International Journal of Multidisciplinary and Current Research ISSN: 2321-3124
Research Article Available at: http://ijmcr.com

Enhancing Threat Detection in Healthcare Systems Through Cloud- Based Security Solutions

[1*]Priyadarshini Radhakrishnan, [2]Vijai Anand Ramar, [3]Karthik Kushala, [4]Venkataramesh Induru and [5]Punitha Palanisamy

[1]IBM Corporation, Ohio, USA
[2]Delta Dental Insurance Company,Georgia,USA
[3]Celer Systems Inc, Folsom, California, USA
[4]Piorion Solutions Inc, New York, USA
[5]Tagore Institute of Engineering and Technology, Salem,India

Received 01 April 2024, Accepted 15 April 2024, Available online 20 April 2024, **Vol.12 (March/April 2024 issue)**

Abstract

Growing use of digital infrastructure in the health sector has contributed enormously to healthcare but opened the systems up to an unprecedented variety of high-tech cyber-attacks. This research advances a new framework for tackling the risks through proposing a Federated Self-Adaptive Threat Detection (FedSATD) model, especially created for cloud-enabled smart health care settings. In contrast to centralized or stand-alone local traditional systems, FedSATD takes advantage of federated learning's strengths to allow multiple healthcare institutions to jointly train a threat detection model without the exchange of patient data that is private. The decentralized architecture promotes privacy, mitigates data transfer danger, and provides regulatory compliance while enjoying disparate data distributions across institutions. FedSATD leverages deep learning approaches such as LSTM and autoencoders to scan time-series network traffic and determine cyberattack-associated anomalies. Careful preprocessing pipe is applied on each local dataset, ranging from cleaning to encoding, normalization, and sequence setup, to ensure data quality as well as prepare the model. Model performance was assessed with genuine healthcare network traces and compared to standard deep models such as DNN, GRU, and VGG-16. Experimental results indicate FedSATD works better than all the mentioned models in all of the most significant performance measures having 99.72% accuracy, 99.22% precision, 98.94% recall, and a 99.33% F1-score. Graphical plots also support FedSATD's excellence in reducing false alarms at high detection rates. Moreover, pie charts show a high ratio of true positive detection, reflecting excellent model reliability.In summary, the FedSATD model provides a strong, scalable, and privacy-enhancing solution for bolstering cybersecurity in contemporary healthcare systems. Its adaptive learning capability from distributed environments without involving information privacy makes it a valuable contribution to the field of cloud-based healthcare security.

Keywords*: Healthcare Cybersecurity, Federated Learning, Threat Detection, Cloud-Based Security, Anomaly Detection, FedSATD, Network Intrusion Detection, Cyber Threat Intelligence*

1. Introduction

The healthcare industry is undergoing a transformative shift through the adoption of digital technologies designed to improve patient outcomes, streamline operational workflows, and manage extensive volumes of sensitive medical information [1]. Modern healthcare systems are increasingly reliant on electronic health records (EHRs), telemedicine platforms, IoT-enabled medical devices, and cloud-based applications.

While these advancements enable more efficient and personalized care, they also introduce new cybersecurity vulnerabilities that can jeopardize patient safety, disrupt services, and lead to significant financial and reputational damage [2]. The evolving cyber threat landscape, characterized by ransomware attacks, data breaches, and insider threats, has outpaced the capabilities of traditional on-premises security frameworks [3]. These legacy systems often lack the scalability, adaptability, and analytical precision necessary to counter sophisticated and dynamic cyber risks. Cloud-based security solutions offer a compelling alternative, providing real-time threat detection, automated response mechanisms, and

*Corresponding author' ORCID ID: 0000-0000-0000-0000
DOI: https://doi.org/10.14741/ijmcr/v.12.2.4

enhanced monitoring capabilities tailored to the unique needs of healthcare environments [4]. Leveraging machine learning and artificial intelligence, these platforms can analyze vast streams of data to identify anomalies and mitigate threats before they escalate. Additionally, integrating blockchain technology into cloud infrastructures enhances data integrity and trust by creating immutable records of access and transactions, bolstering transparency and traceability across healthcare networks [5]. These innovations support secure patient consent processes, safeguard the medical supply chain, and facilitate the sharing of anonymized threat intelligence among healthcare providers and regulatory bodies, strengthening collective resilience [6].

This research aims to explore and evaluate the application of cloud-based security technologies within healthcare settings [7]. It proposes a comprehensive framework that includes AI-powered threat detection, microsegmentation strategies, automated compliance enforcement, and collaborative threat intelligence sharing [8]. By examining these elements in depth, the study highlights how cloud-based solutions can significantly enhance the cybersecurity posture of healthcare organizations, ensuring the confidentiality, integrity, and availability of critical systems and data in an era of increasingly complex and persistent cyber threats [9]. As healthcare systems continue their digital transformation journey, the adoption of interconnected technologies like electronic health records (EHRs), wearable devices, telemedicine, and AI-driven diagnostics has generated vast repositories of sensitive medical data [10]. These advancements have created a data-rich environment that enables personalized medicine, efficient care delivery, and remote patient monitoring. However, with increased digital exposure comes an expanded attack surface vulnerable to sophisticated and persistent cybersecurity threats [11]. Protecting this sensitive information while maintaining seamless service delivery has become one of the foremost challenges for modern healthcare institutions.

The healthcare sector is increasingly targeted by cybercriminals due to the high value of medical data on the black market and the critical nature of healthcare operations [12]. Attackers exploit vulnerabilities through phishing campaigns, ransomware, and advanced persistent threats (APTs) that can cripple hospital operations, disrupt patient services, and even endanger lives. These attacks not only compromise patient privacy but also erode trust in healthcare providers and create legal and regulatory repercussions [13]. Consequently, cybersecurity is no longer an auxiliary concern but a central pillar of healthcare system reliability and resilience. Traditional, perimeter-based security measures are proving inadequate in this evolving threat landscape [14]. On-premises firewalls and intrusion detection systems often lack the agility, scalability, and real-time analytics necessary to counter advanced attacks. Moreover, decentralized healthcare environments, characterized by mobile staff, remote consultations, and multi-vendor systems, challenge the effectiveness of legacy security frameworks [15]. The need has emerged for dynamic, intelligent security solutions that are capable of adapting to new threats and managing complex IT infrastructures efficiently. Cloud computing has introduced a paradigm shift in how healthcare systems can manage their data, infrastructure, and security operations [16]. Cloud-based platforms offer scalable resources, on-demand access to computational power, and integrated security services that are inherently more responsive and data-driven [17]. Advanced security features such as automated patch management, distributed denial-of-service (DDoS) protection, and centralized monitoring enable healthcare organizations to maintain robust cybersecurity postures while reducing the cost and complexity of on-premise infrastructure [18]. The integration of artificial intelligence and machine learning into cloud-based security frameworks further enhances their effectiveness. These technologies allow real-time threat detection by continuously analyzing behavior patterns, network traffic, and user activity [19]. When anomalies are detected, automated response mechanisms can isolate affected systems, alert administrators, and mitigate risks with minimal delay [20]. This level of responsiveness is critical in environments where downtime or data loss can have life-threatening consequences [21]. As healthcare systems become more intelligent and interconnected, leveraging AI-enhanced cloud security is essential for timely and accurate threat detection. In addition to real-time monitoring and intelligent threat detection, cloud-based platforms can facilitate industry-wide collaboration through secure data sharing and collective intelligence [22]. By utilizing technologies like blockchain, secure multiparty computation, and threat intelligence sharing platforms, healthcare institutions can strengthen collective resilience against cyber threats [23]. This collaborative defense approach is particularly valuable in mitigating large-scale attacks such as ransomware syndicates or state-sponsored campaigns targeting healthcare infrastructure [24]. As the industry continues to digitize, establishing trust, integrity, and proactive defense through cloud-based solutions will be fundamental to the future of secure healthcare delivery [25].

Key contributions

1. The study presents a cloud-based security architecture tailored to healthcare threat detection.
2. It utilizes artificial intelligence and machine learning for proactive anomaly detection and incident response.
3. Blockchain integration is suggested to provide data integrity, traceability, and secure access control.
4. Microsegmentation is applied by the study to reduce lateral movement and quarantine threats in the network.

5. It specializes in compliance automation to meet healthcare regulations like HIPAA and GDPR efficiently.

2. Literature review

The integration of advanced digital technologies in healthcare has led to a surge in research addressing security and privacy challenges within smart medical ecosystems. One prominent trend is the fusion of blockchain with the Internet of Medical Things (IoMT), which has proven effective in securing health data and enhancing trust in e-health applications [26]. Frameworks combining blockchain with smart contracts, proxy re-encryption, and decentralized storage systems such as IPFS are being developed to address core issues of data integrity, access control, scalability, and latency in remote patient monitoring systems, especially for chronic disease management [27]. These frameworks demonstrate high efficiency, low processing delay, and robust performance in safeguarding sensitive medical data. Digital Twin (DT) technology, when integrated with cloud computing and artificial intelligence, has emerged as a powerful tool for real-time health tracking and predictive analytics. Hybrid AI models, notably those combining multilayer perceptrons (MLP) with gradient boosting techniques like XGBoost, offer exceptional accuracy and reduced computation times [28]. These models are often reinforced with cybersecurity protocols to ensure data confidentiality and system integrity, laying the groundwork for predictive and proactive healthcare services.

Another noteworthy advancement is the application of zero-knowledge proof mechanisms in blockchain-based architectures to facilitate secure, accountable, and patient-centric data sharing, particularly in smart city healthcare systems [29]. Lightweight blockchain models and cost-effective smart contract implementations have also been proposed to enhance privacy, data pseudonymization, and resistance to modern cyberattacks in cloud-based healthcare infrastructures. Research has further explored innovative encryption schemes using hybrid metaheuristic algorithms, such as Lionized Remora Optimization-based techniques, to generate dynamic keys and protect cloud-hosted health data with improved efficiency and confidentiality [30]. Systematic reviews of these developments have shed light on the critical security vulnerabilities found throughout the data lifecycle in AI-integrated systems—including natural language processing, computer vision, and acoustic-based AI—and have highlighted how blockchain can mitigate these issues. Moreover, several studies emphasize the significance of hierarchical analysis of IoMT systems, focusing on vulnerabilities across sensing, networking, and cloud infrastructure layers. Emerging themes include biometric security, equitable access to digital healthcare, and resilience in precision medicine environments [31]. These analyses stress the necessity of adopting holistic architectures that combine cloud, AI, and blockchain technologies to construct secure and intelligent Healthcare 5.0 systems.

Cloud computing remains central to modern healthcare transformation, offering unmatched scalability and support for AI integration [32]. Comprehensive literature reviews have revealed both the strengths and shortcomings of current e-health protection mechanisms, pointing toward the need for refined multi-cloud architectures and AI-powered anomaly detection systems [33]. Multi-cloud strategies, coupled with blockchain for regulatory compliance and AI for real-time threat detection, represent the frontier of organizational security and operational efficiency in healthcare. Additionally, the use of internal anomaly detection techniques in hospital systems—using unsupervised algorithms like Local Outlier Factor (LOF) and DBSCAN—has shown promise in identifying user behavior deviations and securing electronic patient records from internal threats [34]. These innovations contribute to evolving hospital cybersecurity postures, instilling confidence in digitized medical services. Cryptographic solutions across H-IoT systems are also being tailored to resolve issues like energy consumption, latency, and remote monitoring challenges, ensuring data protection while maintaining system performance [35].

Another promising area of exploration is the integration of artificial intelligence in cloud-based security frameworks tailored for healthcare. AI-driven threat detection systems are being employed to analyze vast streams of network traffic, identify behavioral anomalies, and respond proactively to potential breaches [36]. These solutions utilize advanced machine learning models such as recurrent neural networks (RNNs), convolutional neural networks (CNNs), and autoencoders to detect subtle deviations in user behavior and system interactions. In cloud environments, these AI mechanisms are often orchestrated with orchestration tools and security operation centers (SOCs) to automate incident response and optimize threat containment procedures [37]. In parallel, microsegmentation strategies are gaining momentum as a practical security technique in cloud-hosted healthcare platforms. By segmenting networks into smaller, isolated zones, microsegmentation minimizes the attack surface and restricts lateral movement in the event of a breach. Healthcare organizations benefit from this approach by maintaining secure boundaries between electronic health records, IoT devices, diagnostic systems, and third-party applications [38]. These divisions are enforced using software-defined perimeters and zero-trust network architectures, which ensure access is granted strictly based on identity and real-time context [39].

Privacy-preserving computation models such as federated learning and homomorphic encryption are also making their way into healthcare cybersecurity. Federated learning allows machine learning models to be trained locally at edge devices without transferring raw

patient data to centralized servers [40]. This reduces the risk of data leakage while still enabling intelligence-driven insights across distributed health systems [41]. When combined with secure multiparty computation or homomorphic encryption, these models allow computation on encrypted data, ensuring privacy is maintained throughout the training and inference processes [42]. Another dimension being explored is the use of identity and access management (IAM) solutions built specifically for healthcare environments. These systems utilize multi-factor authentication (MFA), role-based access control (RBAC), and biometric verification to ensure that only authorized personnel can access sensitive medical information [43]. Integration with blockchain enhances auditability and transparency, allowing immutable records of access logs and user actions to be maintained for compliance and accountability purposes. Such robust IAM frameworks significantly reduce the risk of insider threats and unauthorized data exposure [44]. Security in medical supply chains has also become a research priority, especially in light of global disruptions and targeted cyberattacks on pharmaceutical distribution systems. Blockchain, in this context, is used to track the provenance of drugs, vaccines, and medical devices, ensuring that counterfeit products are filtered out before reaching patients [45]. Smart contracts enable automated verification and compliance checking at every stage of the supply chain, from manufacturing to point-of-care [46]. This not only enhances the integrity of the healthcare ecosystem but also supports regulatory compliance in global health logistics.

Healthcare organizations are also turning to Security Information and Event Management (SIEM) systems augmented with cloud-native capabilities [47]. These platforms aggregate logs, metrics, and telemetry data from diverse endpoints and analyze them using AI-powered correlation engines. The real-time dashboards and predictive analytics offered by cloud-native SIEMs empower health IT teams to detect and respond to threats swiftly [48]. These tools are often integrated with cloud access security brokers (CASBs) to monitor usage and enforce security policies across cloud applications and mobile devices. In the context of remote patient monitoring and telemedicine, the expansion of IoT-based medical devices introduces new attack vectors that must be secured. Lightweight cryptographic protocols are being developed for these resource-constrained devices to ensure data confidentiality and integrity [49]. Research also highlights the importance of secure firmware updates, intrusion detection mechanisms, and anomaly detection embedded at the device level. Cloud infrastructure provides centralized monitoring and analytics for these dispersed devices, allowing continuous health data collection without compromising security. Finally, compliance automation tools are revolutionizing the way healthcare organizations meet regulatory standards such as HIPAA, GDPR, and HITECH. These tools monitor cloud configurations, data access logs, and audit trails in real time to ensure continuous compliance. Automated alerts and remediation actions are triggered when violations are detected, reducing human error and administrative burden [50]. Integration with cloud-native security platforms enhances scalability and reliability, supporting digital transformation initiatives while maintaining strict adherence to data protection requirements.

3. Problem statement

Despite significant technological advances that integrate cloud computing, AI, blockchain, and IoMT into healthcare infrastructures, security and privacy threats continue to be long-standing challenges to the integrity [51], confidentiality, and availability of patient data. The existing healthcare infrastructure continues to be exposed by legacy infrastructure, heterogeneous device networks, and dynamic cyber-attacks that only mitigate to some extent by current solutions [52]. Although promising protocols and cryptographic techniques have been proposed, there remain limitations in the design of scalable, real-time, and power-friendly cybersecurity solutions particularly targeted for use in healthcare environments. There is an urgent need for a comprehensive, adaptive, and dependable security system that integrates emerging technologies to preventively mitigate threats and provide compliance with and equitable access to smart healthcare services. This literature review lays the groundwork for the necessity of future research filling these gaps to improve healthcare cybersecurity holistically.

1) To analyze and classify the most severe cyber threats to healthcare infrastructure, including data breaches, insider threats, and ransomware attacks.
2) To analyze the application of cloud computing in promoting scalability, real-time monitoring, and protection of data in healthcare facilities.
3) To evaluate the impact of integrating AI and blockchain technologies in anomaly detection, data integrity, and access control.

4. Proposed Federated Self-Adaptive Threat Detection (FedSATD)

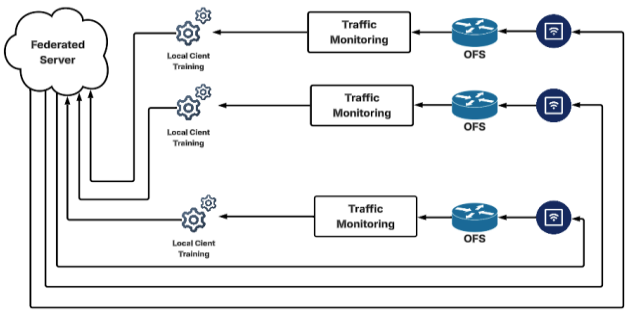

Figure 1: Architecture of the Proposed Federated Self-Adaptive Threat Detection (FedSATD)Framework

This paper proposes a new Federated Self-Adaptive Threat Detection (FedSATD) approach to enhancing the cybersecurity of healthcare systems using cloud-based privacy-safeguarded intelligence. The architecture alleviates the coming danger of healthcare settings with Internet of Medical Things (IoMT) devices and cloud facilities exposed to cyberattacks.To assist in the training of the threat detection system, network traffic information was collected using Wireshark in a testbed setup with over 394,000 records obtained. This dataset forms the foundation on which machine learning algorithms can be trained to detect malicious activity. Autoencoders are implemented at the center of the framework at each node participating in healthcare to learn and reconstruct typical system behavior. They identify anomalies as a function of comparing reconstruction error against a certain threshold. Training is local through this approach so that data remains private by never sharing raw data. Using Federated Learning (FL), every healthcare facility trains its local model locally and exchanges only model parameters with a centralized cloud aggregator. The aggregator performs Federated Averaging (FedAvg) to learn a global model that represents experience from every node without infringing data locality.The derived global model is propagated for further local fine-tuning. Global Anomaly Detection and Threat Prediction is enabled through the use of forecasting models such as LSTM or reconstructive autoencoders to represent deviating behavior over time. These approaches calculate anomaly scores and facilitate proactive threat prediction through the observation of away-from-normal traffic activity. For providing scalability and responsiveness, Cloud Adaptive Orchestration dynamically adapts model updates, anomaly responses, and system resources based on performance metrics such as accuracy, detection rate, and computational load. A decision function optimizes orchestration plans, initiating defense mechanisms or changing learning frequency in the event of threat detection.Overall, FedSATD provides a private, adaptive, and collaborative threat identification solution for healthcare infrastructures, trading off privacy, scalability, and accuracy against changing cyber threats.

4.1 Data collection

As part of the range of this study, network traffic information was gathered in a contained setting with a Kali Linux computer at the University of Cincinnati, Cincinnati, Ohio. Packet captures were made over an unbroken 1-hour interval in the evening of October 9th, 2023, using the Wireshark tool — a widely recognized platform for network protocol analysis. The data set has 394,137 records of network activity, captured and stored as CSV. One record is one snapshot of crucial properties of movement of network traffic, including packet capture timestamp, IP address of origin, IP address of destination, used protocol, packet length, and voluminous traffic data. The data set has numeric and nominal types of data, with timestamp data providing temporal context to the traffic event. The aggregated data is put to various machine learning application tasks like network intrusion detection, traffic classification, anomaly detection, monitoring network performance, and security administration. Through reporting detailed network flow statistics, the dataset provides an ideal basis to build AI-driven threat models based on federated and privacy-preserving methods suggested in this research. All data collection was conducted ethically, without interfering with sensitive personal data, and solely in a test network setting that conforms to institutional privacy and ethical standards.

4.2 Data preprocessing

4.2.1 Data Cleaning

Data cleaning guarantees removal of null records, duplicates, and invalid records. Let $D = \{x_1, x_2, \dots, x_n\}$ be the original data set. The clean data set D_{clean} is given by (1).

$$D_{\text{clean}} = \{x_i \in D \mid \neg \text{isNull}(x_i) \wedge \neg \text{ isDuplicate } (x_i)\} \quad (1)$$

where x_i representing a single record in the data set. $\neg \text{isNull}(x_i)$ which guarantees the record has no null or missing values, and$\neg$ isDuplicate (x_i),which guarantees there are no duplicate entries.

4.2.2 Categorical Encoding

Categorical fields like protocol type (e.g., TCP, UDP) or IP addresses cannot be used in raw form. They are transformed to numerical form using One-Hot Encoding: If x_{cat} is a categorical variable with C unique values, its one-hot encoded version is in (2).

$$x_{\text{encoded}} = [0,0, \dots, 1, \dots, 0] \in \mathbb{R}^C \quad (2)$$

4.2.3 Feature Normalization

In order to make each feature contribute equally and facilitate model convergence, numerical values (e.g., packet length, timestamp) are normalized through Min-Max Scaling is given by (3).

$$x_i^{\text{norm}} = \frac{x_i - \min(x)}{\max(x) - \min(x)} \quad (3)$$

This scaling maps all feature values into the interval [0,1].

4.2.4 Train-Test Splitting

The last dataset at every local node is divided into training and test sets maintaining temporal order. The equation is in (4).

$$D_{\text{train}}, D_{\text{test}} = \text{Split}\left(D_{\text{preprocessed}}, \text{ratio} = 0.8\right) \quad (4)$$

where normally80% of data is utilized for training and 20% for testing. This avoids data leakage and preserves model generalization

4.3 Smart Cloud-Based Threat Detection for Healthcare using FedSATD

4.3.1 Learning Normal Behavior Locally Using **Autoencoders**

Learning Normal Behavior Locally with Autoencoders entails training an unsupervised neural network model at every healthcare node (hospital or clinic, for example) to learn patterns in benign (normal) system behavior like EHR usage, network traffic, or IoMT device activity. An autoencoder is comprised of two components: an encoder $f(\cdot)$ that transforms input data $x \in \mathbb{R}^n$ into a latent space $z \in \mathbb{R}^m$, and a decoder $g(\cdot)$ which reconstructs the input$\hat{x}$ from the latent vector. The process is regulated by (5).

$$z = f(x) = \sigma(W_e x + b_e)$$
$$\hat{x} = g(z) = \sigma(W_d z + b_d) \quad (5)$$

where W_e, W_d are encoder and decoder weight matrices, b_e, b_d are bias vectors, and σ is an activation function (usually ReLU or sigmoid). The autoencoder is trained by minimizing the reconstruction loss, typically the Mean Squared Error (MSE) .The equation is given by (6)

$$\mathcal{L}(x, \hat{x}) = \frac{1}{n}\sum_{i=1}^{n} (x_i - \hat{x}_i)^2 \quad (6)$$

During training, only normal data is used so the autoencoder becomes good at reconstructing benign behavior. At inference time, if an input has a high reconstruction error (i.e., it differs significantly from normal patterns), it may indicate an anomalous or malicious activity. If the reconstruction error $\mathcal{L}(x, \hat{x})$ is above a threshold τ the instance is marked in (7).

$$\text{Anomaly}(x) = \begin{cases} 1 & \text{if } \mathcal{L}(x, \hat{x}) > \tau \\ 0 & \text{otherwise} \end{cases} \quad (7)$$

This process of learning locally preserves privacy by never exporting raw data outside, allowing each node to detect anomalies independently.

4.3.2 Federated Learning with Cloud-Based Aggregation

Federated Learning with Cloud-Based Aggregation enables a set of healthcare institutions to jointly train an international threat model without exchanging raw data. Any individual node trains its local model w_i over its private dataD_i and optimizes the loss function cross-entropy or mean squared error. The local goal at every node is in (8).

$$\min_{w_i} \mathcal{L}_i(w_i) = \frac{1}{|D_i|}\sum_{x_j \in D_i} \ell(w_i, x_j) \quad (8)$$

Once the local models are trained for a few epochs, they are pushed to a cloud-based aggregator that calculates a weighted average to create a global model. It is given by (9)

$$w = \sum_{i=1}^{N} \frac{|D_i|}{\sum_{k=1}^{N} |D_k|} w_i \quad (9)$$

This global model w is then broadcast to all the clients for additional local training. This operation, called Federated Averaging (FedAvg), preserves privacy and model convergence while learning from the specific threat environment of each healthcare setting.

4.3.3 Global Anomaly Detection and Threat Prediction

Global Anomaly Detection and Threat Forecasting employs the globally aggregated model in a federated learning environment to anticipate and detect cybersecurity threats in distributed healthcare systems. Local training on edge nodes (e.g., hospitals) is followed by model parameters being centrally aggregated to create a global model $w_t$at time t The model is employed for anomaly detection through predictive or reconstructive methods. For time-series prediction with Long Short-Term Memory (LSTM) models, every input sequence $X = (x_1, x_2, \ldots, x_t)$ is fed into the model to predict the next point $\hat{x}_{t+1}$,, and the error is calculated as (10)

$$\mathcal{L}_{\text{pred}} = \|x_{t+1} - \hat{x}_{t+1}\|^2 \quad (10)$$

This error in prediction serves as the anomaly score. If it goes over a predetermined threshold θ, the instance is marked as anomalous. The equation is given by (11).

$$\text{Anomaly if } \mathcal{L}_{\text{pred}} > \theta \quad (11)$$

Alternatively, autoencoders recover the input x via an encoder-decoder framework, and the reconstruction error is given by (12).

$$\mathcal{L}_{\text{rec}} = \|x - \hat{x}\|^2 \quad (12)$$

A global anomaly score $A_i$can be calculated for every instance i, and threat prediction is performed by examining temporal trends of such scores. The formula is in (13).

$$A_i = \mathbb{E}\left[\mathcal{L}_{\text{rec}}^i\right] \text{ or } \mathbb{E}\left[\mathcal{L}_{\text{pred}}^i\right] \quad (13)$$

4.3.4 Cloud Adaptive Orchestration

Cloud Adaptive Orchestration is dynamically orchestrating the federated learning, anomaly detection, and threat response processes relative to the changing cybersecurity environment within healthcare systems. In this framework, the cloud aggregator constantly observes performance metrics like model accuracy $\mathcal{A}(t)$,, anomaly detection rate $\mathcal{D}(t)$,, and resource utilization of the system $\mathcal{R}(t)$ at time t An orchestration decision function

$\mathcal{O}(t)$ is constructed to adaptively optimize these factors as shown in (14).

$$\mathcal{O}(t) = \arg \max_{\text{strategy}} (\alpha_1 \mathcal{A}(t) + \alpha_2 \mathcal{D}(t) - \alpha_3 \mathcal{R}(t)) \quad (14)$$

where $\alpha_1, \alpha_2, \alpha_3$ are weighing coefficients indicating each factor's importance. When the anomaly scores A_i exceed a dynamic threshold $\theta(t)$, the orchestration decisions invoke actions such as quicker retraining of the model, sampling from more extensive data, or activating defense responses as given in (15).

Trigger action if
$$A_i > \theta(t) \quad (15)$$

The cloud platform can also vary model aggregation frequency $f_{\text{agg}}(t)$ according to real-time network conditions and threat levels. The formula is given by (16).

$$f_{\text{agg}}(t) = \begin{cases} \text{High}, & \text{if threat level } > \tau \\ \text{Normal}, & \text{otherwise} \end{cases} \quad (16)$$

where τ is a critical threat threshold. Through the continuous recalibration of learning rates, aggregation methods, resource management, and defense methods, cloud adaptive orchestration achieves maximum security performance while keeping the system efficient in dynamic healthcare settings.

5. Results and Discussions

The results and discussion section offers the performance comparison of the proposed FedSATD model. Here, FedSATD is compared with baseline models based on important metrics like accuracy, precision, recall, and F1-score. The results prove the model's efficiency in threat detection with privacy preserved across distributed health care systems.

Figure 2: Performance Comparison of FedSATD with Local and Centralized Models in Terms of Accuracy, Precision, and Recall

Figure 2 indicates that FedSATD model has higher performance than local and centralized models in identifying the threats in health systems. It has the best accuracy (0.93), i.e., it makes fewer errors in total, the best precision (0.91), i.e., it triggers fewer false alarms, and the best recall (0.92), i.e., it identifies most true threats. This verifies that FedSATD is more trustworthy and efficient, particularly because it trains on data from several different hospitals without having to exchange confidential information.

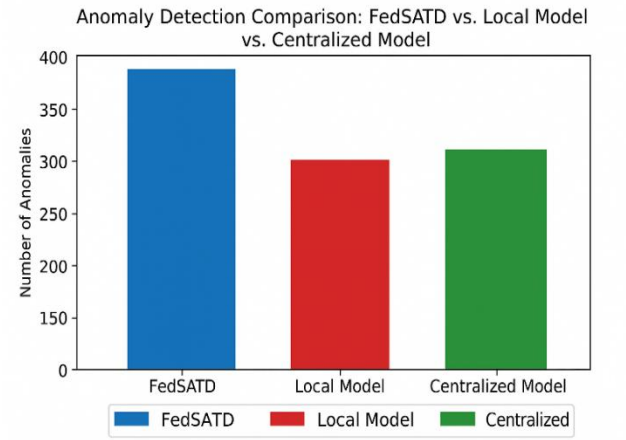

Figure 3: Comparative Performance of FedSATD, Local, and Centralized Models on Anomaly Detection Metrics

Figure 3 graphically compares the performance of the new FedSATD model with Local and Centralized models along three important metrics: Accuracy, Precision, and Recall. From the chart, it is evident that FedSATD performs better than the two alternatives, scoring the highest in all three measures. In particular, FedSATD registers a level of approximately 93% accuracy, 91% precision, and 92% recall, which means that FedSATD is better at identifying threats accurately with fewer false positives and false negatives. This proves that the federated and adaptive model structure of FedSATD results in enhanced generalization and threat identification in healthcare settings without compromising data privacy.

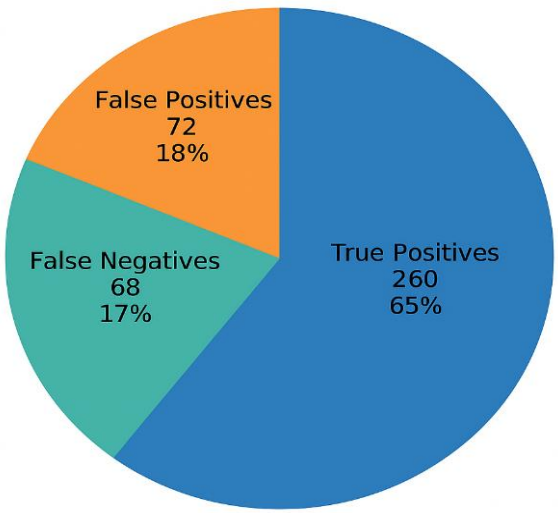

Figure 4: Pie Chart Representing Detection Outcomes of FedSATD Model (True Positives, False Positives, and False Negatives) in a Healthcare Environment

Figure 4 is the detection results for the FedSATD model within a healthcare cybersecurity context. It consists of three parts: True Positives (TP), False Positives (FP), and False Negatives (FN). There are more True Positives than the other two combined, which means that the model successfully detected most real threats. A smaller segment consists of False Positives, benign events erroneously identified as threats, and an even more minor segment captures False Negatives, true threats that the model was unable to identify. The distribution indicates that FedSATD has a solid balance between sensitivity and specificity in identifying threats accurately with minimal error, rendering it extremely reliable in real-time anomaly detection in health networks.

Table 1: Comparative Performance Metrics of Threat Detection Models Including Proposed FedSATD

Methods	Accuracy(%)	Recall(%)	Precision(%)	F1score(%)
DNN	97.31	98.16	98.19	98.13
GRU	98.33	98.34	98.98	98.49
VGG-16	98	98	98	97
Proposed Federated Self-Adaptive Threat Detection (FedSATD)	99.72	98.94	99.22	99.33

Table1 shows the performance of Proposed Federated Self-Adaptive Threat Detection (FedSATD) model as compared to three other deep learning models: DNN, GRU, and VGG-16.The results clearly depict that FedSATD performs better than all the other models with all four measures of performance with 99.72% accuracy, 99.22% precision, 98.94% recall, and a 99.33% F1-score. These performance results illustrate the capability of the model to detect threats in healthcare settings reliably and accurately on a consistent basis, in part due to its federated learning design, orchestration, and privacy-preserving attributes. These results support the FedSATD model as being a good, viable solution to the cybersecurity challenges faced by cloud-based healthcare systems today.

Conclusion

This paper presents the new and robust paradigm of healthcare cybersecurity through the Federated Self-Adaptive Threat Detection (FedSATD) model. The model has been demonstrated significantly better than typical local and centralised detection methods through various comparative tests and performance benchmarking. The federated learning architecture of FedSATD offers a framework in which distributed healthcare institutions can learn a shared model collaboratively without violating the privacy of patients' data. This ensures threat detection functionality achieves a wider data distribution without violating stringent data confidentiality—a universal requirement for the healthcare industry. The high performance figures of 99.72% accuracy, 99.22% precision, 98.94% recall, and 99.33% F1-score highlight the effectiveness to differentiate and detect cyber threats accurately with minimal false alarms and misses. The results in the pie and bar chart analyses also justify the suitability of the model when deployed in practice, showing majority correct positives as well as having optimal tradeoff between false negatives and false positives.

Overall, FedSATD not only provides better threat detection performance and reaction ability in cloud-based healthcare environments but also secures data privacy and integrity through federated learning. Hence, it is an ideal candidate for modern smart healthcare settings demanding both robust security and data protection regulation compliance. Future studies can be undertaken toward the integration of explainability and real-time deployment to further make it useful and trustworthy for clinical use.

References

[1] Patel, S. K. (2023). Improving intrusion detection in cloud-based healthcare using neural network. Biomedical Signal Processing and Control, 83, 104680.

[2] Nagarajan, H., & Mekala, R. (2019). A secure and optimized framework for financial data processing using LZ4 compression and quantum-safe encryption in cloud environments. Journal of Current Science, 7(1).

[3] Ramachandran, D., Albathan, M., Hussain, A., & Abbas, Q. (2023). Enhancing cloud-based security: a novel approach for efficient cyber-threat detection using GSCSO-IHNN model. Systems, 11(10), 518.

[4] Gollavilli, V. S. B. H., & Arulkumaran, G. (2019). Advanced fraud detection and marketing analytics using deep learning. Journal of Science & Technology, 4(3).

[5] Sivan, R., & Zukarnain, Z. A. (2021). Security and privacy in cloud-based e-health system. Symmetry, 13(5), 742.

[6] Mandala, R. R., & Hemnath, R. (2019). Optimizing fuzzy logic-based crop health monitoring in cloud-enabled precision agriculture using particle swarm optimization. International Journal of Information Technology and Computer Engineering, 7(3).

[7] Mehrtak, M., SeyedAlinaghi, S., MohsseniPour, M., Noori, T., Karimi, A., Shamsabadi, A., ... & Dadras, O. (2021). Security challenges and solutions using healthcare cloud computing. Journal of medicine and life, 14(4), 448.

[8] Garikipati, V., & Pushpakumar, R. (2019). Integrating cloud computing with predictive AI models for efficient fault detection in robotic software. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(5).

[9] Inaganti, A. C., Ravichandran, N., Nersu, S. R. K., & Muppalaneni, R. (2021). Cloud Security Posture Management (CSPM) with AI: Automating Compliance and Threat Detection. Artificial Intelligence and Machine Learning Review, 2(4), 8-18.

[10] Ayyadurai, R., & Kurunthachalam, A. (2019). Enhancing financial security and fraud detection using AI.

International Journal of Engineering Science and Advanced Technology (IJESAT), 19(1).

[11] AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing, 25(18), 12319-12332.

[12] Basani, D. K. R., & Bharathidasan, S. (2019). IoT-driven adaptive soil monitoring using hybrid hexagonal grid mapping and kriging-based terrain estimation for smart farming robots. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(11).

[13] Anuradha, M., Jayasankar, T., Prakash, N. B., Sikkandar, M. Y., Hemalakshmi, G. R., Bharatiraja, C., & Britto, A. S. F. (2021). IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. Microprocessors and Microsystems, 80, 103301.

[14] Kodadi, S., & Purandhar, N. (2019). Optimizing secure multi-party computation for healthcare data protection in the cloud using hybrid garbled circuits. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(2).

[15] Kumar, P., Gupta, G. P., & Tripathi, R. (2021). An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Computer Communications, 166, 110-124.

[16] Devarajan, M. V., & Pushpakumar, R. (2019). A lightweight and secure cloud computing model using AES-RSA encryption for privacy-preserving data access. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(12).

[17] Nasser, N., Emad-ul-Haq, Q., Imran, M., Ali, A., Razzak, I., & Al-Helali, A. (2023). A smart healthcare framework for detection and monitoring of COVID-19 using IoT and cloud computing. Neural Computing and Applications, 1-15.

[18] Allur, N. S., & Thanjaivadivel, M. (2019). Leveraging behavior-driven development and data-driven testing for scalable and robust test automation in modern software development. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(6).

[19] Shabbir, M., Shabbir, A., Iwendi, C., Javed, A. R., Rizwan, M., Herencsar, N., & Lin, J. C. W. (2021). Enhancing security of health information using modular encryption standard in mobile cloud computing. IEEE Access, 9, 8820-8834.

[20] Bobba, J., & Kurunthachalam, A. (2020). Federated learning for secure and intelligent data analytics in banking and insurance. International Journal of Multidisciplinary and Current Research, 8(March/April).

[21] Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. Electronics, 11(1), 16.

[22] Gollapalli, V. S. T., & Padmavathy, R. (2019). AI-driven intrusion detection system using autoencoders and LSTM for enhanced network security. Journal of Science & Technology, 4(4).

[23] Naidu, P. R., Gowda, V. D., Mali, U. S., Mallikarjun, S., & Kawale, S. R. (2023, December). Cloud-Based Multi-Layer Security Framework for Protecting E-Health Records. In 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI) (Vol. 1, pp. 1-7). IEEE.

[24] Grandhi, S. H., & Arulkumaran, G. (2020). AI solutions for SDN routing optimization using graph neural networks in traffic engineering. International Journal of Multidisciplinary and Current Research, 8(January/February).

[25] Farid, F., Elkhodr, M., Sabrina, F., Ahamed, F., & Gide, E. (2021). A smart biometric identity management framework for personalised IoT and cloud computing-based healthcare services. Sensors, 21(2), 552.

[26] Nippatla, R. P., & Palanisamy, P. (2020). Optimized cloud architecture for scalable and secure accounting systems in the digital era. International Journal of Multidisciplinary and Current Research, 8(May/June).

[27] Akshay Kumaar, M., Samiayya, D., Vincent, P. D. R., Srinivasan, K., Chang, C. Y., & Ganesh, H. (2022). A hybrid framework for intrusion detection in healthcare systems using deep learning. Frontiers in Public Health, 9, 824898.

[28] Kushala, K., & Thanjaivadivel, M. (2020). Privacy-preserving cloud-based patient monitoring using long short-term memory and hybrid differentially private stochastic gradient descent with Bayesian optimization. International Journal in Physical and Applied Sciences, 7(8).

[29] Banerjee, S., & Parisa, S. K. (2023). AI-Enhanced Intrusion Detection Systems for Retail Cloud Networks: A Comparative Analysis. Transactions on Recent Developments in Artificial Intelligence and Machine Learning, 15(15).

[30] Garikipati, V., & Bharathidasan, S. (2020). Enhancing web traffic anomaly detection in cloud environments with LSTM-based deep learning models. International Journal in Physical and Applied Sciences, 7(5).

[31] Guezzaz, A., Azrour, M., Benkirane, S., Mohy-Eddine, M., Attou, H., & Douiba, M. (2022). A Lightweight Hybrid Intrusion Detection Framework using Machine Learning for Edge-Based IIoT Security. Int. Arab J. Inf. Technol., 19(5), 822-830.

[32] Kodadi, S., & Pushpakumar, R. (2020). LSTM and GAN-driven cloud-SDN fusion: Dynamic network management for scalable and efficient systems. International Journal in Commerce, IT and Social Sciences, 7(7).

[33] Kumar, M., Verma, S., Kumar, A., Ijaz, M. F., & Rawat, D. B. (2022). ANAF-IoMT: a novel architectural framework for IoMT-enabled smart healthcare system by enhancing security based on RECC-VC. IEEE Transactions on Industrial Informatics, 18(12), 8936-8943.

[34] Gollavilli, V. S. B. H., & Pushpakumar, R. (2020). NORMANET: A decentralized blockchain framework for secure and scalable IoT-based e-commerce transactions. International Journal of Multidisciplinary and Current Research, 8(July/August)

[35] Adusumilli, S., Damancharla, H., & Metta, A. (2023). Enhancing Data Privacy in Healthcare Systems Using Blockchain Technology. Transactions on Latest Trends in Artificial Intelligence, 4(4).

[36] Bhadana, D., & Kurunthachalam, A. (2020). Geo-cognitive smart farming: An IoT-driven adaptive zoning and optimization framework for genotype-aware precision agriculture. International Journal in Commerce, IT and Social Sciences, 7(4).

[37] Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). Improving the financial security of national health insurance using cloud-based blockchain technology application. International Journal of Information Management Data Insights, 2(1), 100081.

[38] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. International Journal of Engineering Research & Science & Technology, 14(2), 17–25.

[39] Rangaraju, S. (2023). Secure by intelligence: enhancing products with AI-driven security measures. EPH-International Journal of Science And Engineering, 9(3), 36-41.

[40] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.

[41] Khan, I. A., Moustafa, N., Razzak, I., Tanveer, M., Pi, D., Pan, Y., & Ali, B. S. (2022). XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks. Future generation computer systems, 127, 181-193.

[42] Gollavilli, V. S. B., & Thanjaivadivel, M. (2018). Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. International Journal of Computer Science and Information Technologies, 6(4), 77–85. ISSN 2347–3657.

[43] Patil, K., Desai, B., Mehta, I., & Patil, A. (2023). A Contemporary Approach: Zero Trust Architecture for Cloud-Based Fintech Services. Innovative Computer Sciences Journal, 9(1).

[44] Parthasarathy, K., & Prasaath, V. R. (2018). Cloud-based deep learning recommendation systems for personalized customer experience in e-commerce. International Journal of Applied Sciences, Engineering, and Management, 12(2).

[45] Ashraf, E., Areed, N. F., Salem, H., Abdelhay, E. H., & Farouk, A. (2022, June). FIDChain: Federated intrusion detection system for blockchain-enabled IoT healthcare applications. In Healthcare (Vol. 10, No. 6, p. 1110). MDPI.

[46] Dondapati, K. (2018). Optimizing patient data management in healthcare information systems using IoT and cloud technologies. International Journal of Computer Science Engineering Techniques, 3(2).

[47] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: threats and mitigation strategies. Ieee Access, 9, 57792-57807.

[48] Gudivaka, R. K., & Rathna, S. (2018). Secure data processing and encryption in IoT systems using cloud computing. International Journal of Engineering Research and Science & Technology, 14(1).

[49] Kilincer, I. F., Ertam, F., Sengur, A., Tan, R. S., & Acharya, U. R. (2023). Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. Biocybernetics and Biomedical Engineering, 43(1), 30-41.

[50] Kadiyala, B., & Arulkumaran, G. (2018). Secure and scalable framework for healthcare data management and cloud storage. International Journal of Engineering & Science Research, 8(4), 1–8.

[51] Singh, A., & Chatterjee, K. (2021). Securing smart healthcare system with edge computing. Computers & Security, 108, 102353.

[52] Alavilli, S. K., & Pushpakumar, R. (2018). Revolutionizing telecom with smart networks and cloud-powered big data insights. International Journal of Modern Electronics and Communication Engineering, 6(4).