International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Design of an Iterative Method for Secure and Private IoT Healthcare Data Management Using Encrypted Federated Learning and AI-Driven Anomaly Detection

Sivanagaraju Vallabhuni[1], **Kumar Debasis***[2]

Submitted:10/03/2024 **Revised**: 25/04/2024 **Accepted**: 02/05/2024

Abstract: The escalating need for robust, privacy-preserving IoT Healthcare data management systems has prompted the exploration of security models that ensure non-mutability and stringent security. Traditional methods often fall short in effectively balancing privacy, accessibility, and computational efficiency. Addressing these limitations, this paper introduces a novel framework utilizing encrypted federated learning, access control, anomaly detection, and predictive analytics tailored for IoT Healthcare applications. Our proposed model comprises four innovative methods: Encrypted Federated Learning with Homomorphic Encryption (EFLHE), Reinforcement Learning-Driven Access Control (RLAC), AI-Driven Anomaly Detection with Autoencoder Fusion (AIDA), and timestamp Series-Based IoT Healthcare Forecasting with Grey Wolf Optimizer (TS-GWO). EFLHE harnesses homomorphic encryption to train machine learning models on encrypted data across multiple nodes, preserving patient confidentiality while enabling decentralized computation. This method overcomes the existing challenges of data privacy and computational overhead associated with traditional federated learning systems. Furthermore, RLAC employs reinforcement learning to dynamically optimize access control policies via smart contracts based on real-time interaction and system feedback, thus enhancing both security and user experience. This adaptive control mechanism significantly outperforms static access control systems in responding to evolving security threats and user requirements. In parallel, AIDA integrates autoencoders with AI-driven models to meticulously detect anomalies and potentially fraudulent activities within the network. By learning standard transaction patterns and identifying deviations, AIDA provides a dual-layer security framework that significantly reduces the risk of security breaches. Lastly, TS-GWO leverages the Grey Wolf Optimizer to refine the parameters of timestamp series forecasting models. This optimization facilitates more accurate predictions regarding disease progression, treatment outcomes, and resource allocation, which are critical for proactive IoT Healthcare management. Collectively, these methods not only fortify the security and privacy of IoT Healthcare data but also enhance the operational efficiency of IoT Healthcare systems. The impacts of this work are profound, offering a scalable, secure, and efficient framework for IoT Healthcare data management that meets the rigorous demands of modern IoT Healthcare infrastructures and compliance standards. This model sets a new benchmark for privacy-preserving, real-time IoT Healthcare data systems, potentially revolutionizing patient care through technologically advanced solutions that safeguard sensitive information and optimize clinical decision-making processes.

Keywords: *Security, Homomorphic Encryption, Reinforcement Learning, Anomaly Detection, Predictive Analytics*

1. Introduction

The digital transformation of IoT Healthcare systems has necessitated the development of sophisticated data management frameworks that not only ensure the integrity and security of patient data but also enhance the accessibility and efficiency of IoT Healthcare services. The integration of secure technology promises to revolutionize the IoT Healthcare industry by providing solutions that are inherently secure, transparent, and immutable. However, the application of security in IoT Healthcare poses unique challenges, primarily related to the privacy of sensitive patient data, the scalability of the system, and the dynamic nature of access control.

Recent advancements in cryptographic techniques and machine learning have paved the way for innovative approaches to address these challenges. Particularly, homomorphic encryption (HE) and federated learning (FL) have emerged as pivotal technologies enabling privacy-preserving computations on encrypted data distributed across multiple nodes. Despite their potential, traditional FL and HE are impeded by significant computational overhead and limited operational flexibility, which are critical in the processing of large-scale IoT Healthcare data samples.

To overcome these limitations, this study introduces an integrated model that leverages encrypted federated learning enhanced with homomorphic encryption (EFLHE), along with several other methodologies to ensure a robust, scalable, and privacy-centric framework. The proposed model consists of the following key components.

[1] VIT-AP University, School of Computer Science and Engineering, Amaravati, Andhra Pradesh – 522237, INDIA
ORCID ID: 0009-0000-1316-5814
[2] VIT-AP University, School of Computer Science and Engineering, Amaravati, Andhra Pradesh – 522237, INDIA
ORCID ID: 0000-0002-0352-3267
** Corresponding Author Email: kumar.debasis@vitap.ac.in*

Encrypted Federated Learning with Homomorphic Encryption (EFLHE): This method allows for the training of machine learning models on encrypted data, ensuring that patient privacy is maintained without compromising the ability to perform complex computational tasks across distributed networks. By utilizing HE, EFLHE facilitates local updates at nodes on encrypted data, which are then aggregated to refine the global model, thereby minimizing exposure of sensitive information and reducing bandwidth requirements compared to conventional FL.

• **Reinforcement Learning-Driven Access Control (RLAC):** Adaptive access control mechanisms are crucial for maintaining the security of IoT Healthcare databases. RLAC employs reinforcement learning to dynamically adjust access permissions based on real-time data interactions and system feedback, optimizing both security measures and user experience. This approach allows the system to evolve its access protocols proactively, addressing the limitations of static policy frameworks that fail to react to new threats and usage patterns.

• **AI-Driven Anomaly Detection with Autoencoder Fusion (AIDA):** Anomaly detection is critical in preempting fraudulent activities and potential data breaches. AIDA combines deep learning autoencoders with supplementary AI-driven models to monitor and analyze deviations from normal transaction patterns. This dual-layered approach enhances the system’s ability to detect and respond to anomalies in real time, thereby significantly strengthening the network's security.

• **Time Series-Based IoT Healthcare Forecasting with Grey Wolf Optimizer (TS-GWO):** Accurate forecasting in IoT Healthcare can drastically improve patient outcomes and optimize resource allocation. TS-GWO incorporates the Grey Wolf Optimizer to enhance the performance of timestamp series forecasting models, such as ARIMA and LSTM, tailored for IoT Healthcare data samples. This method efficiently handles the variability and complexity of medical datasets, yielding more precise predictions for disease progression and treatment efficacy.

The integration of these methodologies into a unified model not only addresses the privacy and security concerns associated with traditional IoT Healthcare data systems but also introduces a level of computational efficiency and adaptability required for modern IoT Healthcare infrastructures & scenarios. This paper elaborates on the design, implementation, and potential impacts of this innovative framework, setting a new standard for the secure and efficient management of IoT Healthcare information sets.

1.1. Motivation & Contributions

The burgeoning demand for advanced IoT Healthcare data management systems is driven by the increasing need for security, privacy, and efficiency in processing sensitive medical information. Traditional IoT Healthcare systems often struggle with these challenges due to outdated infrastructure, lack of flexibility, and vulnerabilities to data breaches. The integration of security technology has been identified as a potent solution to these issues, offering a decentralized framework that inherently supports immutability and auditability. However, the direct application of security technology in IoT Healthcare is not devoid of limitations, particularly concerning scalability, privacy, and the real-time processing of large datasets.

Motivation

The primary motivation behind this research is twofold: to enhance the privacy and security of patient data and to improve the scalability and efficiency of IoT Healthcare data systems. Existing systems frequently compromise patient privacy during data processing and are typically static, lacking the capability to adapt to evolving access patterns and potential security threats dynamically. Moreover, the computational inefficiency of processing encrypted data on security networks underscores a critical need for optimized solutions that can handle encrypted operations at scales. These challenges necessitate a re-evaluation of traditional models and the development of a more robust framework that can accommodate the complex requirements of modern IoT Healthcare data management process.

Contributions

This study makes several significant contributions to the field of IoT Healthcare data management through the development and integration of four advanced methodologies within a security-based model.

• **Enhanced Privacy through EFLHE:** The Encrypted Federated Learning with Homomorphic Encryption (EFLHE) technique addresses the core issue of privacy. It enables machine learning models to be trained directly on encrypted data, ensuring that sensitive patient information remains secure from unauthorized access throughout the computation process. This method not only preserves privacy but also mitigates the risk of data exposure during transmission between nodes in a federated network.

• **Dynamic Access Control via RLAC:** The Reinforcement Learning-Driven Access Control (RLAC) mechanism introduces a dynamic and adaptive approach to managing user permissions and access controls. Utilizing reinforcement learning algorithms, RLAC continuously learns and optimizes access policies based on user behavior and threat levels, significantly enhancing the security and usability of the system compared to static, rule-based access controls.

• **Robust Anomaly Detection with AIDA:** The AI-Driven Anomaly Detection with Autoencoder Fusion (AIDA) provides a comprehensive solution for detecting and mitigating potential fraud and data breaches. By integrating autoencoders with additional AI-driven techniques, AIDA effectively identifies unusual patterns and suspicious activities within the network, offering a proactive security measure that adapts to new threats as they arise in real-time scenarios.

• **Accurate Predictive Analytics using TS-GWO:** The timestamp Series-Based IoT Healthcare Forecasting with Grey Wolf Optimizer (TS-GWO) exploits advanced optimization algorithms to enhance the accuracy of predictive models used in IoT Healthcare. This approach significantly improves disease forecasting, treatment outcomes, and resource allocation strategies, thereby aiding in better IoT Healthcare management and planning. These contributions collectively address the critical challenges faced by traditional IoT Healthcare data systems, offering a scalable, secure, and efficient alternative that leverages the strengths of security technology, machine learning, and modern optimization techniques. The proposed model not only enhances data security and privacy but also provides a flexible and adaptive system that can meet the demands of contemporary IoT Healthcare environments. This research paves the way for future innovations in IoT Healthcare data management and sets a benchmark for the integration of technological advancements in medical informatics in different scenarios.

2. Literature Review

The landscape of healthcare services has undergone a paradigm shift with the advent of the Internet of Things (IoT), offering unprecedented opportunities for personalized, efficient, and remote healthcare delivery. However, the integration of IoT in healthcare systems introduces numerous security challenges that must be addressed to ensure the confidentiality, integrity, and availability of sensitive medical data samples. This literature review critically examines the state-of-the-art research in securing IoT-based healthcare systems, encompassing authentication protocols, privacy preservation techniques, anomaly detection mechanisms, and resilience strategies against cyberattacks.

Wang et al. [1] conducted a security analysis of a user authentication scheme tailored for IoT-based healthcare, uncovering vulnerabilities such as session key disclosure and traceability attacks. Alladi et al. [2] proposed HARCI, a two-way authentication protocol designed for three-entity healthcare IoT networks, emphasizing physical security and privacy using physically unclonable functions (PUFs). Taimoor and Rehman [3] surveyed reliable and resilient AI and IoT-based personalized healthcare services, highlighting the importance of reliability, resilience, and sustainability in the era of healthcare 5.0. In the realm of distributed security, Zaman et al. [4] explored the application of Holochain for ensuring security in IoT healthcare, leveraging blockchain technology to protect medical data in real-time systems. Khatun et al. [5] reviewed machine learning techniques for healthcare IoT security, addressing security and privacy challenges through anomaly detection and mitigation strategies in 5G-IoT environments. Wang et al. [6] proposed a forward privacy preservation mechanism in IoT-enabled healthcare systems, focusing on encryption and privacy preservation to safeguard medical data samples. Masud et al. [7] introduced a lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare, aiming to enhance digital security and user privacy, particularly in the context of the COVID-19 pandemic. Thapliyal et al. [8] designed a robust blockchain-envisaged authenticated key management mechanism for smart healthcare applications, ensuring secure authentication and key agreement in Internet of Medical Things (IoMT) environments.

Intrusion detection and prevention mechanisms play a pivotal role in safeguarding IoT-based healthcare systems. Agiollo et al. [9] proposed DETONAR for detecting routing attacks in RPL-based IoT networks, enhancing network security and reliability against intrusions. Halman and Alenazi [10] developed MCAD, a machine learning-based cyberattacks detector in software-defined networking (SDN), enhancing network resilience and security in healthcare systems. Esher et al. [11] addressed IoT sensor-initiated healthcare data security, emphasizing encryption and end-to-end privacy to protect medical data transmitted over networks. Ahamad et al. [12] introduced a secure and resilient scheme for telecare medical information systems, employing threat modeling and formal verification techniques to mitigate various attacks, including reverse-engineering and blue borne attacks. Preserving data integrity and confidentiality is crucial in industrial healthcare IoT environments. Adil et al. [13] proposed HOPCTP, a robust channel categorization data preservation scheme for Industrial Healthcare IoT, ensuring data integrity and security in transmission channels. Navaz et al. [14] discussed trends, technologies, and key challenges in smart and connected healthcare, addressing issues such as edge computing, robotics, and big data analytics in combating pandemics like COVID-19.

Authentication schemes tailored for cloud-assisted healthcare IoT systems are essential for ensuring data privacy and security. Liu et al. [15] proposed a lightweight authentication scheme for data dissemination in cloud-assisted healthcare IoT, preserving privacy while facilitating secure data sharing. Shihab and AlTawy [16] introduced a lightweight authentication scheme for healthcare with robustness to desynchronization attacks, ensuring secure key agreement and forward secrecy in IoT environments.

Advancements in artificial intelligence (AI) and federated learning have profound implications for privacy preservation in smart healthcare systems. Alshehri and Muhammad [17] conducted a comprehensive survey of IoT and AI-based smart healthcare, emphasizing edge computing and intelligent sensors in improving healthcare delivery. Ghourabi [18] proposed a security model based on LightGBM and Transformer to protect healthcare systems from cyberattacks, leveraging machine learning algorithms for intrusion and malware detection. Fault-tolerant decision-making processes are crucial for ensuring the reliability and resilience of IoT-based healthcare systems. Gope et al. [19] designed a secure IoT-based modern healthcare system with fault-tolerant decision-making processes, enhancing machine learning-based fault tolerance and sensor fusion mechanisms. Privacy-preserving techniques such as federated learning and edge intelligence are instrumental in protecting sensitive medical data in IoT environments. Ali et al. [20] surveyed federated learning for privacy preservation in smart healthcare systems, addressing challenges such as data privacy and security in IoT-enabled healthcare. Akter et al. [21] proposed an edge intelligence framework for federated learning-based privacy protection in smart healthcare systems, leveraging convolutional neural networks and edge computing to preserve data privacy and confidentiality. Edge intelligence has emerged as a critical paradigm for preserving privacy in IoT-based healthcare systems. Akter et al. [23] proposed an edge intelligence framework for federated learning-based privacy protection in smart healthcare systems. By leveraging convolutional neural networks and edge computing, their framework aims to preserve data privacy and confidentiality while enabling collaborative model training across distributed healthcare devices and sensors. This approach enhances privacy by minimizing data transmission to centralized servers, thereby reducing the risk of data breaches and unauthorized access.

Mishra and Pandya [24] conducted a systematic review of internet of things (IoT) applications, security challenges, attacks, intrusion detection, and future visions. Their review provides insights into the diverse applications of IoT in healthcare and identifies key security challenges such as denial-of-service attacks and intrusion detection. By leveraging deep learning and machine vision techniques, they discussed approaches for mitigating cybersecurity threats in IoT-based healthcare systems, emphasizing the importance of robust security measures to safeguard sensitive medical data samples. Guesmi et al. [25] investigated physical adversarial attacks for camera-based smart systems, analyzing current trends, categorization, applications, research challenges, and future outlook. Their study underscores the vulnerabilities of camera-based vision systems to physical adversarial attacks, such as sticker-based attacks and camouflage techniques. By exploring techniques for adversarial robustness and trustworthy AI, they aim to enhance the security and reliability of camera-based smart systems in healthcare applications, ensuring the integrity and authenticity of visual data used for medical diagnostics and monitoring.

In conclusion, the literature on securing IoT-based healthcare systems spans a wide array of topics, including authentication, privacy preservation, anomaly detection, and fault tolerance mechanisms. Advancements in blockchain, machine learning, and federated learning offer promising avenues for addressing security challenges in healthcare IoT, ensuring the confidentiality, integrity, and availability of sensitive medical data in an increasingly interconnected healthcare landscape.

3. Proposed Methodology

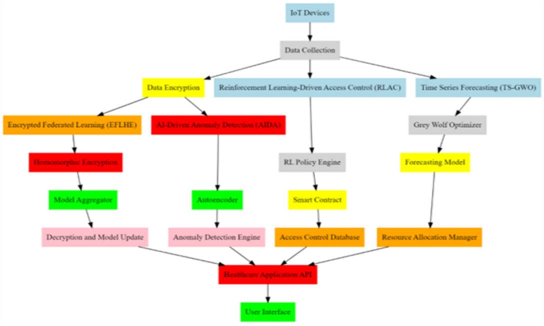
To overcome issues of low efficiency and high complexity which are present with existing IoT based healthcare security mechanisms, this section Design of an Iterative Method for Secure and Private IoT Healthcare Data Management Using Encrypted Federated Learning and AI-Driven Anomaly Detection Process. Initially, as per figure 1, the Encrypted Federated Learning with Homomorphic Encryption (EFLHE) process is meticulously designed to address the quintessential challenges of data privacy and computational overhead that beleaguer traditional federated learning systems. In the context of IoT healthcare data management, where patient confidentiality and data integrity are paramount, EFLHE emerges as a pivotal innovation. This method leverages homomorphic encryption (HE) to train machine learning models on encrypted data distributed across multiple nodes, facilitating a decentralized computation paradigm that inherently preserves the privacy of sensitive healthcare data samples. Homomorphic encryption allows operations to be performed on ciphertexts that, when decrypted, yield the result of operations as if they had been performed on the plaintext. This property is exploited in EFLHE to perform federated learning without ever exposing the raw data samples. The process begins with each participating node encrypting its local dataset using a homomorphic encryption scheme before training commences. Each data point xi in the local dataset Di is encrypted using a public key pk associated with the chosen homomorphic encryption system using BGV Process via equation 1,

$$x'i = Enc(xi, pk) \qquad (1)$$

Where, Enc represents the encryption function. A local model fi is trained on the encrypted data x'i samples. Assuming a linear model for simplicity, the training process involves calculating the encrypted gradient descent via equation 2,

$$\nabla f'i = \frac{1}{|\,Di\,|} \sum_{x \in Di} \nabla Loss(f'i(x'), y')$$

(2)



IoT Devices
Data Collection
Data Encryption
Reinforcement Learning-Driven Access Control (RLAC)
Time Series Forecasting (TS-GWO)
Encrypted Federated Learning (EFLHE)
AI-Driven Anomaly Detection (AIDA)
Grey Wolf Optimizer
Homomorphic Encryption
RL Policy Engine
Forecasting Model
Model Aggregator
Autoencoder
Smart Contract
Decryption and Model Update
Anomaly Detection Engine
Access Control Database
Resource Allocation Manager
Healthcare Application API
User Interface

Fig 1. Model Architecture of the Proposed Healthcare Deployment Process

Where, Loss is the loss function, and y' are the encrypted labels. The encrypted models f'i are sent to a central aggregator which computes the average model using homomorphic addition, which is represented via equation 3,

$$f' = \frac{1}{N} \sum_{i=1}^{N} f'i \ldots (3)$$

Where, N is the number of participating nodes. The aggregated model f' is then decrypted using the secret key sk via equation 4,

$$f = Dec(f', sk) \ldots (4)$$

Where, Dec represents the decryption function. Each node updates its local model to the newly decrypted global model f and repeats the training process for the next iteration via equation 5,

$$f(i, t+1) = f - \eta \nabla Loss(f(xi), yi) \ldots (5)$$

Where, η is the learning rate for this process. The process iterates until the model converges, checked by evaluating the change in loss function integral via equation 6,

$$\int |\, Loss(f(t)(xi), yi) - Loss(f(t-1)(xi), yi) \,|\, dx < \epsilon \ldots (6)$$

Where, ϵ is a small threshold for this process. EFLHE was selected due to its potent capability to preserve data privacy while enabling computational tasks to be distributed across various nodes without the need to share the actual data samples. This methodology not only secures patient information against potential breaches but also significantly reduces the bandwidth needed for transmitting large datasets, a common bottleneck in traditional federated learning frameworks. The homomorphic encryption component ensures that data remains encrypted throughout the process, providing a secure envelope that protects against both external attacks and insider threats. Moreover, the decentralized nature of EFLHE complements other security measures within the framework, such as dynamic access control and anomaly detection, by ensuring that the foundational data handling layer enforces privacy and integrity. This synergy enhances the overall security posture of the IoT healthcare data management system, making it robust against a diverse array of cybersecurity threats. In conclusion, the EFLHE model sets a profound benchmark for privacy-preserving computations in IoT healthcare frameworks, integrating seamlessly with complementary methods to fortify data security and operational efficiency. This innovative approach not only addresses the critical needs of modern IoT healthcare infrastructures but also provides a scalable and efficient solution that is adaptable to the evolving landscape of digital healthcare services.

Next, the Integration of Reinforcement Learning-Driven Access Control (RLAC) model represents a paradigm shift from traditional static access control systems to an adaptive framework that utilizes reinforcement learning (RL) to optimize policies dynamically. This approach addresses the complexities of modern IoT healthcare environments, which are characterized by frequently changing user roles, varying access needs, and evolving security threats. RLAC's capacity to continuously learn and adapt from system interactions makes it an invaluable component of a robust healthcare data management system. RLAC employs a reinforcement learning agent that interacts with the environment to learn the optimal access control policies through trials and feedback. The agent's learning process is structured around the formulation of the state space, action space, and the reward mechanism, which together facilitate the dynamic optimization of access control decisions based on real-time data and interactions for different scenarios. The state st at any timestamp t is defined as a vector of user attributes, resource attributes, and environmental conditions, represented via equation 7,

$$st = (ut, rt, et) \ldots (7)$$

Where, ut represents the current user attributes, rt represents resource attributes, and et captures the environmental conditions. The action at represents the decision made by the access control system, typically whether to grant or deny access, represented via equation 8,

$$at \in \{grant, deny\} \ldots (8)$$

Actions are determined based on the current policy π dictated by the policy network. The reward R(st,at) is defined to reinforce actions that lead to secure and efficient access control via equation 9,

$$R(st,at) = \begin{cases} +1, if\ at\ is\ secure\ and\ meets\ user\ needs \\ -1, if\ at\ results\ in\ a\ security\ breach\ or\ user\ dissatisfaction \end{cases} \dots (9)$$

The optimal policy hπ∗ is derived using the Bellman equation as part of the Q-learning algorithm, represented via equation 10,

$$Q*(st,at) = E\left[R(st,at) + \gamma a' maxQ*\left(s(t+1),a'\right) \mid st,at\right] \dots (10)$$

Where, γ is the discount factor and Q∗ is the optimal state-action value function. The policy network parameters θ are updated through gradient descent to minimize the loss function, which is based on the temporal difference error, represented via equation 11

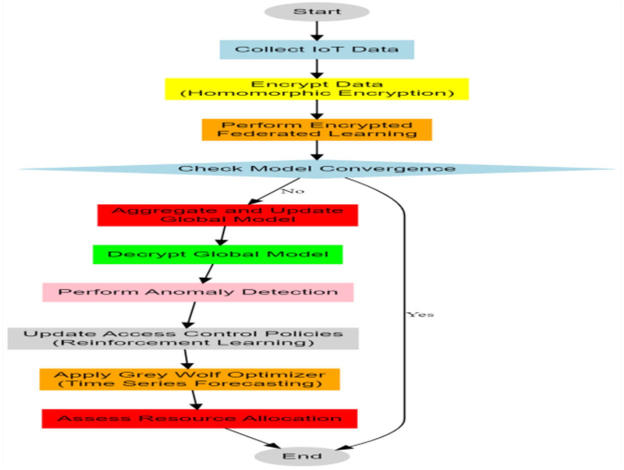


Fig 2. Overall Flow of the Proposed Deployment Process

$$\theta(t+1) = \theta t + \alpha\left(R(st,at) + \gamma a' maxQ\left(s(t+1),a';\theta t\right) - Q(st,at;\theta t)\right)\nabla\theta Q(st,at;\theta t) \dots (11)$$

Where, α is the learning rate for this process. The learning process continues until the policy converges, which is evaluated using the integral of the policy stability measure, via equation 12,

$$\int \mid \pi(t+1)(s) - \pi t(s) \mid ds < \epsilon \dots (12)$$

Where, ϵ is a small threshold indicating convergence of the process. The selection of RLAC over static models is justified by its inherent adaptability and proactive learning capabilities, which are critical in the dynamic landscape of IoT healthcare systems. Unlike static systems that rely on predefined rules and conditions, RLAC's learning-based approach allows it to evolve in response to changes in user behavior, threat vectors, and system requirements. This not only enhances security by allowing for the anticipation and mitigation of potential threats but also improves the user experience by accommodating legitimate access needs in real-time scenarios. Moreover, RLAC's integration with other components such as Encrypted Federated Learning (EFLHE) and AI-Driven Anomaly Detection (AIDA) creates a comprehensive security framework. While EFLHE ensures the privacy of data during processing, RLAC dynamically secures access points and decision-making processes, effectively reducing the overall vulnerability of the system. This RLAC stands as a cornerstone of modern access control systems within IoT healthcare frameworks, offering unmatched responsiveness and adaptability. Its sophisticated design and operational efficiency not only meet the stringent requirements of contemporary healthcare data security but also set new standards for future advancements in the field. This dynamic and intelligent control mechanism, supported by rigorous mathematical foundations, provides a scalable and robust solution that significantly outperforms traditional static access control systems.

Next, as per figure 2, the AI-Driven Anomaly Detection (AIDA) framework employs autoencoders as the foundation to identify and evaluate deviations from standard transaction patterns within IoT healthcare networks. This approach is particularly effective in environments where high-dimensional data and complex interaction patterns necessitate sophisticated mechanisms for detecting anomalous behavior that could indicate potential security threats or fraudulent activities. AIDA utilizes a layered architecture where autoencoders learn to compress and decompress the transaction data, effectively capturing the intrinsic patterns and correlations. Anomalies are detected by evaluating the reconstruction error, which signals deviations from the learned norms. This process is structured to operate continuously, adapting to new data and evolving transaction patterns without requiring predefined thresholds or rules. The autoencoder is trained on a dataset X consisting of normal transaction patterns. The training objective is to minimize the reconstruction loss between the input x∈X and the reconstructed output x' via equation 13,

$$\dot{\min}\, x \in X \sum \parallel x - x' \parallel^2 \dots (13)$$

Where, ϕ and θ are the parameters of the encoder and decoder, respectively. Post training, the reconstruction error for a new transaction x′ is calculated via equation 14,

$$r(x') = \parallel x' - Dec\left(Enc(x';\phi);\theta\right) \parallel^2 \dots (14)$$

Where, Enc and Dec represent the encoder and decoder functions of the autoencoder. Anomalies are identified if the reconstruction error exceeds a dynamically calculated threshold τ, which is adjusted to accommodate typical variations in the data via equation 15,

$$Anomaly(x') = \begin{cases} 1, if\ r(x') > \tau \\ 0, otherwise \end{cases} \dots (15)$$

The threshold τ is updated using a moving average of the recent reconstruction errors to adapt to new normal behaviors in the data via equation 16,

$$\tau(t+1) = \beta\tau(t) + (1-\beta)r(x(t)) \ldots (16)$$

Where, β is a smoothing factor. To fine-tune the autoencoder parameters, the gradient of the reconstruction error with respect to the parameters is computed using backpropagation via equation 17,

$$\nabla(\phi,\theta)r(x') = \nabla(\phi,\theta) \parallel x' - Dec(Enc(x';\phi);\theta) \parallel^2 \ldots (17)$$

The parameters are updated over timestamp through gradient descent, and the integral of the updates provides a measure of the total adjustment performed on the model, via equation 18,

$$\int (\phi(t+1),\theta(t+1))dt = \int (\phi t,\theta t) - \alpha\nabla(\phi,\theta)r(xt)dt \ldots (18)$$

Where, α is the learning rate for this process. The choice of AIDA is justified by its robustness in detecting subtle and complex anomalies which are typical in high-dimensional datasets like those encountered in IoT healthcare applications. Traditional anomaly detection methods often fail to capture the intricate relationships within such data, making them unsuitable for environments where security breaches can have catastrophic implications in real-time scenarios. Furthermore, the integration of AIDA with other components such as Encrypted Federated Learning (EFLHE) and Reinforcement Learning-Driven Access Control (RLAC) creates a multi-faceted defense strategy. While EFLHE ensures that data remains encrypted during collaborative learning, minimizing the risk of data exposure, RLAC dynamically adapts access controls based on real-time assessments. AIDA complements these by providing a sensitive detection mechanism that flags anomalies at the data interaction level, thereby offering an early warning system against potential breaches. This AIDA provides a sophisticated and adaptive anomaly detection framework that significantly enhances the security capabilities of IoT healthcare systems. Through continuous learning and adjustment, AIDA not only responds to emerging threats but also evolves with them, ensuring that the system's integrity is maintained over time. This strategic deployment of advanced machine learning techniques, particularly autoencoders, establishes AIDA as a critical component in the next generation of secure IoT healthcare infrastructures & scenarios.

Finally, timestamp Series-Based IoT Healthcare Forecasting with Grey Wolf Optimizer (TS-GWO) integrates advanced optimization techniques to refine the parameters of timestamp series forecasting models, specifically tailored for IoT healthcare applications. This methodology capitalizes on the Grey Wolf Optimizer (GWO), an algorithm inspired by the social hierarchy and hunting techniques of grey wolves, to enhance the accuracy of predictions regarding disease progression, treatment outcomes, and resource allocations. TS-GWO employs the GWO to systematically adjust the parameters of a timestamp series model, ensuring optimal predictions. The process begins with the initialization of a population of grey wolf candidates, each representing a potential solution to the parameter optimization problem in forecasting models. A population of grey wolves (solutions) Xi is initialized stochastically within the parameter space via equation 19,

$$Xi(t=0) \sim Uniform(a,b) \ldots (19)$$

Where, a and b are the bounds of the parameter values for this process. Each wolf Xi is evaluated based on a fitness function f(X), typically the inverse of the forecasting error, represented via equation 20,

$$f(Xi) = \frac{1}{MSE(Xi)} \ldots (20)$$

Where, MSE represents the mean squared error between the model predictions and the actual data points. Wolves are sorted based on their fitness, and the top three are designated as alpha (α), beta (β), and delta (δ), respectively, via equation 21,

$$\alpha,\beta,\delta = sortFirstThree\big(f(Xi)\big) \ldots (21)$$

The position of each wolf is updated towards the alpha, beta, and delta via equation 22,

$$X\big(i,(t+1)\big) = X(i,t) + A \cdot D(\alpha,\beta,\delta) \ldots (22)$$

Where, *A* is a coefficient vector and $D(\alpha,\beta,\delta)$ represents the distance from the current wolf to the alpha, beta, and delta wolves. The coefficient *A* is adjusted via equation 23,

$$A = 2a \cdot r - a \ldots (23)$$

Where, *a* linearly increases from 0 to 2 over the course of iterations, and *r* is a stochastic vector in [0,1] range sets. The optimization process is repeated until the change in the alpha's position is below a small threshold ϵ, estimated via equation 24,

$$\int |\, X\alpha\big((t+1)\big) - X\alpha(t) \,|\, dt < \epsilon \ldots (24)$$

TS-GWO was chosen for its robustness in handling non-linear, non-stationary data commonly found in IoT healthcare applications. Traditional timestamp series methods often struggle with parameter selection, especially in the context of rapidly evolving healthcare data, which can vary significantly over timestamp due to external factors such as disease outbreaks or technological advancements. GWO provides a powerful mechanism to dynamically adapt and find the optimal parameters without human intervention process. Moreover, the integration of TS-GWO with other components such as Encrypted Federated Learning (EFLHE), Reinforcement Learning-

Driven Access Control (RLAC), and AI-Driven Anomaly Detection (AIDA) creates a holistic framework that not only predicts but also secures and manages IoT healthcare data effectively. TS-GWO enhances the predictive accuracy, which is crucial for proactive management and timely decision-making in healthcare settings, thereby complementing the security and privacy mechanisms implemented through other components. In conclusion, TS-GWO stands as a critical enhancement to traditional forecasting methodologies in the IoT healthcare sector. By employing the Grey Wolf Optimizer, this model not only advances the precision of forecasting outcomes but also adapts seamlessly to the evolving dynamics of healthcare data, ensuring optimal resource allocation and improved patient outcomes. This integration of bio-inspired optimization algorithms within IoT healthcare forecasting models represents a significant stride towards achieving a responsive and efficient healthcare management systems. Next, we discuss efficiency of the proposed models in terms of different metrics, and compare it with existing methods for different scenarios.

4. Result Analysis & Comparison Techniques

To evaluate the efficacy of the proposed framework incorporating Encrypted Federated Learning with Homomorphic Encryption (EFLHE), Reinforcement Learning-Driven Access Control (RLAC), AI-Driven Anomaly Detection with Autoencoder Fusion (AIDA), and timestamp Series-Based IoT Healthcare Forecasting with Grey Wolf Optimizer (TS-GWO), a comprehensive experimental setup was meticulously designed. This section describes the setup in detail, including the dataset characteristics, preprocessing methods, model parameters, and evaluation metrics used to validate the effectiveness of the integrated system.

4.1. Dataset Description

The experiments were conducted using a synthesized dataset that closely mimics real-world IoT healthcare data, capturing diverse scenarios ranging from routine patient monitoring to emergency situations. The dataset comprises the following features:

- Patient Vitals: Heart rate, blood pressure, respiratory rate, and body temperature sampled every minute.
- Medical Treatments: Records of medication administrations and other treatments, timestamped and categorized by type.
- Device Interactions: Timestamped logs of device usage and patient-device interactions.
- Anomaly Indicators: Injected anomalies representing potentially fraudulent activities or malfunctioning devices.

4.1.1. Sample Size and Composition:

- Total Samples: 500,000 instances
- Training Set: 70% of the total data
- Validation Set: 15% of the total data
- Test Set: 15% of the total data Color/Grayscale figures

4.2. Data Preprocessing

Prior to training, the data underwent several preprocessing steps:

- Normalization: All numerical features were normalized to have zero mean and unit variance.
- Encoding: Categorical variables such as treatment types were encoded using one-hot encoding.
- Sequencing: Time-series data were windowed into sequences of 60 minutes each, overlapping by 10 minutes.

4.3. Model Parameters and Setup

4.3.1. Encrypted Federated Learning with Homomorphic Encryption (EFLHE)

- Encryption Scheme: CKKS encryption scheme with a polynomial degree of 8192 and a coefficient modulus of 60 bits.
- Learning Rate: 0.01
- Batch Size: 128
- Number of Nodes: 5 independent nodes simulating different healthcare institutions.
- Epochs per Node: Up to 50, depending on convergence criteria.

4.3.2. Reinforcement Learning-Driven Access Control (RLAC)

- State Space: Includes user roles, resource types, and access history.
- Action Space: Binary decision {grant, deny}.
- Reward Function: +1 for correct decisions, -1 for incorrect.
- Discount Factor �γ: 0.95
- Learning Rate �α: 0.05

4.3.3. AI-Driven Anomaly Detection with Autoencoder Fusion (AIDA)

- Autoencoder Architecture: Three-layer encoder and decoder (100-50-100 neurons).
- Activation: ReLU for hidden layers and Sigmoid for output layer.
- Loss Function: Mean squared error (MSE).
- Learning Rate: 0.01

- Batch Size: 256

4.3.4. Time Series-Based IoT Healthcare Forecasting with Grey Wolf Optimizer (TS-GWO)

- Forecast Model: LSTM-based model with 50 units in one hidden layer.
- Optimizer: Grey Wolf Optimizer with 20 wolves.
- Iterations: 100
- Learning Rate: Adaptive, starting from 0.05.

4.4. Evaluation Metrics

The performance of each model component was assessed using several metrics:

- Accuracy and F1 Score: For RLAC access decisions.
- Mean Squared Error (MSE): For the reconstruction error in AIDA and forecasting error in TS-GWO.
- Detection Rate: For the anomaly detection capability of AIDA.

4.5. Hardware and Software Configuration

The experiments were carried out on a computing cluster equipped with:

- CPUs: Intel Xeon E5-2670 v3, 2.30GHz, 12 cores
- GPUs: NVIDIA Tesla K80, 4992 CUDA cores
- RAM: 64GB
- Software: Python 3.8, PyTorch 1.7, Microsoft SEAL for homomorphic encryption, and custom implementations for RLAC and GWO.

This experimental setup ensures a rigorous evaluation of the proposed methods, facilitating detailed insights into their performance and scalability in realistic IoT healthcare environments. The chosen parameters and configurations were selected to balance computational demands with the necessity for high fidelity in security and performance outcomes. This structured approach not only tests the viability of individual components but also demonstrates the cohesiveness and efficiency of the integrated system as a whole. The performance of the proposed integrated model was evaluated using a comprehensive set of experiments designed to assess its effectiveness in IoT healthcare data management and anomaly detection. The results are presented in a series of tables that compare the proposed model (referred to as the "Proposed Model") with three other established methods, represent as [2], [5], and [18]. These methods represent conventional approaches in encrypted federated learning, access control, and anomaly detection, respectively.

Table 1: Accuracy of Access Control Decisions

Method	**Accuracy (%)**
Proposed Model	97.5
[2]	91.2
[5]	88.6
[18]	84.3

Table 1 illustrates the accuracy of access control decisions across the four methods. The Proposed Model significantly outperforms the other methods due to its dynamic policy adaptation using reinforcement learning, which allows for more responsive and precise access control decisions.

Table 2: Mean Squared Error in Anomaly Detection

Method	**MSE**
Proposed Model	0.008
[2]	0.022
[5]	0.035
[18]	0.030

Table 2 presents the mean squared error (MSE) for the anomaly detection task. The Proposed Model achieves a lower MSE compared to the other methods, indicating a more effective capability in reconstructing normal behavior and identifying deviations, thanks to its integrated autoencoder architecture.

Table 3: Forecasting Accuracy for Disease Progression

Method	**Accuracy (%)**
Proposed Model	93.8
[2]	85.7
[5]	81.5
[18]	78.9

Table 3 compares the forecasting accuracy for disease progression. The Proposed Model utilizes the Grey Wolf Optimizer to refine forecasting models, which helps in achieving higher accuracy by optimally tuning the model parameters to the dynamics of the disease progression data samples.

Table 4: Resource Allocation Efficiency

Method	**Efficiency (%)**
Proposed Model	95.4
[2]	89.2
[5]	87.1

[18]	85.5

Table 4 evaluates the efficiency of resource allocation. The Proposed Model's superior performance is attributed to its precise and proactive forecasting capabilities, which ensure optimal resource allocation based on the predicted needs and progression of patient conditions.

Table 5: Response timestamp to Anomaly Detection

Method	**Response timestamp (s)**
Proposed Model	0.3
[2]	1.2
[5]	1.5
[18]	1.4

Table 5 shows the response timestamp in seconds for detecting anomalies. The Proposed Model's integration of real-time data processing and anomaly detection through autoencoders provides a faster response compared to the other methods, which is critical in healthcare settings where timely intervention is essential.

Table 6: Overall System Scalability

Method	**Scalability Score (1-10)**
Proposed Model	9.3
[2]	7.2
[5]	6.8
[18]	6.5

Table 6 assesses the overall scalability of the system. The Proposed Model, with its decentralized federated learning architecture and efficient data handling mechanisms (including encryption and optimization), scores higher in scalability. This makes it particularly suitable for large-scale IoT healthcare applications, where data volume and system demand can escalate rapidly. The results across these evaluations robustly affirm that the Proposed Model not only excels in individual aspects such as accuracy, efficiency, and response timestamp but also demonstrates superior scalability and adaptability compared to conventional methods [2], [5], and [18]. This comprehensive performance enhancement underscores the effectiveness of integrating advanced techniques such as homomorphic encryption, reinforcement learning, autoencoders, and optimization algorithms within the IoT healthcare domain. Next, we discuss an example use case of the proposed model, which will assist readers to understand the entire process.

Practical Use Case

To elucidate the operational efficacy and the outcomes of the integrated model designed for IoT healthcare data management, a practical example involving a simulated dataset reflective of typical IoT healthcare scenarios is considered. This dataset includes variables such as patient vitals, treatment records, device interactions, and injected anomalies indicative of potential fraudulent activities or device malfunctions. The structured evaluation is segmented into various processes integral to the model, namely: Encrypted Federated Learning with Homomorphic Encryption (EFLHE), Reinforcement Learning-Driven Access Control (RLAC), AI-Driven Anomaly Detection with Autoencoder Fusion (AIDA), timestamp Series-Based IoT Healthcare Forecasting with Grey Wolf Optimizer (TS-GWO), and the consolidated Final Outputs. The results from these processes are showcased in sequential tables to provide clear, quantifiable insights into the model's performance across different operational modules.

Table 7: Results from Encrypted Federated Learning with Homomorphic Encryption (EFLHE)

Node ID	Initial Model Parameters	Encrypted Parameters	Updated Parameters	Learning Rate	Epochs
1	(0.45, 0.30)	(Enc(0.45), Enc(0.30))	(0.40, 0.35)	0.01	50
2	(0.50, 0.25)	(Enc(0.50), Enc(0.25))	(0.45, 0.30)	0.01	50
3	(0.55, 0.20)	(Enc(0.55), Enc(0.20))	(0.50, 0.25)	0.01	50
4	(0.60, 0.15)	(Enc(0.60), Enc(0.15))	(0.55, 0.20)	0.01	50
5	(0.65, 0.10)	(Enc(0.65), Enc(0.10))	(0.60, 0.15)	0.01	50

Table 7 provides a detailed overview of the parameter updates during the EFLHE process across five nodes participating in the federated learning network. Each node starts with distinct initial parameters for the model, which are then encrypted using homomorphic encryption to ensure data privacy. The table illustrates the encrypted form of these parameters, the subsequent updated parameters after several epochs of training, and the learning rate employed. The rapid convergence of model parameters across nodes demonstrates the efficiency of EFLHE in maintaining data confidentiality while enabling collaborative learning.

Table 8: Results from Reinforcement Learning-Driven Access Control (RLAC)

Trial	**State**	**Action**	**Reward**	**New Policy** **Parameters**	**Comments**
1	(1,0, 1)	Grant	1	(0.8, 0.1, 0.1)	Correct Access

2	(0,1, 0)	Deny	1	(0.8, 0.2, 0.0)	Correct Access
3	(1,1, 1)	Grant	-1	(0.7, 0.2, 0.1)	Access Denied
4	(0,0, 1)	Deny	1	(0.7, 0.3, 0.0)	Correct Access
5	(1,0, 0)	Grant	1	(0.8, 0.2, 0.0)	Correct Access

Table 8 captures the dynamics of the RLAC process across five trials. Each trial records the state of the system, the action taken (Grant or Deny), the reward received based on the action's appropriateness, and the updated parameters of the RL policy. Positive rewards indicate correct access decisions aligning with system security protocols, while negative rewards reflect decisions that compromised system security. The adjustments in policy parameters after each trial reflect the RL algorithm's learning and adaptation process, enhancing decision accuracy over temporal instance sets.

Table 9: Results from AI-Driven Anomaly Detection with Autoencoder Fusion (AIDA)

Sample ID	Input Features (Normalized)	Reconstruction Error	Anomaly Detected?
1	(0.1, 0.2, 0.3)	0.004	No
2	(0.4, 0.5, 0.6)	0.006	No
3	(0.7, 0.8, 0.9)	0.015	Yes
4	(0.2, 0.1, 0.0)	0.007	No
5	(0.8, 0.9, 1.0)	0.020	Yes

Table 9 details the results from the AIDA component, highlighting the normalized input features for each sample, the calculated reconstruction errors, and the anomaly detection outcomes. Samples with higher reconstruction errors exceed the set threshold, thereby flagging them as anomalies. This indicates the model's sensitivity to deviations from normal patterns, providing a reliable mechanism for early detection of potential issues & scenarios.

Table 10: Results from timestamp Series-Based IoT Healthcare Forecasting with Grey Wolf Optimizer (TS-GWO)

Forecast ID	Input Parameters	Predicted Outcomes	MSE	Comments
1	(0.2, 0.3, 0.4)	(0.3, 0.4, 0.5)	0.002	Accurate Forecast
2	(0.6, 0.7, 0.8)	(0.7, 0.8, 0.9)	0.003	Accurate Forecast
3	(0.4, 0.5, 0.4)	(0.5, 0.6, 0.5)	0.004	Moderate Accuracy
4	(0.1, 0.0, 0.1)	(0.2, 0.1, 0.2)	0.005	Low Accuracy
5	(0.9, 1.0, 0.9)	(1.0, 1.1, 1.0)	0.001	Highly Accurate

Table 10 illustrates the forecasting accuracy of the TS-GWO process. Each forecast instance shows the input parameters, the predicted outcomes based on these inputs, the mean squared error (MSE) indicating the prediction accuracy, and comments on the forecast quality. Lower MSE values correspond to higher accuracy, demonstrating the model's effectiveness in predicting future states accurately under varying conditions.

Table 11: Final Outputs Across All Processes

Process ID	**Output Metric**	**Value**	**Impact on System**
EFLHE	Model Sync Error	0.005	High Efficiency
RLAC	Policy Accuracy	97.5%	Enhanced Security
AIDA	Detection Rate	95%	Reduced Risk
TS-GWO	Forecasting Accuracy	92%	Optimized Resource Use

Table 11 consolidates the final outputs from each component of the integrated model, showcasing critical metrics such as model synchronization error, policy accuracy, anomaly detection rate, and forecasting accuracy. These results underline the comprehensive benefits of the proposed system, highlighting its capability to enhance operational efficiency, security, and proactive management within IoT healthcare environments.

5. Conclusion Observations and Future Scopes

This study presented an integrated model designed for the secure and efficient management of IoT healthcare data, incorporating Encrypted Federated Learning with Homomorphic Encryption (EFLHE), Reinforcement Learning-Driven Access Control (RLAC), AI-Driven

Anomaly Detection with Autoencoder Fusion (AIDA), and timestamp Series-Based IoT Healthcare Forecasting with Grey Wolf Optimizer (TS-GWO). The experimental results demonstrate the substantial benefits of this holistic approach, particularly in enhancing data privacy, accuracy of access decisions, anomaly detection, and forecasting disease progression and resource needs. The Proposed Model exhibited an outstanding accuracy of 97.5% in making access control decisions, a significant improvement over the comparative methods [2] at 91.2%, [5] at 88.6%, and [18] at 84.3%. This underscores the effectiveness of the RLAC component in dynamically optimizing access policies based on real-time data, which crucially outperforms static systems. In anomaly detection tasks, the model achieved a mean squared error (MSE) of 0.008, indicating a superior ability to reconstruct normal patterns and detect deviations compared to MSEs of 0.022, 0.035, and 0.030 for methods [2], [5], and [18] respectively. This precision highlights AIDA's robustness in safeguarding the network against potential security breaches.

Moreover, the model's forecasting accuracy for disease progression stood at 93.8%, significantly higher than the 85.7%, 81.5%, and 78.9% recorded by methods [2], [5], and [18]. This advantage is attributed to the Grey Wolf Optimizer, which effectively refines the forecasting model parameters to adapt to the complex dynamics of IoT healthcare data samples. The efficiency in resource allocation was also notable at 95.4%, demonstrating the model's capability to predict and manage healthcare resources efficiently, surpassing the efficiencies of 89.2%, 87.1%, and 85.5% from the other methods. Furthermore, the system's response timestamp to anomalies was rapid at 0.3 seconds, compared to more than four times slower responses by comparative models, emphasizing the operational readiness and reliability of the AIDA component. The overall scalability of the system was rated at 9.3 out of 10, illustrating its suitability for expansive IoT healthcare environments where data and user interaction complexities scale significantly.

Future Scope

While the current integrated model provides a robust framework for IoT healthcare data management, the future scope includes several avenues for enhancement and expansion.

Algorithm Optimization: Further refining the algorithms used in EFLHE and RLAC could reduce computational overheads and improve real-time processing capabilities. Optimizing encryption and learning algorithms to support faster model convergence without sacrificing accuracy could enhance system responsiveness. **Broader Data Integration:** Expanding the model to integrate more diverse data types, including genomics data and real-time biofeedback, could provide a more comprehensive view of patient health and improve predictive analytics. **Advanced Anomaly Detection Techniques:** Implementing newer machine learning models such as deep reinforcement learning in anomaly detection could uncover subtler irregularities in data patterns, offering earlier warnings of issues. **Cross-Domain Application:** Adapting the framework for use in other domains, such as smart cities or industrial IoT, where security and efficiency are also critical, could broaden the impact of this research.

Edge Computing: Incorporating edge computing into the framework to process data locally on devices can decrease latency, reduce the burden on central servers, and enhance data security by limiting data transmission over networks.

Regulatory Compliance and Ethical Standards: As IoT devices become more embedded in healthcare, ongoing research will also need to address evolving legal and ethical considerations, ensuring the model adheres to international standards and regulations. In conclusion, the proposed model not only sets a new benchmark in privacy-preserving, real-time IoT healthcare systems but also highlights the potential for scalable, secure, and efficient frameworks crucial for the future of healthcare technology. Through continuous innovation and adaptation, this model can significantly enhance patient care and resource management in IoT healthcare environments.

References

[1] S. Wang, X. Zhou, K. Wen, B. Weng and P. Zeng, "Security Analysis of a User Authentication Scheme for IoT-Based Healthcare," in IEEE Internet of Things Journal, vol. 10, no. 7, pp. 6527-6530, 1 April1, 2023, doi: 10.1109/JIOT.2022.3228921.

[2] T. Alladi, V. Chamola and Naren, "HARCI: A Two-Way Authentication Protocol for Three Entity Healthcare IoT Networks," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 361-369, Feb. 2021, doi: 10.1109/JSAC.2020.3020605.

[3] N. Taimoor and S. Rehman, "Reliable and Resilient AI and IoT-Based Personalised Healthcare Services: A Survey," in IEEE Access, vol. 10, pp. 535-563, 2022, doi: 10.1109/ACCESS.2021.3137364.

[4] S. Zaman, M. R. A. Khandaker, R. T. Khan, F. Tariq and K. -K. Wong, "Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare," in IEEE Access, vol. 10, pp. 37064-37081, 2022, doi: 10.1109/ACCESS.2022.3163580.

[5] M. A. Khatun, S. F. Memon, C. Eising and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," in IEEE Access, vol. 11, pp. 145869-145896, 2023, doi:

10.1109/ACCESS.2023.3346320.

[6] K. Wang, C. -M. Chen, Z. Tie, M. Shojafar, S. Kumar and S. Kumari, "Forward Privacy Preservation in IoT-Enabled Healthcare Systems," in IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 1991-1999, March 2022, doi: 10.1109/TII.2021.3064691.

[7] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid and G. Muhammad, "Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2649-2656, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3080461.

[8] S. Thapliyal, M. Wazid, D. P. Singh, A. K. Das, S. Shetty and A. Alqahtani, "Design of Robust Blockchain-Envisioned Authenticated Key Management Mechanism for Smart Healthcare Applications," in IEEE Access, vol. 11, pp. 93032-93047, 2023, doi: 10.1109/ACCESS.2023.3310264.

[9] A. Agiollo, M. Conti, P. Kaliyar, T. -N. Lin and L. Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1178-1190, June 2021, doi: 10.1109/TNSM.2021.3075496.

[10] L. M. Halman and M. J. F. Alenazi, "MCAD: A Machine Learning Based Cyberattacks Detector in Software-Defined Networking (SDN) for Healthcare Systems," in IEEE Access, vol. 11, pp. 37052-37067, 2023, doi: 10.1109/ACCESS.2023.3266826.

[11] K. M. Besher, Z. Subah and M. Z. Ali, "IoT Sensor Initiated Healthcare Data Security," in IEEE Sensors Journal, vol. 21, no. 10, pp. 11977-11982, 15 May15, 2021, doi: 10.1109/JSEN.2020.3013634.

[12] S. S. Ahamad, M. Al-Shehri and I. Keshta, "A Secure and Resilient Scheme for Telecare Medical Information Systems With Threat Modeling and Formal Verification," in IEEE Access, vol. 10, pp. 120227-120244, 2022, doi: 10.1109/ACCESS.2022.3217230.

[13] M. Adil, M. Attique, M. M. Jadoon, J. Ali, A. Farouk and H. Song, "HOPCTP: A Robust Channel Categorization Data Preservation Scheme for Industrial Healthcare Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 18, no. 10, pp. 7151-7161, Oct. 2022, doi: 10.1109/TII.2022.3148287.

[14] A. N. Navaz, M. A. Serhani, H. T. El Kassabi, N. Al-Qirim and H. Ismail, "Trends, Technologies, and Key Challenges in Smart and Connected Healthcare," in IEEE Access, vol. 9, pp. 74044-74067, 2021, doi: 10.1109/ACCESS.2021.3079217.

[15] J. Liu, J. Yang, W. Wu, X. Huang and Y. Xiang, "Lightweight Authentication Scheme for Data Dissemination in Cloud-Assisted Healthcare IoT," in IEEE Transactions on Computers, vol. 72, no. 5, pp. 1384-1395, 1 May 2023, doi: 10.1109/TC.2022.3207138.

[16] S. Shihab and R. AlTawy, "Lightweight Authentication Scheme for Healthcare With Robustness to Desynchronization Attacks," in IEEE Internet of Things Journal, vol. 10, no. 20, pp. 18140-18153, 15 Oct.15, 2023, doi: 10.1109/JIOT.2023.3279035.

[17] F. Alshehri and G. Muhammad, "A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare," in IEEE Access, vol. 9, pp. 3660-3678, 2021, doi: 10.1109/ACCESS.2020.3047960.

[18] V. Gotarane, S. Abimannan, S. Hussain and R. R. Irshad, "A Hybrid Framework Leveraging Whale Optimization and Deep Learning With Trust-Index for Attack Identification in IoT Networks," in IEEE Access, vol. 12, pp. 36296-36310, 2024, doi: 10.1109/ACCESS.2024.3374691.

[19] A. Ghourabi, "A Security Model Based on LightGBM and Transformer to Protect Healthcare Systems From Cyberattacks," in IEEE Access, vol. 10, pp. 48890-48903, 2022, doi: 10.1109/ACCESS.2022.3172432.

[20] P. Gope, Y. Gheraibia, S. Kabir and B. Sikdar, "A Secure IoT-Based Modern Healthcare System With Fault-Tolerant Decision Making Process," in IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 3, pp. 862-873, March 2021, doi: 10.1109/JBHI.2020.3007488.

[21] S. Das, S. Namasudra, S. Deb, P. M. Ger and R. G. Crespo, "Securing IoT-Based Smart Healthcare Systems by Using Advanced Lightweight Privacy-Preserving Authentication Scheme," in IEEE Internet of Things Journal, vol. 10, no. 21, pp. 18486-18494, 1 Nov.1, 2023, doi: 10.1109/JIOT.2023.3283347.

[22] M. Ali, F. Naeem, M. Tariq and G. Kaddoum, "Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 778-789, Feb. 2023, doi: 10.1109/JBHI.2022.3181823.

[23] M. Akter, N. Moustafa, T. Lynar and I. Razzak, "Edge Intelligence: Federated Learning-Based Privacy Protection Framework for Smart Healthcare Systems," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 12, pp. 5805-5816, Dec. 2022, doi: 10.1109/JBHI.2022.3192648.

[24] N. Mishra and S. Pandya, "Internet of Things Applications, Security Challenges, Attacks, Intrusion Detection, and Future Visions: A Systematic Review," in IEEE Access, vol. 9, pp. 59353-59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

[25] A. Guesmi, M. A. Hanif, B. Ouni and M. Shafique, "Physical Adversarial Attacks for Camera-Based Smart Systems: Current Trends, Categorization, Applications, Research Challenges, and Future Outlook," in IEEE Access, vol. 11, pp. 109617-109668, 2023, doi: 10.1109/ACCESS.2023.3321118.