.int*, 2023.
37. Pokharel, B. P., Kshetri, N., Sharma, S. R., & Paudel, S. (2025). blockHealthSecure: Integrating Blockchain and Cybersecurity in Post-Pandemic Healthcare Systems. *Information*, *16*(2), 133.
38. Sunna, A. A., Sultana, T., Kshetri, N., & Uddin, M. M. (2025, April). AssessCICA: Assessing and Mitigating Financial Losses from Cyber Attacks with Role of Cyber Insurance in Post-Pandemic Era. In *2025 13th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE.
39. A. A. Hady, A. Ghubaish, T. Salman, D. Unal, and R. Jain, "Intrusion Detection System for Healthcare Systems Using Medical and Network Data: A Comparison Study", *IEEE Access*, 2020.