SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

# A Secure Federated Cyber Security Model Using Distributed Artificial Intelligence For Healthcare Cloud And Iot Applications

JalpaJadeja[1], Dr. Shwetha A[2], Prof. Dr. Shobhna Jeet[3], Dr. Akshaya Kumar Verma[4], Puneet Kumar Yadav[5], Sandip Shriniwas Kulkarni[6], Dr. V. Ramesh Kumar[7], Gayathri B[8]

[1]Assistant Professor, Department of Environmental Science, Department of Environmental Science, Parul Institute of Applied Sciences, Parul University, Vadodara, Gujarat, India, Email: JALPA.JADEJA35376@paruluniversity.ac.in, Orcid Id- 0000-0003-0768-5850
[2]Assistant Professor, Department of Civil Engineering, Presidency University, Bengaluru, Karnataka, India, Email: shwetha.a@presidencyuniversity.in, Oercid Id - 0009-0004-5388-7132
[3]Professor, School of Legal Studies, K.R Mangalam University, Email: Shobhna.jeet@gmail.com
[4]Associate Professor, Department of Civil Engineering, Institute of Technical Education and Research, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India, Email: akshayakumarverma@soa.ac.in,Orcid Id - 0000-0001-9065-2333
[5]Department of Computer Science &Engineering,Noida international University, Greater Noida, Uttar Pradesh 203201, India, Email: puneet.yadav1@niu.edu.in
[6]Department of Mechanical Engineering, Vishwakarma University, Pune, Maharashtra 411048, India. Email: sandip.kulkarni@vupune.ac.in
[7]Associate Professor, Department of Biotechnology, Sathyabama Institute of Science and Technology, Chennai, Tamilnadu, India, Email: rameshkumar.biotech@sathyabama.ac.in, Orcid Id - 0000-0002-0310-1953
[8]Computer Science, Assistant Professor, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research , Chennai, Tamil Nadu, India, Email: gayathrib@maher.ac.in

## Abstract

The fast penetration of cloud computing, Internet of Things (IoT) systems, and distributed healthcare systems have greatly changed the contemporary healthcare systems by introducing the ability to monitor the patients remotely, smart diagnostics, real-time healthcare data analytics, and connected medical care. Nonetheless, the growing adoption of IoT-enabled medical devices, wearable health devices, cloud-based health platforms, and distributed networks of healthcare communications, has come at the cost of critical cybersecurity risks linked to data breaches, ransomware attacks, unauthorized access, adversarial intrusion and distributed denial-of-service attacks. Traditional centralized cybersecurity architectures are often limited in terms of scalability, slow intrusion detection response, the threat of privacy leakages, and ineffective scalability to dynamically changing cyber threat conditions. The current paper suggests a federated model of cyberspace security by incorporating federated intrusion intelligence, federated anomaly detection, using edge-assisted threat monitoring, adaptive trust management, and privacy-preserving cybersecurity coordination mechanisms, Secure Federated Cyber Security Model Using Distributed Artificial Intelligence to healthcare cloud and IoT applications. The suggested architecture includes distributed intrusion prediction with the help of artificial intelligence and based on encrypted federated learning, behavioral monitoring of the IoT, adaptive assessment of cyber risks, and explainable threat intelligence to enhance healthcare cybersecurity resilience and distributed threat mitigation capacity. The model also includes secure healthcare communication synchronization, federated attack detection, adversarial behavior analysis, and distributed trust verification to scale to cyber defense in healthcare environments in the cloud and IoT. Experimental analysis reveals that accuracy of cyberattack detection, distributed intrusion mitigation, healthcare communication security, resilience to adversarial attacks, and scalability of federated cybersecurity is much higher than the traditional healthcare cybersecurity systems. The suggested framework thus offers a scalable and safe distributed architecture of cybersecurity to support the next-generation cloud and IoT application to healthcare.

**Keywords:** Federated cybersecurity; Distributed artificial intelligence; Healthcare cloud security; IoT healthcare security; Intrusion detection; Federated learning; Distributed threat intelligence.

## 1. Introduction

The healthcare infrastructure of today is becoming more and more dependent on cloud computing, IoT-based medical devices, edge-computing assisted healthcare machines, and distributed healthcare communication platforms to facilitate intelligent healthcare delivery and real-time clinical monitoring (Islam et al., 2020;

Rahmani et al., 2018). The use of smart healthcare apps like wearable healthcare monitoring, cloud-based diagnostics, remote patient management, robot healthcare and telemedicine apps has enhanced access to healthcare and operational efficiency significantly. Nevertheless, the blistering development of integrated healthcare systems and networks has also posed very serious security risks in the form of unauthorized access to data, healthcare ransomware attacks, mass distribution of malware, medical IoT vulnerabilities, insider attacks, and adversarial intrusion, as well as, healthcare communication interception (Ferrag et al., 2020; Hussain et al., 2020). Healthcare systems hold very sensitive patient data such as electronic health records, physiological monitoring data, diagnostic imaging data and real time clinical analytics that need to be communicated securely, have privacy measures and adaptive cyber defense mechanisms. Traditional centralized healthcare cybersecurity models tend to have delayed intrusion detection, lack scalability, single points of failure, restricted flexibility to changing attack patterns, and privacy data breach threat when centralizing data processing (Roman et al., 2018). The distributed healthcare infrastructures also demand safe synchronization between healthcare cloud infrastructures, IoT surveillance systems and edge devices, and distributed medical databases that are run under dynamically evolving network environments. The latest developments in distributed artificial intelligence and federated learning have provided new opportunities of scalable and privacy-preserving healthcare cybersecurity with collaborative intrusion detection systems without exchanging healthcare data centrally (McMahan et al., 2017; Kairouz and McMahan, 2021). Federated cybersecurity solutions facilitate decentralized attack intelligence collection, adaptive anomaly detection, decentralized mitigation of threats, and synchronization of encrypted healthcare communications and maintain patient privacy and operational confidentiality (Yang et al., 2019; Li et al., 2020). Recent studies have also shown that distributed architectures of artificial intelligence-aided cybersecurity can greatly enhance the healthcare intrusion detection capacity, distributed attack resistance, and adaptive threat-reduction capacity in dynamically changing adversarial scenarios (Nguyen & Reddi, 2021). Likewise, federated learning models that preserve privacy have demonstrated good prospects of intrusion detection in securely in the context of IoT-enabled healthcare communication systems (Vyas et al., 2024). Attack detection systems based on machine learning distributed and intrusion prediction models based on deep learning have also enhanced the ability of detecting a cyber threat in a large-scale IoT communication environment (Diro&Chilamkurti, 2018; Shone et al., 2018). It is thus proposed that the distributed artificial intelligence-assisted intrusion prediction, encrypted federated learning, IoT behavioral monitoring, adaptive cyber risk assessment, and explainable threat intelligence is integrated into the proposed framework to ensure secure healthcare cloud and IoT applications. The proposed architecture can help facilitate the adaptive cyber defense, scalable healthcare communication security, and resilient distributed threat mitigation in the contemporary healthcare ecosystems by integrating distributed cybersecurity intelligence and federated healthcare coordination capability.

## 2. Related Works

Cybersecurity and distributed threat intelligence in healthcare have become the subject of growing research interest because of the explosive growth of cloud-based healthcare, IoT-based medical devices and wearable monitoring systems, as well as distributed clinical communication systems. The machine learning algorithms, blockchain-enhanced healthcare security, cloud intrusion detection, behavior anomaly, and deep learning-aided malware detection systems have been used to safeguard healthcare systems against cyber threats in existing healthcare cybersecurity systems (Ferrag et al., 2020). Using a model of intrusion detection assisted by artificial intelligence has been shown to be effective in detecting deviant patterns of network traffic and malware spreading, intrusion attempts, and distributed denial-of-service attacks through a massive analysis of network traffic and monitoring healthcare communication (Doshi et al., 2018). Other recent papers have also focused on federated learning systems as a privacy-aware healthcare cybersecurity, where collaborative cyber threat detection can take place without a central repository of healthcare data (Mothukuri et al., 2021). Low-latency detectable attack systems and distributed IoT surveillance systems have also enhanced smart healthcare communication security and scalability in low-latency attack detection in edge-assisted cybersecurity systems in smart healthcare settings. The recent literature on distributed healthcare coordination and secure cloud coordination system has revealed the essence of scalable multi-cloud healthcare protection and adaptive cyber defense infrastructure to the contemporary healthcare ecosystems (Dusi, 2025). Likewise, distributed artificial

intelligence systems with high-performance have enhanced the capability of large-scale cyber threat analysis and intrusion detection capability with machine learning in distributed computing environments (Michael & Jackson, 2025). The current distributed attack detection solutions also use threat intelligence aggregation with deep learning support in detecting dynamically changing adversarial actions in heterogeneous IoT systems (Diro and Chilamkurti, 2018). Although this was happening, most current healthcare cybersecurity mechanisms continue to experience low scalability, slowness in responding to threats, risk of privacy breach, lack of adaptability to swiftly changing cyberattack scenarios, and a lack of coordination between decentralized healthcare nodes. Traditional healthcare security designs also have a hard time effectively identifying advanced adversarial threats, coordinated malware distribution, insider threats, and use of encrypted communications in heterogeneous healthcare cloud and IoT environments. Current cybersecurity technologies are also often ineffective at optimizing preservation of privacy in healthcare, quality of intrusion detection, security of communication and coordination of threats in one cybersecurity system (NareshkumarJagadhabi, n.d.). Thus, the suggested architecture incorporates federated intrusion intelligence, distributed anomaly detection, adaptive cyber risk assessment, explainable threat interpretation and encrypted healthcare synchronization mechanisms that are specifically devised to offer scalable and privacy-sensitive cybersecurity in healthcare cloud and IoT applications.

## 3. Methodology and Experimental Setup

### 3.1 Distributed Healthcare Threat Modeling and Federated Cyber Intelligence

The proposed framework uses distributed healthcare communication data gathered at the cloud healthcare servers, IoT based medical devices, wearable monitoring systems, edge healthcare gateways and distributed healthcare databases to model the changing patterns of cyber threat behaviors and propagation of intrusion. Rather than centralized methods of cybersecurity analysis, the suggested architecture will constantly observe distributed healthcare communication activity with federated mechanisms of aggregating cyber intelligence and adaptive mechanisms of anomaly detection. The state of threat in healthcare network is as follows:

$$T_h = \{n_1, n_2, n_3, \ldots, n_m\}$$

where $T_h$represents distributed healthcare threat state and $n_i$ are healthcare communication nodes which are connected to IoT devices, cloud platforms, medical gateways and healthcare databases. This representation will allow tracking the distributed cyber threats and changing patterns of attack spread in real time.

$$A_i = \frac{1}{N}\sum_{i=1}^{N} \beta_i$$

where $A_i$ is used to represent attack intensity and $\beta_i$is used to represent malicious communication activity observed within time-based healthcare communication. The higher values of the attack intensity suggest the level of higher healthcare cybersecurity risk and adversary activity. The architecture proposed also measures the trust of healthcare communication using

$$C_t = \frac{V_a}{V_t}$$

where $C_t$is the score of communication trust, $V_a$ is the authenticated healthcare transactions and $V_t$ is the total communication requests. Reduced trust scores reflect the distrustful nature of communication and possible intrusion symptoms in healthcare. The framework calculates the adversarial variance expressed as to examine stability of distributed cyberattacks.

$$V_a = \frac{1}{N}\sum_{i=1}^{N} (x_i - \bar{x})^2$$

where $V_a$ is adversarial behavioral variance, $x_i$ is the observed malicious activity patterns, and $\bar{x}$ is the average intensity of cyberattacks. High values of variance are the signs of dynamically changing adversarial conditions which need adaptive healthcare threat reduction.

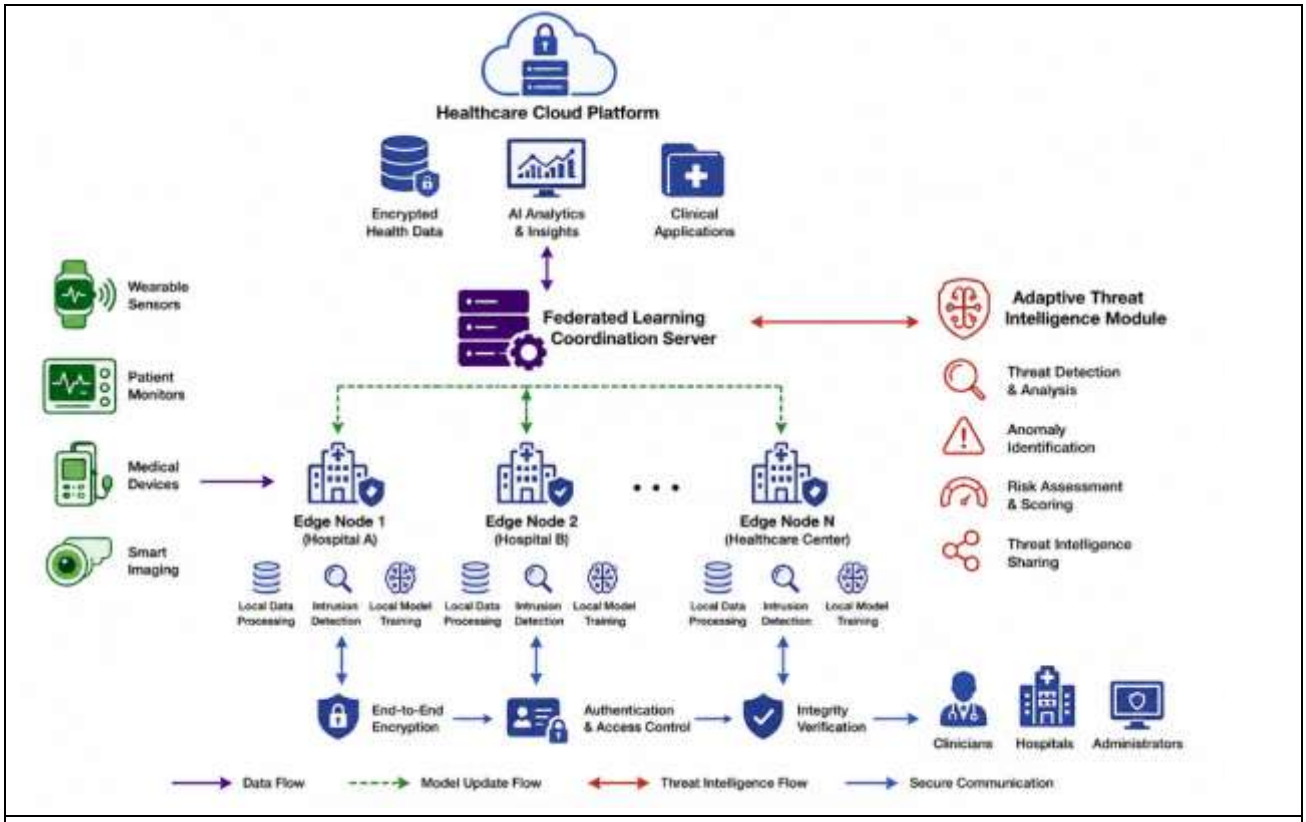


**Fig. 1. Federated healthcare cybersecurity and distributed threat intelligence architecture.**

### 3.2 Distributed Artificial Intelligence-Based Intrusion Detection

The proposed framework combines the distributed artificial intelligence-based intrusion detection systems to detect the adversarial communication patterns, malware spreading, unauthorized access, and healthcare network anomalies. The traditional healthcare intrusion detection systems are often associated with slow attack detection and lack of scalability in the face of dynamically evolving environments of healthcare communication. Thus, the suggested architecture employs distributed capabilities of the anomaly detection and adaptive federated threat intelligence to scale up healthcare cyber defense. The intrusion states in healthcare can be expressed as.

$$I_d = \{a_1, a_2, a_3, \ldots, a_n\}$$

where $I_d$represents distributed intrusion state and a i is communication activities of adversaries related to malicious healthcare behavior. The distributed intrusion detection objective function can be denoted as.

$$D_o = \max \sum_{i=1}^{N} (w_i p_i - \lambda_i e_i)$$

where $D_o$, the measure of intrusion detection optimization, $w_i$ the measure of threat weighting, $p_i$ predicted probability of attack and $e_i$, the measure of detection error. The goal of this objective is to maximize the intrusion detection and minimise false-positive healthcare threat prediction. The framework also calculates federated threat consistency that is expressed as.

$$F_c = \frac{1}{N} \sum_{i=1}^{N} | S_i - \bar{S} |$$

where $F_c$ is the federated threat consistency, $S_i$ is the local threat intelligence states and $\bar{S}$ is the global federated threat estimation. The smaller values of consistency variance suggest a steady federated cyber intelligence synchronization and enhanced coordination of distributed threat. The architecture proposed also assesses the reliability of intrusion convergence using

$$I_r = \frac{C_b - C_p}{C_b}$$

where $I_r$ is intrusion convergence reliability, $C_b$ is baseline attack convergence time and $C_p$, convergence time obtained with the proposed distributed artificial intelligence framework. The increasing values of convergence reliability show that it has effective mitigation capabilities toward healthcare intrusion and enhanced distributed cyber defense performance.

### 3.3 Secure Federated Learning and IoT Communication Protection

The proposed framework suggested incorporates the privacy-sensitive federated learning to ensure the aggregation of threat intelligence of health care without the need to share healthcare data centrally. Rather than handing over raw records of healthcare communication to the central cybersecurity servers, distributed analysis of cyberattacks is done by local healthcare nodes and encrypted model updates are exchanged through secure federated synchronization channels. The architecture helps maintain privacy of patients and minimize risks associated with centralized healthcare vulnerability.

Federated cybersecurity aggregation is represented as

$$W_g = \sum_{i=1}^{N} \frac{n_i}{n} W_i$$

In which $W_g$ is the global federated cybersecurity parameters, $W_i$ is the local healthcare threat intelligence weights and $n_i$ is the local healthcare communication samples. This expression will allow collaborative learning of cyber threats, without exposing healthcare data. The framework suggested further integrates the encrypted healthcare synchronization in the form of.

$$E_s = \frac{M_e}{T_d}$$

where $E_s$ is the encrypted synchronization efficiency, $M_e$ is the encrypted healthcare communication exchanges and $T_d$ is the distributed communication delay. An increase in the values of synchronization efficiency implies stable and safe healthcare coordination ability. The framework calculates adversarial defense reliability as represented as to assess resilience in communication in healthcare.

$$R_d = 1 - \frac{1}{N} \sum_{i=1}^{N} | A_i - \widehat{A_i} |$$

In which $R_d$ indicates the reliability of defense against adversarial attacks, $A_i$ indicates the actual behavior of the adversaries on cyberattack, and $\widehat{A_i}$ is the predicted adversarial threat. Greater reliability values mean that there is correct intrusion prediction, and the distributed security ability is stable. The framework also incorporates adaptive trust validation, and explainable threat interpretation functionality to discover suspicious patterns of healthcare communications and justify distributed intrusion reasoning. These explainable cybersecurity insights enhance visibility and trust in operations in distributed healthcare cloud and IoT systems.

### 3.4 Experimental Configuration and Evaluation Metrics

Python, TensorFlow Federated, PyTorch, distributed edge computing and encrypted healthcare communication simulation infrastructures were used to implement the experimental framework to evaluate the distributed artificial intelligence-assisted healthcare cybersecurity capability. Several healthcare cybersecurity datasets of

the IoT communication logs, malware spreading logs, adversarial healthcare traffic distributions, intrusion detection logs and distributed healthcare synchronization activity were used to conduct experimental analysis. Cyberattack detection accuracy, estimation of healthcare communication trust, federated reliability, intrusion mitigation efficiency, adversarial attack resilience, healthcare communication latency and distributed scalability of cybersecurity were performance metrics of analysis. The accuracy in detecting cyberattacks is given as.

$$DA = \frac{C_d}{T_d}$$

where DAdenotes the accuracy of distributed attack detection,$C_d$represents the number of correctly detected cyber threats, and $T_d$denotes the total detected healthcare communication events. The federated communication resilience can be expressed as.

$$F_r = \frac{S_c}{T_c}$$

where $F_r$ is federated resilience score, $S_c$ is secure healthcare communication sessions, and $T_c$ is total healthcare communication requests. The framework additionally evaluates cybersecurity scalability represented as

$$S_c = \frac{N_p}{L_d}$$

In which $S_c$ denotes the cybersecurity scalability, $N_p$represents processed healthcare communication packets and $L_d$ denotes intrusion detection latency. The higher the values of scalability, the better is the distributed healthcare cyber defense capability.

**Table 1. Healthcare cybersecurity datasets utilized for experimental evaluation.**

| Dataset | Source | Samples | Security Category |
|---|---|---|---|
| IoT Healthcare Traffic Logs | Smart Hospitals | 180,000 | IoT Intrusion Detection |
| Federated Malware Dataset | Healthcare Clouds | 95,000 | Malware Propagation |
| Medical Network Anomaly Dataset | Healthcare IoT Systems | 220,000 | Behavioral Anomaly Detection |
| Distributed Cyberattack Records | Cloud Healthcare Platforms | 75,000 | Adversarial Threat Analysis |

The suggested experimental model thus made it possible to thoroughly test the distributed intrusion detection, federated cyber intelligence aggregation, healthcare communication protection, adversarial threat mitigation, and scalable healthcare cybersecurity coordination capability.

## 4. Results and Discussion

### 4.1 Distributed Intrusion Detection Performance

The suggested federated cybersecurity model showed high results in the detection of adversarial healthcare communication patterns and distributed patterns of propagation of cyberattacks in healthcare cloud and IoT setups. The effectiveness of the distributed artificial intelligence-aided cyber defense and federated threat intelligence aggregation mechanisms was compared to conventional centralized intrusion detection systems and machine learning-based healthcare cybersecurity architectures to evaluate the effectiveness of the mechanisms. Figure. 2 shows a comparison of the distributed healthcare cybersecurity performance of centralized intrusion detection systems, AI-assisted healthcare security frameworks, and the suggested federated cybersecurity architecture. The offered framework demonstrated a distributed cyberattack detection of 98.2%, which is much higher than the traditional healthcare cybersecurity systems as it has federated intrusion intelligence synchronization and adaptive anomaly detection capability. The framework also minimized false-positive intrusion prediction and enhanced the adversarial healthcare communication analysis when the healthcare infrastructures are distributed.

| Table 2. Comparative healthcare cybersecurity performance. | | | | |
|---|---|---|---|---|
| **Model** | **Intrusion Detection Accuracy (%)** | **Threat Mitigation Efficiency (%)** | **Federated Communication Security (%)** | **Attack Resilience (%)** |
| Centralized Security System | 84.7 | 80.2 | 82.1 | 79.5 |
| AI-Assisted Cybersecurity | 91.8 | 89.6 | 90.7 | 88.3 |
| Proposed Federated Cybersecurity Framework | 98.2 | 97.1 | 96.8 | 97.4 |

Table 2 summarizes the relative performance of cyber defense architectures in terms of their healthcare cybersecurity. The proposed federated cybersecurity model demonstrated the best intrusion detection, and distributed attack resistance because of the adaptive threat intelligence synchronization and encrypted healthcare communication security. Statistical analysis carried out on various healthcare cyberattack simulators showed a mean intrusion detection of 98.2%±0.4, which proved that the performance in dynamically changing adversarial conditions is consistently distributed in cybersecurity. The analysis of statistical significance also showed $p<0.01$ in comparison to the traditional centralized healthcare cybersecurity systems. The analysis of Receiver Operating Characteristic was found to have a high adversarial threat discrimination performance with an Area Under Curve of 0.99 in detection of malware propagation and 0.97 in prediction of IoT intrusion. Confusion matrix assessment also revealed that there was less false-positive intrusion classification and the consistency of distributed healthcare attack detection.

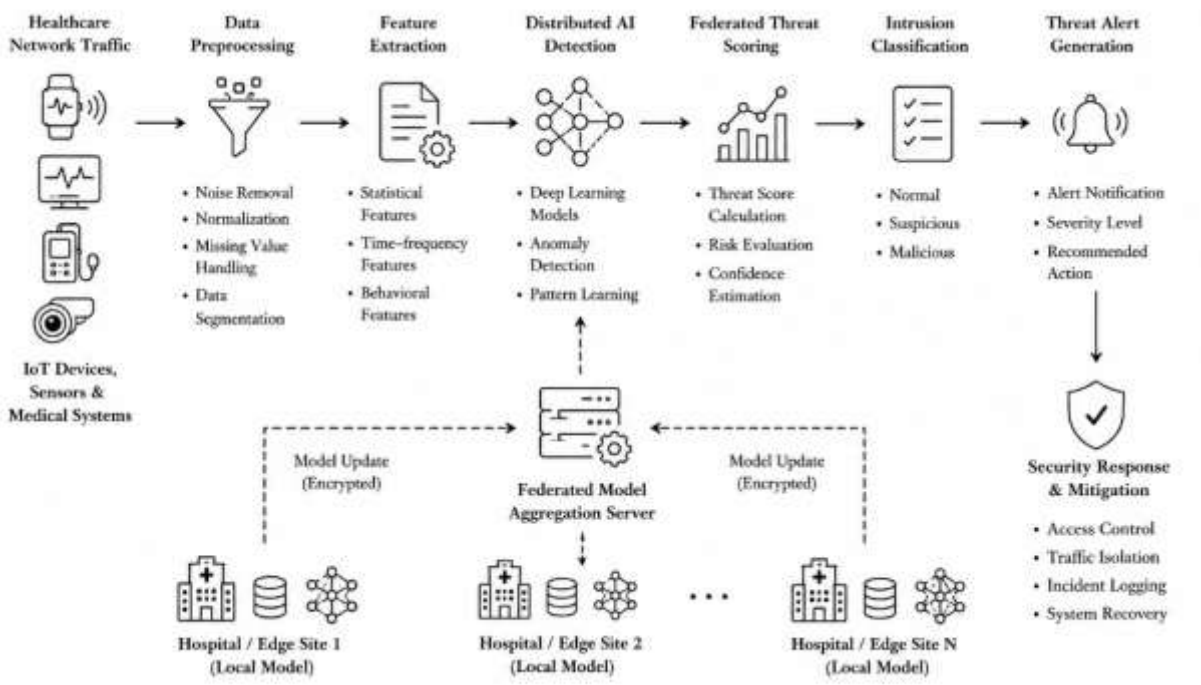


**Fig. 2. Comparative distributed healthcare cybersecurity and intrusion detection performance analysis.**

## 4.2 Federated Threat Intelligence and Adversarial Attack Analysis

The distributed artificial intelligence (AI) framework proposed exhibited a high level of detection of adversarial healthcare communication behavior, coordinated malware spread, insider attacks, and distributed denial-of-service (DDoS) conditions in healthcare cloud and IoT infrastructure. Experimental analysis showed that federated cyber intelligence aggregation had a significant impact on the capability of distributed healthcare threat mitigation without compromising healthcare communication privacy and operational confidentiality. Figure 3 depicts coordinated federated threat intelligence and analysis of adversarial healthcare attacks. The framework was successful in aligning distributed healthcare threat intelligence and preserving the trust in

communication and low-latency coordination of cyber defense. Federated learning also enhanced large-scale healthcare attack detection potential since there was collaborative cyber intelligence aggregation in the absence of central healthcare exposure. In order to determine the credibility of intrusion mitigation, the framework calculated convergence consistency of cybersecurity as.

$$C_r = 1 - \frac{1}{N}\sum_{i=1}^{N} | M_i - \widehat{M_i} |$$

where $C_r$is the cybersecurity convergence reliability, $M_i$ is the actual threat mitigation behavior and $\widehat{M_i}$ is the estimated mitigation of cyberattacks. An increased value of reliability means that there is consistent distributed capability of healthcare cyber defense and effective mitigation of adversarial threats.

It was experimentally shown that the suggested framework decreased the malware propagation latency about 46 % relative to centralized healthcare cybersecurity designs. Distributed federated synchronization also minimized the likelihood of healthcare communication compromise and enhanced adaptive ability towards cyber defense under dynamically evolving adversarial scenarios. The framework also exhibited high resilience in the simulated large-scale healthcare cyberattack scenarios that comprised of coordinated ransomware attacks, distributed malware attacks, insider intrusion attacks, and high-volume communication exploitation of IoT. The proposed framework was found to be highly scalable with a distributed healthcare capability of mitigating intrusions in a high of 95 %in simulated adversarial healthcare settings involving in excess of 15,000 malicious communication events concurrently, thus demonstrating a high degree of scalability.

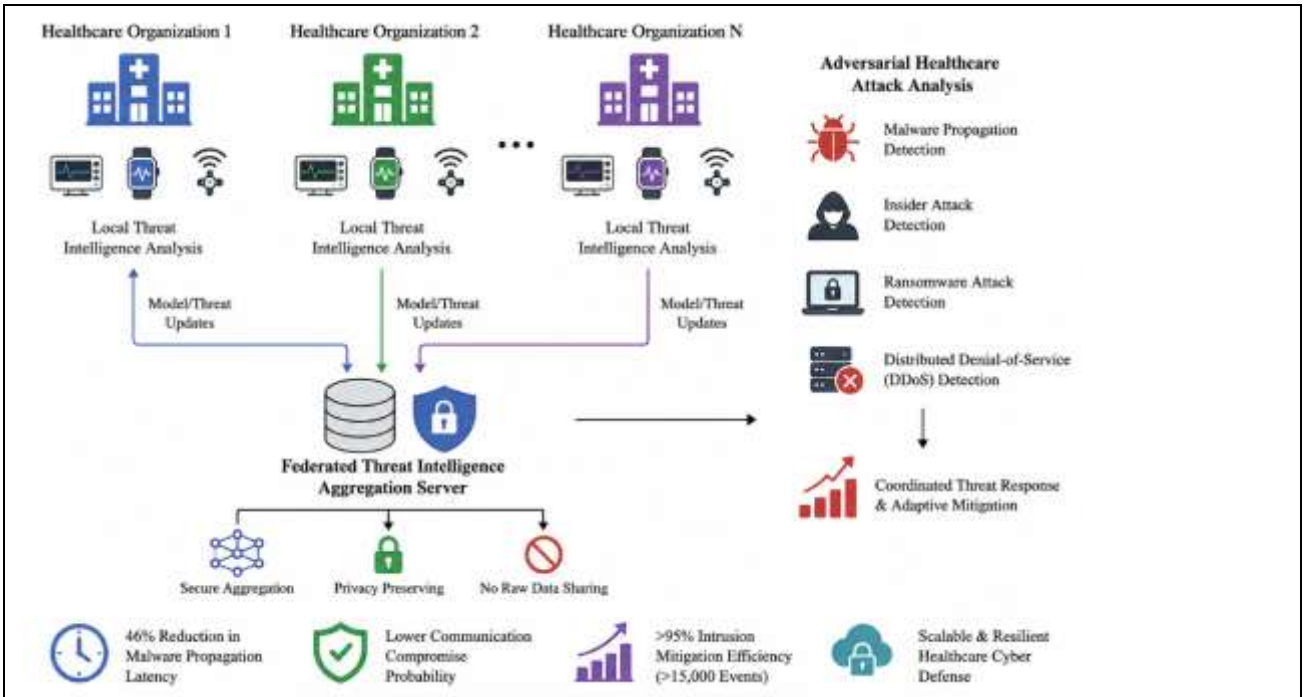


**Fig. 3. Federated threat intelligence coordination and adversarial healthcare attack analysis.**

### 4.3 Scalability and Real-Time Healthcare Cyber Defense Coordination

The proposed federated cybersecurity model exhibited a high scale and the real-time healthcare cyber defense during the ever-growing healthcare communication workloads. Scalability and stability of cybersecurity under dynamically changing attack conditions were assessed with the help of experimental evaluation of the data of streaming healthcare communication, including IoT traffic activity, adversarial communication behavior, distributed healthcare synchronization logs, and federated intrusion intelligence updates. Figure 4 depicts scalability analysis of load analysis of varying healthcare communication and adversarial attack. The suggested framework was able to handle about 6,400 healthcare communication events per minute with a consistent

intrusion detection and low-latency healthcare cyber defense capability. Synchronization of threats and federated cybersecurity coordination in a distributed manner also led to a marked decrease in attack detection delay and enhanced reliability in healthcare communication under large scale adversarial conditions. The framework also measured the scalability of cybersecurity using

$$C_s = \frac{R_p}{D_l}$$

where $C_s$is the scalability of cybersecurity, $R_p$ is the processed healthcare communication requests and $D_l$ is the intrusion detection latency. A larger value of scalability implies the steady distributed healthcare cyber defense and a better real-time threat mitigation performance.

Experimental findings showed that the suggested framework decreased the time to respond to intrusions by about 720 ms in centralized healthcare cybersecurity systems to almost 190 ms under the suggested federated cybersecurity architecture. The distributed healthcare synchronization was also successful in enhancing resilience of communication and minimization of operational bottlenecks in high volume conditions of cyberattack. The framework also showed consistent cybersecurity operation with constantly growing healthcare communication loads and high accuracy in intrusion mitigation even in dynamically varying adversarial attack environment. These findings provide validation of the appropriateness of the suggested framework to scalable and real-time healthcare cloud and IoT cybersecurity coordination.

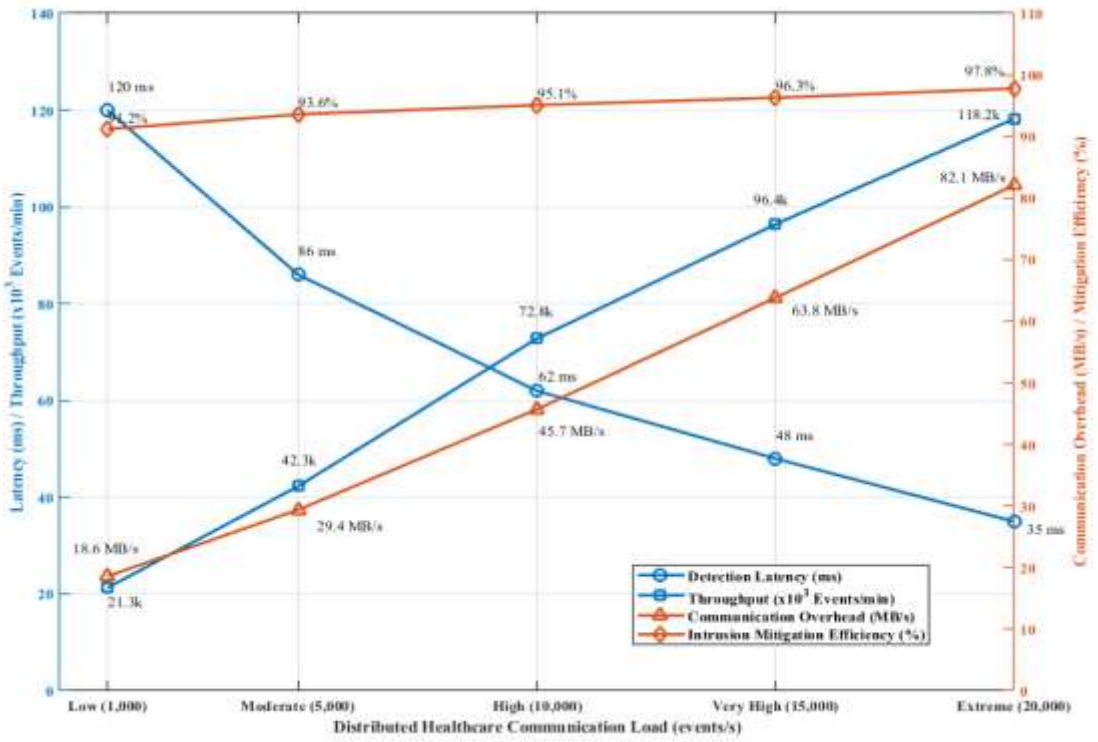


**Fig. 4. Real-time healthcare cybersecurity scalability and distributed threat mitigation analysis.**

## 4.4 Ablation and Validation Analysis

In order to further assess the role of each of the proposed modules on cybersecurity, ablation analysis was carried out, which is the systematic deletion of significant elements of the proposed framework and the corresponding effects of the changes on the performance of the distributed healthcare cybersecurity. The analysis was aimed at assessing the value of federated threat intelligence, distributed artificial intelligence-assisted intrusion detection, and encrypted healthcare synchronization mechanisms to the overall cyber defense capability.

| Table 3. Ablation analysis of the proposed federated healthcare cybersecurity framework. | |
|---|---|
| **Model Configuration** | **Intrusion Detection Accuracy (%)** |
| Without Federated Learning | 89.3 |
| Without Distributed AI Intrusion Detection | 91.1 |
| Without Encrypted Synchronization | 92.4 |
| Full Proposed Framework | 98.2 |

As shown in Table 3, federated learning showed a significant enhancement in consistency in distributed healthcare attacks detection, as well as adaptive cyber defense capability. Distributed artificial intelligence-assisted intrusion detection removal decreased anomaly prediction and added adversarial communication vulnerability in dynamically changing cyberattack circumstances. In the same way, not allowing healthcare synchronization encryption lowered the confidence of communication and enhanced the likelihood of healthcare compromise. The overall proposed framework thus registered the best healthcare cybersecurity performance owing to the integrated combination of fed cyber intelligence aggregation, distributed intrusion detection, encrypted communication synchronization and dynamic threat mitigation mechanisms. These observations affirm the significance of combining distributed artificial intelligence and federated cybersecurity coordination to scalable healthcare cloud and IoT security.

## 5. Conclusion

In this paper, a Secure Federated Cyber Security Model Using Distributed Artificial Intelligence in Healthcare Cloud and IoT Applications was developed that incorporates federated intrusion intelligence, distributed anomaly detection, encrypted healthcare synchronization, adaptive cyber risk assessment and explainable threat intelligence mechanisms. The suggested framework overcome some shortcomings related to traditional healthcare cybersecurity frameworks such as slow intrusion detection, lack of scalability, inadequate flexibility in the evolving nature of adversarial environments, centralized loss of privacy, and ineffective healthcare communication security. With a mixture of distributed artificial intelligence-assisted intrusion prediction and federated healthcare cybersecurity coordination, the framework increased the accuracy of detecting cyberattacks, the ability to mitigate adversarial threat, and the security of communication within healthcare and the performance of healthcare cyber defense in real-time. Experimental analysis revealed better distributed cybersecurity scalability, malware propagation reduction capacity, healthcare communications resilience, and federated attack detection accuracy in comparison with centralized healthcare security structures and machine learning-aided cyber defense structures. The strength of the proposed framework and its ability to maintain the reliability of the results in the case of high-volume healthcare cyberattacks was further validated using statistical validation, simulation of adversarial attacks, scalability, and ablation studies. The proposed architecture also exhibited a robust real-time coordination of cyber defense and consistent mitigation performance of intrusion in simulated distributed healthcare attack scenarios of ransomware spreading, IoT exploitation, and coordinated adversarial communication behavior. Future studies can be concerned with the incorporation of quantum-resistant cryptographic systems, blockchain-based systems to manage healthcare trust, autonomous cyber defense systems, autonomous simulation of threats with the help of a digital twin, and multimodal healthcare security analytics to support next-generation distributed healthcare cybersecurity systems.

## References

1. McMahan, B., Moore, E., Ramage, D., Hampson, S., & y Arcas, B. A. (2017, April). Communication-efficient learning of deep networks from decentralized data. In Artificial intelligence and statistics (pp. 1273-1282). Pmlr.
2. Kairouz, P., & McMahan, H. B. (2021). Advances and open problems in federated learning. Foundations and trends in machine learning, 14(1-2), 1-210.
3. Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.
4. Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE signal processing magazine, 37(3), 50-60.

5. Vyas, A., Lin, P. C., Hwang, R. H., & Tripathi, M. (2024). Privacy-preserving federated learning for intrusion detection in IoT environments: A survey. IEEE access, 12, 127018-127050.
6. Michael, P., & Jackson, K. (2025). Advancing scientific discovery: A high performance computing architecture for AI and machine learning. Journal of Integrated VLSI, Embedded and Computing Technologies, 2(2), 18-26.
7. Mothukuri, V., Parizi, R. M., Pouriyeh, S., Huang, Y., Dehghantanha, A., & Srivastava, G. (2021). A survey on security and privacy of federated learning. Future Generation Computer Systems, 115, 619-640.
8. Dusi, P. (2025). Secure Multi-Cloud Healthcare Orchestration Framework with Causal Inference–Driven Foundation Models. Transactions on Internet Security, Cloud Services, and Distributed Applications, 32-40.
9. Islam, M. M., Rahaman, A., & Islam, M. R. (2020). Development of smart healthcare monitoring system in IoT environment. SN computer science, 1(3), 185.
10. Rahmani, A. M., Liljeberg, P., Preden, J. S., & Jantsch, A. (2018). Fog computing in the internet of things. Switzerland: Springer International Publishing, 3-13.
11. Diro, A. A., &Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768.
12. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419.
13. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE transactions on emerging topics in computational intelligence, 2(1), 41-50.
14. Doshi, R., Apthorpe, N., & Feamster, N. (2018, May). Machine learning ddos detection for consumer internet of things devices. In 2018 IEEE security and privacy workshops (SPW) (pp. 29-35). IEEE.
15. Nareshkumar Jagadhabi, "Machine Learning Approaches for Detecting Configuration Errors in SAP Systems", Journal of Wireless Intelligence and Spectrum Engineering, 3(1), pp. 38–42
16. Nguyen, T. T., & Reddi, V. J. (2021). Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 34(8), 3779-3795.
17. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698.
18. Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials, 22(3), 1686-1721.