Journal of Intelligent Systems and Internet of Things
Vol. 18, No. 01, PP. 12-33, 2026
DOI: https://doi.org/10.54216/JISIoT.180102

ChainGuard 6G+: A Secure and Private Architecture for Wireless Communication Using Federated Learning and Blockchain in IoT Networks

Saleh Ali Alomari[1,*]
[1]Computer Science Department, Faculty of Information Technology, Jadara University, Irbid 21110, Jordan
Email: omari08@jadara.edu.jo

Abstract

The advent of 6G wireless communication systems and the widespread proliferation of Internet of Things devices have necessitated advanced frameworks for secure, private, and intelligent data management. ChainGuard 6G+, a novel privacy-preserving architecture, which integrates Federated Learning with Blockchain, is introduced in this paper to offer data security, integrity, and anomaly detection features for IoT-enabled 6G networks. FL facilitates decentralized model training across distributed edge nodes, thus keeping local data on-device with model updates shared. This ensures user privacy, particularly valuable in sensitive applications such as healthcare, financial services, and industrial IoT networks. For further strengthening privacy, Differential Privacy is applied by introducing statistical noise into model updates, masking individual contributions without degrading learning accuracy. Blockchain is incorporated as an immutable ledger to record model parameters and training securely, enabling traceability and tamper-evident model provenance. Role-based access control for secure data and model access, end-to-end encryption, and secure transmission protocols are included in the architecture. Experimental results demonstrate the efficacy of the system under consideration using a 6G Network Slice Security Attack Detection Dataset, with synthetic and real attacks on various network slices. Performance evaluation reveals that ChainGuard 6G+ not only ensures data privacy but also has excellent detection rates against DoS, DDoS, and spoofing attacks. The proposed framework achieves an overall attack detection accuracy of 99.1%, implemented and experimented using Python, revealing its promise as a secure, scalable solution for future wireless secure communication networks.

Received: March 14, 2025 Revised: June 02, 2025 Accepted: July 10, 2025

Keywords: Federated Learning; Blockchain; 6G Network Security; IoT Privacy; Anomaly Detection

1. Introduction

The advent of 6G wireless communication introduces a new hyper-connectivity paradigm of ultra-low latency, high-bandwidth, and ubiquitous intelligence. As the Internet of Things, which includes billions of smart devices, continues to grow, data security and protection become the top priority. The shift to 6G will most probably allow for advanced, latency-tolerant applications like autonomous vehicles, telesurgery, and immersive AR/VR. These applications demand secure communication platforms. However, current architectures typically do not have data protection and system openness [1]. In response to this, ChainGuard 6G+ architecture is presented herein as an emerging paradigm that combines federated artificial intelligence and blockchain techniques. The combination can offer a decentralized, privacy-preserving, and smart communication platform for future IoT networks. Federated AI protects training to occur on-device without revealing raw data, to address data ownership and privacy concerns. Blockchain guarantees communication and data exchange integrity, traceability, and immutability. Both together form a synergistic system addressing the multidimensional threats of wireless ecosystems today [2].

Yet another of ChainGuard 6G+'s core innovations is its federated AI mechanism, supporting collaborative model training on edge devices without sacrificing data locality. Without aggregating data centrally, the system does not

incur privacy violations and communication overhead. Moreover, the decentralized aspect of federated learning aligns with the distributed nature of IoT networks. This enables scalable deployment of AI across devices and domains. It also reduces reliance on centralized cloud infrastructure [3]. Blockchain incorporation within ChainGuard 6G+ is a trustworthy and transparent layer for identity management, agreement processes, and messaging. Smart contracts are leveraged to support automated rules of trust, authorization of access, and verify compliance among the network members. Utilization of permissioned blockchain holds the promise of faster verification of transactions with the maintenance of system transparency along with accountability. Not only does the system process safe device-to-device communication but also facilitates real-time decisions. It secures a firm position for self-governing IoT systems [4].

The convergence of blockchain and federated AI creates potential for adaptive, self-regulating, and tamper-evident network behavior. ChainGuard 6G+ capitalizes on this convergence to be resilient against adversarial attacks, unauthorized access, and data tampering. Attack detection mechanisms are built into the federated learning process to improve security adaptively. Immutable blockchain records also introduce forensic capability and accountability. The hybrid approach enhances network resilience and trustworthiness for mission-critical application [5]. In order to reinforce the dynamic properties of 6G IoT setups, ChainGuard 6G+ accommodates a lightweight consensus protocol that caters specifically to resource-constrained edge devices. Traditional consensus approaches like PoW and PoS are energy-heavy and unsuitable for such deployments. Hence, a customized model of consensus has been introduced to enable quick verification with low-energy consumption. It makes the system suitable for real-time low-power IoT deployments and promotes energy saving in future networks [6].

Privacy protection is another foundation stone pillar of ChainGuard 6G+. Techniques such as differential privacy, secure aggregation, and homomorphic encryption are incorporated in the federated learning. These prevent data leakage during training while not sacrificing model accuracy. Blockchain-based identity management maintains anonymity of users and prevents identity spoofing as well. Privacy is thus infused at data and communication layers. The entire privacy framework makes ChainGuard 6G+ a revolutionary architecture [7]. ChainGuard 6G+ also addresses interoperability and scalability issues that are inherent in heterogeneous IoT settings. It is designed to support different types of devices, operating systems, and networking protocols with modular and API-based interfaces. It supports seamless onboarding of new devices and services without undermining system consistency. Moreover, federated model updates are made optimally for transmission efficiency to reduce the impact on network bandwidth. This makes the system responsive and adaptive to fluctuating loads of operation [8]. On the deployment level, the architecture supports a hierarchical continuum model of the edge-cloud for which tasks are intelligently split among device, fog, and cloud layers. Federated AI performs localized computing at the edge, and blockchain supports a distributed ledger between the fog and cloud nodes. Such a topology balances processing loads, minimizes latency, and increases reliability. The topology also enables contextual perception and real-time response in mission-critical applications. This multi-layer system maximizes overall network performance [9]. ChainGuard 6G+ offers a paradigm-shifting roadmap for securing future-proof IoT networks using a federated AI and blockchain-based solution. It addresses basic problems such as data privacy, security, scalability, and trust in a decentralized manner. By integrating intelligence with immutable record keeping, it lays the foundation for secure and autonomous wireless ecosystems. When 6G becomes a reality, technology like ChainGuard 6G+ will be the key to determining the future digital infrastructure. The following sections will discuss its design, implementation, and performance analysis [10]. Key Contributions of this article are,

1. The paper introduced ChainGuard 6G+, a novel architecture that combined Federated AI and blockchain to ensure privacy-preserving communication in 6G-enabled IoT networks.
2. It implemented federated LSTM models at the edge for decentralized anomaly detection without exposing raw data.
3. A private Ethereum blockchain was integrated to manage device authentication, model update verification, and secure key rotation via smart contracts.
4. Differential privacy techniques were applied to gradient updates, protecting user data from inference attacks.
5. The architecture was evaluated through simulation, demonstrating improved model accuracy, reduced communication overhead, and enhanced security compared to traditional methods.

The remainder of the document is organized as follows: An overview of relevant research on federated learning, blockchain integration, and protecting privacy in future IoT networks is given in Section 2. The problem statement is introduced in Section 3, outlining the main obstacles to providing safe, effective, and secure communication in IoT ecosystems provided by 6G. The suggested ChainGuard 6G+ architecture is presented in Section 4, along with an overview of the blockchain coordination, privacy-preserving methods, and federated LSTM model structure. The study's setup, simulation outcomes, and the comparisons of the suggested system with traditional learning techniques are all covered in Section 5. The paper is concluded in Section 6 with a summary of the contributions and possible future research topics.

2. Related Work

Wijesekara et al.,[11] worked on how blockchain might be applied in cognitive networks and for improving trust, privacy, and decision reliability in KDN systems. They considered the use of blockchain technology for sharing models and exchanging knowledge in machine learning-based networks. They established blockchain applicability in resource allocation and access control in knowledge-centric SDN systems. They also talked about blockchain's use in traffic optimization and anomaly detection in smart network systems. Finally, they touched upon challenges such as scalability, energy consumption, and processing large data in the integration of blockchain with KDN frameworks.

Fadhil et al.,[12] elaborated on the application of blockchain in smart cities within the framework of 6G with the aim of enhancing urban life through secure and intelligent communication networks. They surveyed existing literature to highlight the key role of blockchain in facilitating trust and transparency in smart city systems. They explored key technologies and deployment scenarios that are essential for sixth-generation communication networks. They identified major challenges to applying blockchain in 6G environments, including technological, infrastructural, and regulatory challenges. The study also proposed future research directions to overcome these challenges and facilitate blockchain use in smart cities based on 6G.

Zhou et al.,[13] reviewed the integration of artificial intelligence and blockchain technologies to address the limitations of traditional communication protocols in future wireless networks. They emphasized AI's capability in dynamic adaptation through big data processing and blockchain's role in ensuring data integrity, security, and privacy. Their survey presented various state-of-the-art applications of both technologies within wireless network scenarios. They also discussed complementarity between blockchain and AI in making FWNs smarter and more reliable. They concluded with the existing limitations and proposed future research directions for their effective utilization in FWNs.

Bobde et al.,[15] In order to solve the increasing problems with integrity of data, privacy, and accessibility control, suggested a blockchain security solution for industrial IoT networks. To secure transmission from sensor nodes, their method uses local data aggregating and ChaCha20-Poly1305 encryption. Data is categorized via a secure blockchain gateway according to secrecy and sent to the Interplanetary filing system or cloud storage for further security. To make data access safe and effective, they used a proof of authority consensus method with Zero Information Evidence for devices authenticating. The study highlights how crucial creative and adaptable security measures are in emerging industrial IoT settings.

Nguyen et al.,[16] presented an exhaustive review of the incorporation of blockchain and edge computing in IoT systems to overcome limitations such as security vulnerabilities, delay, and energy inefficiency. They explored system architectures and categorized blockchain-based edge deployments in various applications in the IoT domain. Their research established complete security requirements like confidentiality, integrity, authentication, and trust, among others. The study detailed real-world use cases where blockchain-edge systems enhance the functions of IoT through the fulfilment of security requirements. Finally, they touched on challenges to date and provided future trends in an effort to further inform research on blockchain-enhanced edge IoT systems.

Bobde et al.,[17] promoted a blockchain-based method for enhancing the security and reliability of Industrial IoT networks as far as issues such as data confidentiality, integrity, and access are concerned. The network uses sensor nodes to fetch data and compact it and then ChaCha20-Poly1305 encrypts it before it is sent to aggregators in proximity. Data is stored in safe places like the cloud or the Interplanetary filing system after being processed by a private blockchain gateway with reference secrecy standards. Zero Knowledge Proof is added for device authorization, and the Validation of Authorities Consent technique is used to guarantee the system's integrity and validity.

Ahakonye et al.,[18] conducted a survey of papers across various domains including AI, blockchain, and IoT to explore future trends and challenges in enhancing IDS performance. Their study highlighted the power of combining AI and blockchain to transform IDS into an open, scalable, and decentralized system. Case studies asserted the viability of integrating the two towards improving the performance of IDS. The article emphasized the need for future progress in blockchain-based cybersecurity, particularly in light cryptography, scalable consensus protocols, and privacy-saving methods.

Patil et al.,[19] found gaps in the literature about the types of data—text, photos, and audio—and how they affect AI model installation and development. The research looked at security issues in the dataset, learning phase, and learned models—the three stages of AI healthcare systems. They argued for more secure methods after taking into account the vulnerabilities unique to computer vision, acoustic AI, and natural language processing systems. In order to overcome those security and privacy issues and enable a broader use of AI in healthcare, the evaluation suggested blockchain technology.

Lin et al.,[20] suggested a blockchain-integrated encryption K-mean clustering-based stellar consensus framework to handle data privacy concerns in the Internet of Medical Things. By using the elliptic curve version of the Menezes–Qu–Vanstone authentication of messages code protocol and the Deltoid curves-based Pallier cryptosystem for safe data storage, their system improves user authentication. The technique lessens the storage load in blockchain networks while addressing majority attacks, Byzantine issues, and unlawful authentication. The generation process also helps to improve data privacy. In comparison to previous methods, experimental results showed increased efficiency, a higher packet delivery ratio, and decreased privacy leaks.

Banti et al.,[21] explored the challenges of ensuring data quality in Next Generation Internet of Things Human-Centric Sensing systems. They identified factors affecting data quality like user participation, trustworthiness, and credibility of data collected through smart devices. Their work proposed a new categorization to address such issues based on task allocation, reputation systems, and blockchain. They outlined a trust-sensitive task assignment scheme that leverages reputation mechanisms and blockchain to gain high-quality contributions of data while preserving user anonymity. The scheme utilizes blockchain decentralization, openness, and impermeability for enabling trusted service provision and sharing of data.

Queralta et al.,[22] canvassed the use of distributed ledger technologies, notably blockchain, in multi-robot systems with focus on their capability to secure and control large-scale autonomous networks. They described how DLTs are moving away from experimental phases to address actual robotics challenges such as intermittent connectivity and scalability. The canvass highlighted the pertinence of permissioned blockchains and novel DLT architectures in industrial and mature robotics uses. They emphasized that most open and permissionless blockchain research is aimed at specific robotics applications.

Pakrooh et al.,[23] examined how deep learning techniques might be used to improve security and privacy in Web of Health systems. Regarding their capacity data produced by health wear technology, they surveyed recent studies on DL-assisted secure models. In order to address privacy problems in IoMT applications, the article categorized and summarized important contributions to the development of intelligent security measures. The authors stressed how crucial it is to use DL in an approach that safeguards private health information exchanged in these kinds of systems. Lastly, they suggested directions for additional study to enhance security and confidentiality in IoMT systems.

Yapa et al.,[24] offered six primary directions in the application of blockchain in addressing the challenge of integrating heterogeneous sources of energy, control of distribution networks, and big data utilization. The article explained how blockchain technology could be used in enabling secure, self-governed energy supply through maximization of Distributed Generation utilization. The authors also pointed out the challenge in all directions and how blockchain technology could help solve them. They went on to explain future research avenues for having fully autonomous and decentralized electricity distribution systems.

Majumdar et al.,[25] provided a thorough analysis of the potential applications of blockchain, AI, and IoT in achieving Society 4.0. They understood how these advances could improve data safety, security, and identification for real-time data collection and decision-making processes, as well as facilitating efficient information management. AI was acknowledged as a crucial tool for enhancing security and productivity in high-risk business settings, along with blockchain. Additionally, the authors pointed out research gaps and the necessity of additional Blockchain application research in Society 4.0. Lastly, they suggested future lines of inquiry for the creation of Society 4.0 products based on blockchain.

Rancea et al.,[26] carried out a thorough analysis of the potential advantages of delay reduction, privacy enhancement, and system capacity to enhance the healthcare industry's use of cloud computing and AI. They considered the issues of edge compute offloading, AI optimization, and data privacy and security. The research has been divided into three main areas: edge dumping, AI-based optimization techniques, and security and confidentiality. Their study highlights the potential for change of edge AI for healthcare and eHealth care, especially for secure communication and immediate decision-making. They did find that more work has to be done to develop effective load orchestrating and security-preserving strategies for distributed systems.

Deepa et al.,[27] discussed how blockchain technology and the Internet of Things are combining, and suggested a unique blockchain-based EoT architecture for use in industrial settings. They underlined the importance of BEoT in delivering high-security, minimal latency services for a range of IoT domains; including grids, smart homes, medical care, and transportation. The study demonstrated how well BEoT preserves security features that include information privacy, detection of attacks, trust management, and access authentication. The main research issues and future perspectives for the integration of blockchain at the network edge were also covered. Their efforts serve as a basis for developing BEoT applications across many industries.

Pattnaik et al.,[28] pointed out the game-changing role played by IoT in Industry 4.0/5.0, smart homes, smart cities, and green wireless communication systems. They illustrated the growing network complexity with rising

numbers of heterogeneous IoT devices and high data rates. The research proposed the implementation of sixth-generation technologies to overcome future communication needs. A location tracking system was demonstrated in real-time using Bluetooth Low Energy for underground industrial application. In addition, an applications-focused investigation into industrial positioning systems was undertaken in order to test performance in hostile environments.

Selvarajan et al.,[29] approach uses unique key pair generation through multiplicative operations and time stamps for secure storage of data in blockchain-based hash blocks. The Quantum Trust Reconciliation Agreement Model offers secure communication through trust-based computation by deriving trust scores from feedback data. For added security, Tuna Swarm Optimization is applied to authenticate nonce messages during communication. Comparative evaluation with existing models sets the effectiveness of the suggested model in reducing computational complexity and enhancing overall cybersecurity performance.

Aluvalu et al.,[30] explored the potential of wearable technology coupled with wireless communication and blockchain for enhancing monitoring of healthcare as well as ensuring privacy in a hospital environment. Their framework captures digital biomarkers from sensors for monitoring parameters including ECG, SPO2, and body activity. They employed gradient boosting alongside a hybrid microwave transmission scheme for real-time decision-making purposes and location. The approach facilitates threat detection and mobile tracking via call data, and it adds to health security. The proposed model in this paper achieved 98% classification accuracy after cleaning irrelevant information, indicating robust data analysis and system performance. Hussein et al.,[31] discussed a new smart irrigation system designed specifically for the oases of Sahara located in southern Tunisia. The use of IoT sensors coupled with AI algorithms allows for both real time environmental monitoring as well as accurate forecasting of water requirements for date palms to be provided. Results indicate considerable savings for water used along with enhancements in crop health and greater yields. Moreover, remote control coupled with cloud monitoring facilitates further enhancement in reducing water usage, providing a comprehensive method to alleviate water scarcity challenges in dry areas while promoting sustainable agricultural practices. Taoufik et al.,[32] presents a system architecture for the Internet of Things application in real-time EEG signal based detection and recognition of epileptic seizures. It includes the state-of-the-art zeta feature selection using metaheuristic optimization coupled with an adaptive deep learning classification layer. Thanks to its cloud computing integration, this system permits instantaneous response to seizure events while ensuring proper management of confidential information, making it possible to monitor patients in real-time. The results obtained from this study were better than those obtained using other systems, thus demonstrating the effectiveness of these novel techniques towards enhancing care provided to patients suffering from epilepsy.

In a number of applications, including healthcare, intelligent cities, industrial internet of things, self-driving cars, and upcoming wireless technologies, and the literature study illustrates how blockchain, artificial intelligence, and edge computing are convergent. Research highlights how blockchain may improve decentralized systems' safety, confidence, data integrity, and access management, while federated and edge AI support real-time decision-making and privacy protection. Among the applications found are energy-conscious IoT systems, anomaly detection, traffic optimization, and intelligent healthcare monitoring. Recurring topics include flexibility, usage of energy, agreement procedures, and compatibility. Novel protocols for cryptography, light blockchain implementations, and safe model training and aggregation methodologies are some of the suggested answers. With the help of these new technologies, the future is headed toward a united, safe, and intelligent infrastructure for Society 4.0.

3. Problem Statement

There is still much to be done to address issues with privacy of data [18], excessive latency [25], lack of confidence in federated environments [30], ineffective consensus algorithms, and flexibility in distributed surroundings, even with the advancements in blockchain, artificial intelligence, and edge computing for safe and clever interactions in future IoT networks. These limitations restrict the use of resource-efficient, real-time, safe systems to vital fields including intelligent cities, industrial IoT, and healthcare. We introduce ChainGuard 6G+, a revolutionary blockchain-based secure system with federated AI, to fill these gaps in knowledge. To enable safe data sharing and reliable decision-making in 6G-powered IoT systems, our approach combines federated learning of distributed model training, an environmentally friendly scalability blockchain platform with optimised consensus techniques, and state-of-the-art encryption methods.

4. Objectives

1. Design a privacy-preserving architecture for 6G-enabled IoT networks by integrating Federated Learning and blockchain technologies.
2. Enable secure and decentralized anomaly detection using LSTM models trained on edge devices without sharing raw data.

3. Establish trust, authentication, and tamper-proof coordination using private Ethereum blockchain and smart contracts.
4. Enhance user privacy by applying differential privacy to local model updates before global aggregation.
5. Evaluate the proposed architecture's performance in terms of model accuracy, latency, and communication efficiency compared to baseline models.

5. Proposed Methodology for ChainGuard 6G+: A Secure and Private Architecture for Wireless Communication Using Federated Learning and Blockchain in IoT Networks

Federated Learning is a distributed machine learning approach in which multiple clients train a global model in parallel without revealing their raw data, thereby enhancing privacy and security—most effective in sensitive domains like healthcare, finance, and edge computing. FL can be decentralized or centralized. Privacy is further boosted using methods like Differential Privacy, introducing noise into updates to the model, and Blockchain, ensuring secure, immutable recording of model parameters. FL has performed well in applications like privacy-preserving health analytics, collaborative fraud detection in finance, and on-device personalization services in edge computing settings. Figure 1 shows Federated Learning with Differential Privacy and Blockchain for Secure and Privacy-Preserving Model Training in IoT Networks.

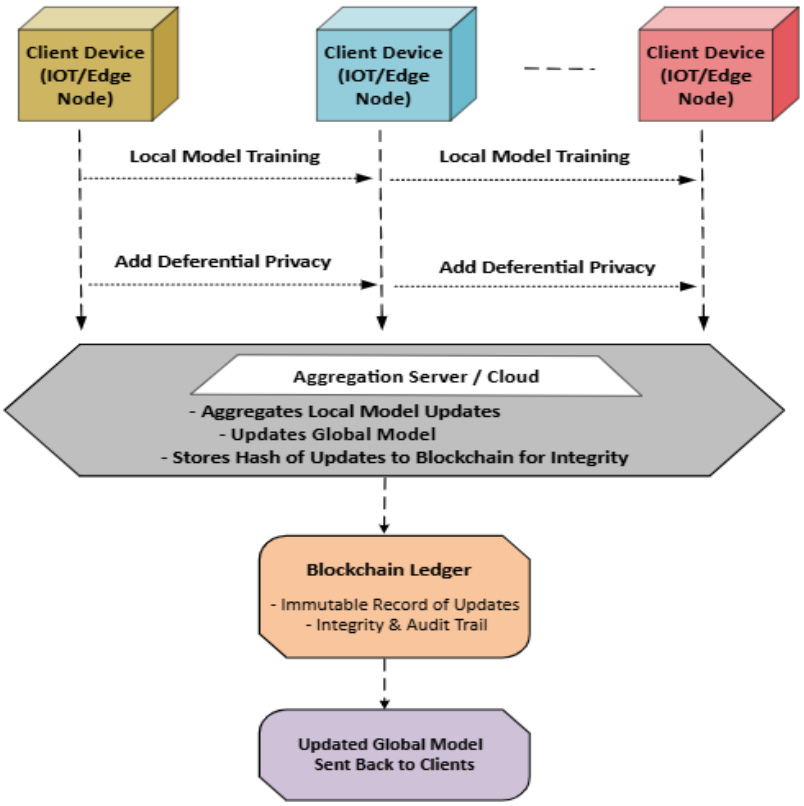

Figure 1. Federated Learning with Differential Privacy and Blockchain for Secure and Privacy-Preserving Model Training in IoT Networks

5.1 Data Collection

6G Network Slice Security Attack Detection Dataset [33] from Kaggle, consists of both synthetic and actual data in the shape of several types of cyberattacks against varied 6G network slices. The dataset contains labeled traffic flows with regular and attack activity from control and user planes, making detailed attack analysis possible. Notable features include source/destination IPs, port numbers, protocol types, payload length, timing features, and attack types such as DoS, DDoS, probing, and spoofing. Preprocessing of data comprised missing value cleansing, normalization, encoding categorical variables, and breaking flows into chunks based on time windows to obtain structured samples to train and test. The trained dataset was employed as the preferred input for models of anomaly detection in a context of 6G network slicing. Table 1 shows Overview of 6G Network Slice Security Attack Detection Dataset.

Table 1: Overview of 6G Network Slice Security Attack Detection Dataset

Aspect	**Description**
Source	Kaggle [33]
Data Type	Combination of synthetic and real-world data
Purpose	Cyberattack detection in 6G network slices
Content	Labeled traffic flows from control and user planes
Key Features	Source/Destination IPs, Port Numbers, Protocol Types, Payload Length, Timing Features, Attack Types
Attack Types	DoS, DDoS, Probing, Spoofing
Preprocessing Steps	Missing value cleansing, Normalization, Encoding categorical variables, Time window chunking
Use Case	Input for training and testing models for anomaly detection in 6G network slicing environments

5.2 Data Preprocessing Using Min Max Normalization

Each edge device does local data preprocessing to prepare TON-IoT data for federated training of models. It includes cleaning of data to eliminate missing or unnecessary records and consistency. In scaling feature values and improving convergence of the model, we utilize Min-Max Normalization that linearly rescales features within a fixed interval, usually [0, 1], and is depicted by equation (1):

$$x' = (x - x\text{min})/(x\text{max} - x\text{min}) \quad (1)$$

where x is the original feature value, x_{min} and x_{max} are the minimum and maximum feature values, respectively, and x' is the normalized value.

For n-dimensional sets of features, each feature xi $(i \in 1.n)$ is normalized separately as in equation (2):

$$x'i = (xi - \min(xi))/(\max(xi) - \min(xi)) \quad (2)$$

To process streaming input in time series, the data is restructured in a sliding window of size w and stride s into a 2D matrix input for LSTM models as presented in equation (3):

$$Xt = [xt - w + 1, xt - w + 2, \ldots, xt] \quad (3)$$

After normalization and sequence formatting, we perform light feature selection according to entropy-based scoring, where the entropy of discrete feature f with value set V is defined in equation (4):

$$H(f) = -\sum p(v)\log_2 p(v), \text{ for } v \in V \quad (4)$$

These preprocessing operations make sure the data is clean, scaled, sequentially arranged, and optimized for training LSTM models in federated settings on resource-constrained edge devices. Figure 2 shows LSTM Architecture.

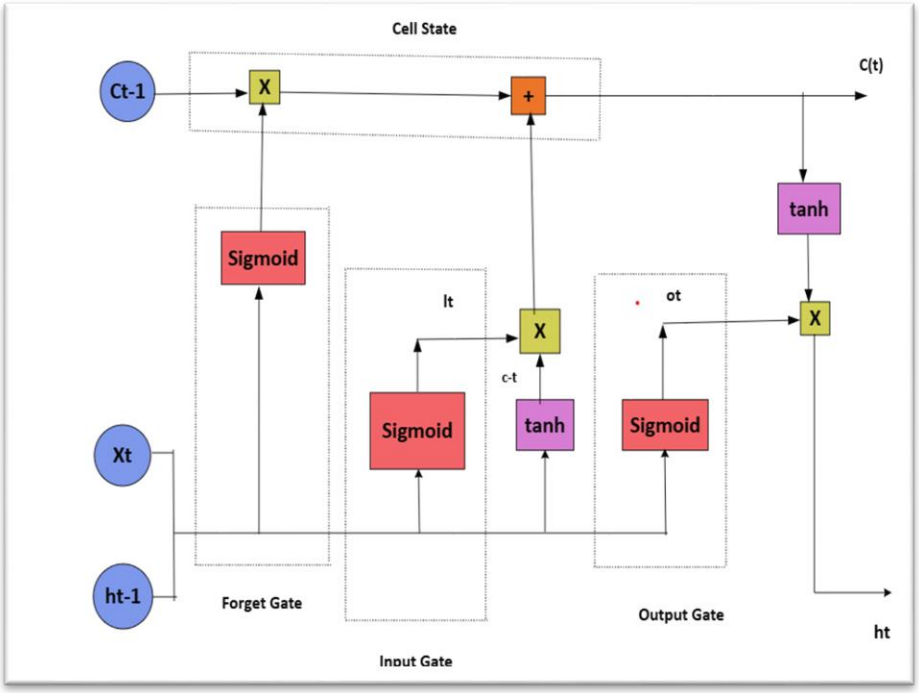

Figure 2. LSTM Architecture

LSTM is a type of recurrent neural network designed carefully to manage and learn sequential data by solving the vanishing gradient problem encountered in typical RNNs. LSTM architecture has memory cells that maintain information during long sequences with three major gates—input gate, forget gate, and output gate—to control the information flow. These gates permit the network to selectively forget or remember information in every time step, essentially extracting temporal dependencies and distant patterns within time-series data. The LSTM can mimic complex periodic conduct, like that of internet traffic or IoT telemetry streams, because it modifies the cell information and concealed state in every phase based on the previous context and present input. LSTM is widely used in applications including identifying anomalies, recognizing speech, and predictive care for linear and dynamic structures due to its ability to store long-term dependencies. Federated LSTM Architecture is depicted in Figure 3.

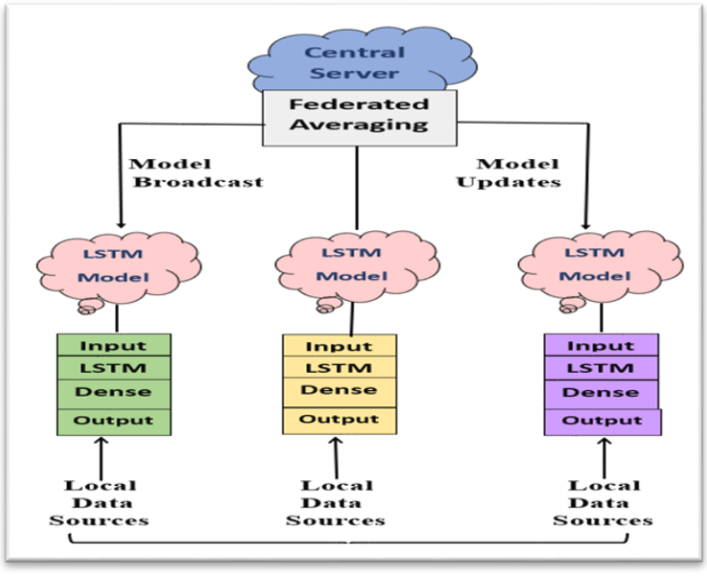

Figure 3. Federated LSTM Architecture

Federated LSTM trains a shared LSTM model cooperatively without sharing raw data by utilizing numerous edge devices. After receiving a global approach, every gadget computes fresh weights and train it locally using IoT time-series data. To create a new planetary model, these are routed to a central aggregate that uses Federation Average. At every edge, the LSTM layer analyzes consecutive sensor data to identify temporal trends and anomalies. For 6G-enabled IoT networks, the distributed architecture guarantees data privacy, scalability, and real-time anomaly detection. The ChainGuard 6G+ Framework's preprocessing methods are displayed in Table 2.

Table 2: Data Preprocessing Techniques Used in ChainGuard 6G+ Framework

Step No.	Preprocessing Task	Description	Mathematical Expression / Equation
1	Data Cleaning	Removes missing, corrupted, or irrelevant entries from the TON-IoT dataset	-
2	Min-Max Normalization	Scales feature values to a fixed range [0, 1] for improved model convergence	$x' = (x - x\min)/(x\max - x\min)$
3	Multi-dimensional Normalization	Normalizes each feature xi individually across n dimensions	$x'i = (xi - \min(xi))/(\max(xi) - \min(xi))$
4	Time-Series Windowing	Segments sequential data using a sliding window of size w and stride s	$Xt = [xt - w + 1, xt - w + 2, \dots, xt]$
5	Feature Selection (Entropy-Based)	Scores and selects relevant features based on information gain	$H(f) = -\sum p(v) \log_2 p(v)$, for $v \in V$

5.3 Federated Model Training

A Federated Long Short-Term Memory model is deployed on edge devices using TensorFlow Federated to enable collaborative but privacy-preserving anomaly detection.

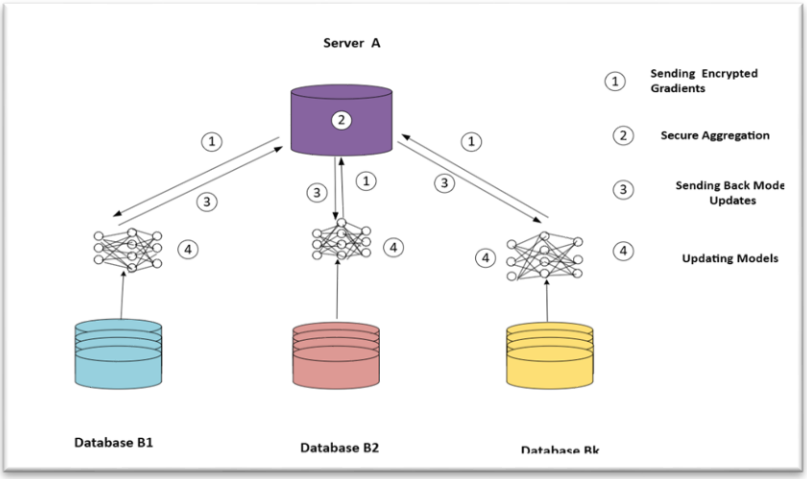

Figure 4. Architecture of Federated Learning

Federated learning is a decentralized learning system that preserves the privacy and security of local data while enabling several edge gadgets or users to jointly train a collective model. Federated learning ensures that only model updates—such as gradients or weights parameters—are shared, in contrast to traditional centralized methods of learning, which send raw data to a single node for training. This design significantly reduces latency, bandwidth usage, and privacy risks, making it ideal for resource-constrained settings like Internet of Things networks. Federated learning algorithms generally include local training for each device, aggregation of local models at a central server via methods such as Federated Averaging, and repeated updates over several communication rounds. Through retention of data locality and reduced susceptibility to outside sources of danger, federated learning aids in fulfilling data privacy legal requirements and maintaining the strength of distributed AI algorithms. Figure 4 shows Architecture of federated learning. Each edge device trains the model locally from pre-processed TON-IoT data without uploading raw data to the central server. Instead, only local model updates are shared, ensuring data privacy.

Let xi be the local data at device i. The local loss function $\mathcal{L}i(\theta)$ at each device is determined using the model parameters θ in equation (5):

$$\mathcal{L}i(\theta) = 1/|\text{xi}| \sum \ \ell(\text{yi}, \text{f}\Theta(\text{xi})) \qquad (5)$$

where $\ell(\cdot)$ is the loss function, $f\theta(xi)$ is the output of the LSTM model, and yi are the corresponding labels.

Following local training, each device computes a gradient update $\Delta\theta i$ and sends it to the aggregator. The global server aggregates the updates with Federated Averaging represented as equation (6):

$$\theta\text{t} + 1 = \sum \ \text{ni}/\text{n} \cdot \theta\text{i} \qquad (6)$$

where ni is the number of samples on device i, n is the total number of samples on all devices, and θi is the local updated model on device i.

The LSTM model on each device receives sequential input $Xt \in \mathbb{R}w \times d$ and updates hidden state ht and cell state ct as in equation (7):

$$\text{ht, ct} = \text{LSTM}(Xt, ht - 1, ct - 1) \qquad (7)$$

This enables temporal pattern learning for anomaly detection in streaming IoT streams.

For improved convergence in decentralized training, local models perform gradient-based updates with learning rate η in equation (8):

$$\theta\text{i} \leftarrow \theta\text{i} - \eta \cdot \nabla\mathcal{L}(\theta\text{i}) \qquad (8)$$

This is repeated over multiple rounds of communication until the global model converges. This federated training reduces model robustness and privacy violations while keeping communication overhead low in the 6G IoT edge environment. Table 3 shows Federated LSTM Model Training Workflow.

Table 3: Federated LSTM Model Training Workflow

Step No.	Component/Task	Description	Equation No. & Expression
1	Local Loss Function	Calculates training error on each device using local data and model parameters	$\mathcal{L}i(\theta) = 1/\|\text{xi}\| \sum \ \ell(\text{yi}, \text{f}\Theta(\text{xi}))$
2	Model Aggregation	Aggregates local model updates to form a new global model	$\theta\text{t} + 1 = \sum \ \text{ni}/\text{n} \cdot \theta\text{i}$
3	LSTM State Update	Updates LSTM hidden and cell states for sequential data input	$\text{ht, ct} = \text{LSTM}(\text{Xt}, \text{ht} - 1, \text{ct} - 1)$
4	Local Gradient Descent Update	Optimizes the local model on each device using gradient descent	$\theta\text{i} \leftarrow \theta\text{i} - \eta \cdot \nabla\mathcal{L}(\theta\text{i})$

5.4 Blockchain Integration and Privacy Preservation

For the sake of offering secure, transparent, and privacy-preserving federated learning across the 6G-enabled IoT environment, we integrate a private Ethereum blockchain with Differential Privacy controls. The integration of blockchain in the ChainGuard 6G+ architecture to offer secure, transparent, and trust-based coordination of federated learning between decentralized IoT edge nodes. In this, edge node updates are digitally signed and made public as transactions to a private Ethereum blockchain. Smart contracts validate these updates, implement authentication, and store every validated transaction immutably. Once validated, the model update block is added to the distributed ledger, and secure session keys are managed using blockchain for end-to-end encrypted communication. Decentralized in this way, the process protects against tampering, model integrity, and enhances accountability while enabling privacy-preserving learning using Differential Privacy mechanisms. Figure 5 shows Blockchain Integration for Secure Federated Learning in ChainGuard 6G+ Architecture.

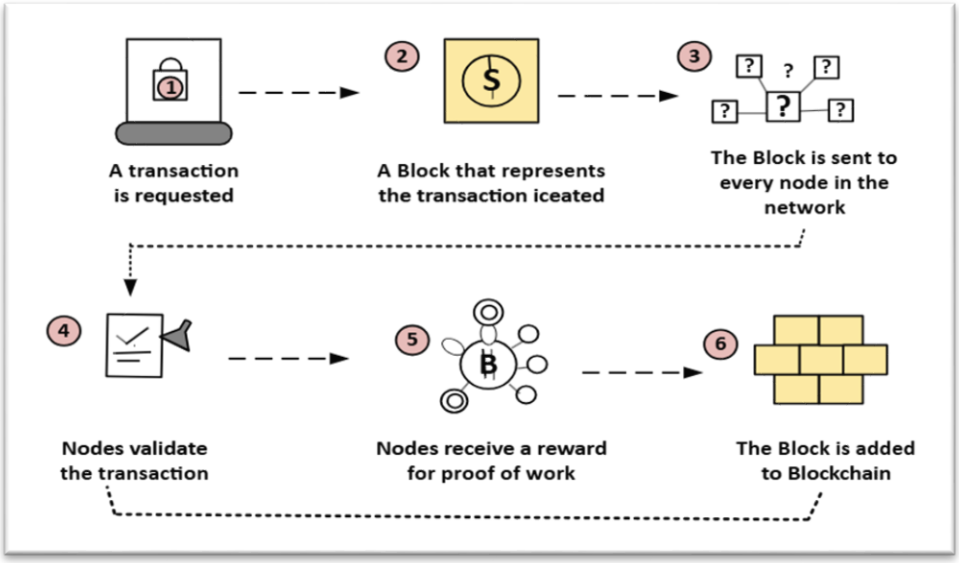

Figure 5. Blockchain Integration for Secure Federated Learning in ChainGuard 6G+ Architecture

Each edge device signs its model update θi with a digital signature scheme before uploading it to the blockchain. The signature σi is generated with the sender's private key sk_i as demonstrated in equation (9):

$$\sigma \mathrm{i} = \mathrm{Sign}(\mathrm{sk_i i}, \theta \mathrm{i}) \quad (9)$$

The blockchain smart contract verifies validity of each update using the corresponding public key pk_i in equation (10):

$$\mathrm{Verify}(\mathrm{pk\_i}, Ɵ\mathrm{i}, б\mathrm{i}) = \mathrm{True} \quad (10)$$

This promise ensures that only authenticated and trusted devices update the global model. We apply ε −Differential Privacy on the local gradient updates before aggregation to ensure user data privacy in federated learning. The private noisy gradient update θi is given as in equation (11):

$$\theta i = \theta i + N(0, \sigma^2) \quad (11)$$

where $N(0, \sigma^2)$ is the gradient function's ε and Δf sensitivity scaled Gaussian noise.

The privacy guarantee can be stated formally as in equation (12):

$$P[M(D1) \in S] \leq e^{\wedge}\varepsilon \cdot P[M(D2) \in S] \quad (12)$$

for all neighboring datasets $D1, D2$ that differ by one record, and for all possible mechanism's outputs S of mechanism M.

This hybrid integration of differential privacy and blockchain offers gradient leakage-resistant, tamper-proof model coordination with establishment of trust, data confidentiality, and accountability in federated IoT systems. Table 4 shows Blockchain Integration and Privacy Preservation in Federated Learning.

Table 4: Blockchain Integration and Privacy Preservation in Federated Learning

Step No.	**Component/Task**	**Description**
1	Digital Signature Generation	Each edge device signs its local model update to ensure authenticity using its private key.
2	Smart Contract Verification	The blockchain smart contract verifies the model update's validity.
3	Differential Privacy	Applies ε-Differential Privacy to the model's gradient updates to protect user data from inference attacks.
4	Privacy Guarantee	Ensures privacy by bounding the probability of inference attacks between adjacent datasets.

5.5 Secure Communication and Performance Evaluation

TLS 1.3 offers better security and performance than previous versions, with dynamic key management and rotation supported through blockchain-based smart contracts. Let public key pk_i of edge device i be used for TLS handshake, and the session key $K\_session$ is computed as in equation (13):

$$K\_session = KDF(pk\_i, sk\_i) \quad (13)$$

Where, KDF generates the session key $K\_session$ from the public key pk_i and private key sk_i of the edge device.

For trust establishment and secure key rotation, the blockchain smart contract stores and maintains the versions of keys. Let the blockchain contract maintain the history of key updates over time, with each version of the key being represented as $K\_version$ in equation (14):

$$K\_version = Contract\_update(pk\_i, K\_session) \quad (14)$$

This makes rotation and renewal of session keys transparent and secure in real-time, preventing potential interception and man-in-the-middle attacks.

Performance of the federated learning system is evaluated through three most important indicators: model accuracy, blockchain latency, and network efficiency. Model accuracy is gauged by the error rate of global model classification, described by equation (15):

$$CER = (1/N) \sum (yi \neq f\Theta(xi)) \quad (15)$$

where yi is the true label, $f\theta(xi)$ is the predicted label, and N is the number of test samples.

Blockchain Latency: This refers to the time during which the model update has been verified and logged in the blockchain, and it is represented by equation (16):

$$Blockchain\_Latency = T\_verification + T\_logging \quad (16)$$

where $T\_verification$ is the time period for smart contract verification and $T\_logging$ is the time period for logging the transaction to the blockchain.

The efficiency of the network in the system is compared by analyzing the communication overhead of federated learning and blockchain-integrated federated learning. This overhead is given by equation (17):

$$Communication\_Overhead = (Data\_size\_fed - Data\_size\_centralized) / Data\_size\_centralized \quad (17)$$

Where, $Data\_size\_fed$ is the data communicated in the federated learning system, and $Data\_size\_centralized$ is the data communicated in a normal centralized learning system.

Based on such performance metrics, the system's performance is compared with centralized and non-blockchain federated learning models against model accuracy, latency, and efficiency in the 6G IoT environment.

The ChainGuard 6G+ architecture incorporates federated learning and blockchain for a secure and privacy-preserving wireless communication platform in IoT-based 6G networks. Distributed IoT devices over various

network slices collect real-time data, which is locally pre-processed through cleaning, normalization, and segmentation. Every edge node learns a local model on such data, uses differential privacy in the form of model update noise addition, and packages the updates into blockchain transactions for secure and permanent storage. During every FL round, a collection of clients is selected and their differentially private model updates are verified and stored on the blockchain. The system also enforces role-based access control for safe data and model access, offers encrypted data storage and transmission, and uses blockchain for tamper-proof auditing and logging while maintaining compliance with security and privacy regulations in future IoT networks. Table 5 shows Pseudocode: ChainGuard 6G+ – Federated Learning and Blockchain for Secure 6G-IoT.

Table 5: Pseudocode: ChainGuard 6G+ – Federated Learning and Blockchain for Secure 6G-IoT

Pseudocode: ChainGuard 6G+ – Federated Learning and Blockchain for Secure 6G-IoT	
Input: *IoT device data from 6G network slices*	
Output: *Privacy-preserving anomaly detection and secure model management*	
*// **Initialization***	
Deploy IoT devices across multiple 6G network slices	*// Data Sources*
Initialize local models on edge nodes	*// FL Setup*
Define global model architecture and aggregation server	*// FL Coordination*
Set privacy parameters for Differential Privacy	*// Privacy Control*
Initialize blockchain ledger for model audit and immutability	*// Security Ledger*
*// **Data Collection and Preprocessing***	
FOR each IoT client device DO	
Collect real-time traffic data from control and user planes	*// Data Capture*
Preprocess data: clean, normalize, encode categorical values	*// Data Cleansing*
Segment data into time-based windows	*// Structured Samples*
END FOR	
*// **Federated Learning Loop***	
FOR each training round r = 1 TO R DO	
Select subset of clients for participation	*// Client Selection*
PARALLEL FOR each selected client k DO	
Train local model W_k on local traffic data	*// Local Training*
Add DP noise to W_k to get W_k'	*// Differential Privacy*
Create blockchain transaction Tx_k with model update	*// Blockchain Packaging*
Sign and broadcast Tx_k to blockchain network	*//Secure Update Transmission*
END PARALLEL FOR	
Blockchain network validates and records valid Tx_k	*// Immutable Logging*
Aggregate validated W_k' models into global model W_r+1	*// Federated Aggregation*
Broadcast updated global model to all clients	*// Model Synchronization*

END FOR	
// Anomaly Detection and Security Enforcement	
Deploy trained global model to edge nodes	*// Edge Intelligence*
Apply model to detect cyberattacks in real-time network traffic	*// Intrusion Detection*
Trigger alerts for DoS/DDoS/probing/spoofing anomalies	*// Threat Response*
// Access Control and Compliance	
Enforce role-based access control on model and data access	*// Data Governance*
Ensure encrypted storage of updates and logs	*// Confidentiality*
Audit compliance using blockchain logs	*// Regulatory Compliance*

6. Results and Discussion

The results confirm the superior performance of the federated learning-based model in accurately detecting anomalies and protecting 6G network slices with high precision, recall, and overall accuracy. The proposed architecture attains well-balanced sensitivity and specificity, as reflected by the low False Negative Rate and False Positive Rate, ensuring robust security without inducing excessive false alarms.

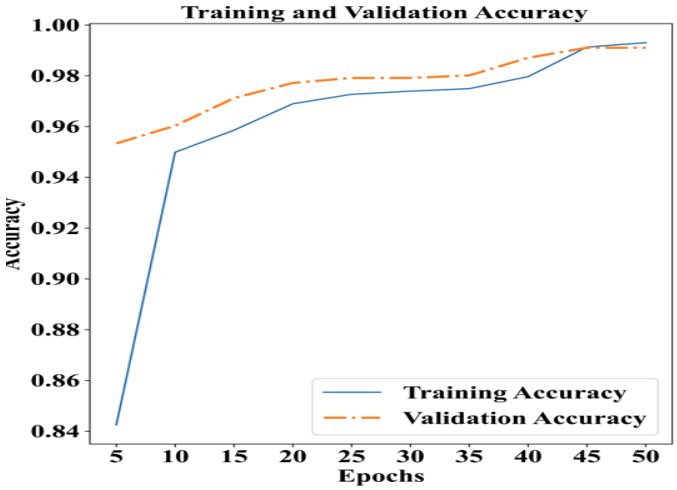

Figure 6. Training and Validation Accuracy

The federated learning model's effectiveness over several communication rounds is displayed in the training and validation accuracy plot, which also shows the degree to which the model extends to new information as it gains knowledge from dispersed client changes. With minor fluctuations due to the variation in client information dispersion and the inclusion of different privacy noise, validation and training accuracy levels both increase gradually at first as the model learns significant trends in the local datasets. While validation accuracy plateaus over time, highlighting the compromise between learning and generalizing, training accuracy keeps increasing over time, demonstrating the model's growing capacity to match the local data. The final model accomplishes an accuracy rate of almost 96.2%, demonstrating the efficacy of integrating federated learning with secure techniques for secure model training with accuracy in diverse IoT environments. The overall trend shows security in integration and good efficiency. Training and Validation Accuracy are displayed in Figure 6.

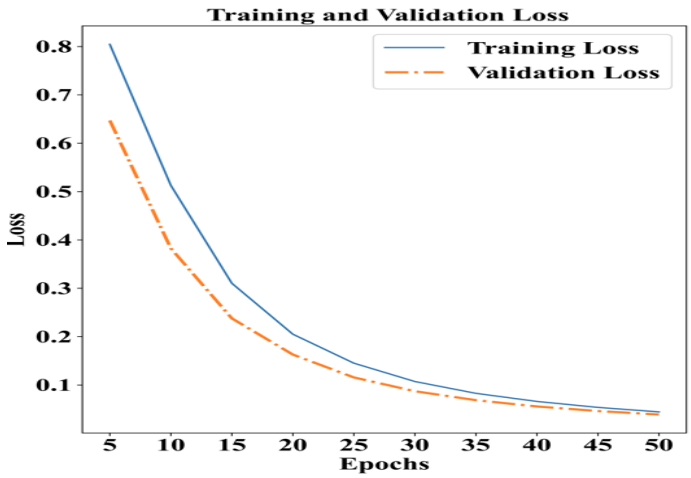

Figure 7. Training and Validation Loss

The plot of training and validation loss is a nice visualization of the model's optimization process over successive rounds of communication in the federated learning setting. Training and validation losses are relatively high initially since the model has not observed much distributed data. As the iterations pass, training loss gradually reduces, indicating that the model is actually minimizing the error on local client datasets. Meanwhile, validation loss also comes down but with a lesser speed due to the model to learn generalizing from unseen data. Loss validation will rise and then return to itself due to increased noise for differential privacy, non-iid data distributions, etc. Nevertheless, reducing overall confirms that there is convergence and learning stability. The loss values at the conclusion inform us that the model has learned robust patterns while maintaining confidentiality, illustrating the efficacy of federated learning in secure, decentralized settings. Figure 7 shows Training and Validation Loss.

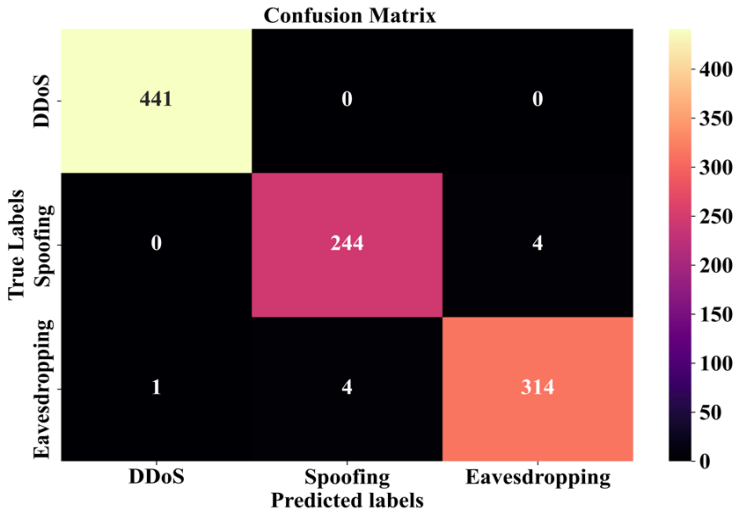

Figure 8. Confusion Matrix

The confusion matrix plot visually displays the classification accuracy of the federated learning model through the comparison of predicted labels against the test set is actual labels. Each cell in the matrix is the count of instances in which the model predicted a specific class versus the actual class, allowing for accurate investigation of true positives, true negatives, false positives, and false negatives. High diagonal dominance of the matrix indicates high accuracy, i.e., the model has correctly predicted the majority of the samples. Off-diagonal entries indicate misclassifications, which show some classes that the model may struggle to differentiate between. This information is helpful in improving model performance and learning its behavior in multi-class classification tasks. The confusion matrix thus becomes an effective way of verifying the reliability and accuracy of the trained model in a federated learning environment. Figure 8 shows Confusion Matrix.

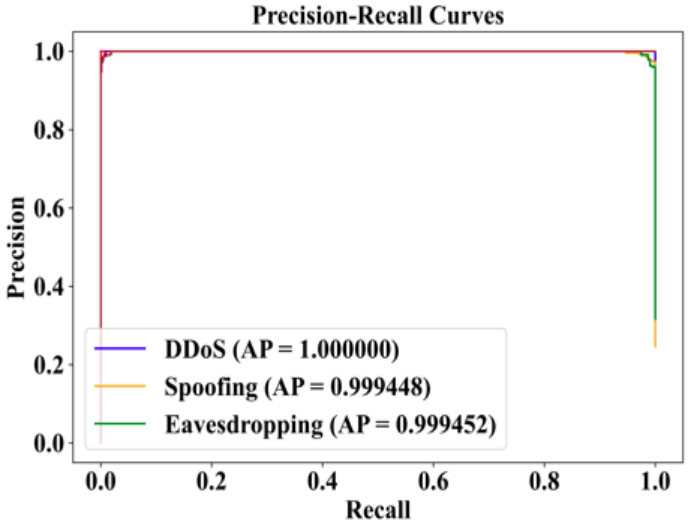

Figure 9. Precision-Recall Curves

The precision-recall plot shows the precision-recall trade-off for all classes in the federated learning model graphically. It is especially helpful when dealing with unbalanced datasets, when accuracy on its alone might be deceptive. The model's ability to classify classes is shown by the curve for each class; a larger area under the curve denotes better performance. Larger and smaller curves indicate that the model has a high recall and precision, which reduces false positives and false negatives. Examining these curves makes it clear how effectively the model performs when classifying data using various thresholds and provides crucial information about how reliable and robust it is when classifying all classes in a federated setting that protects privacy. Precision-Recall Curves are displayed in Figure 9.

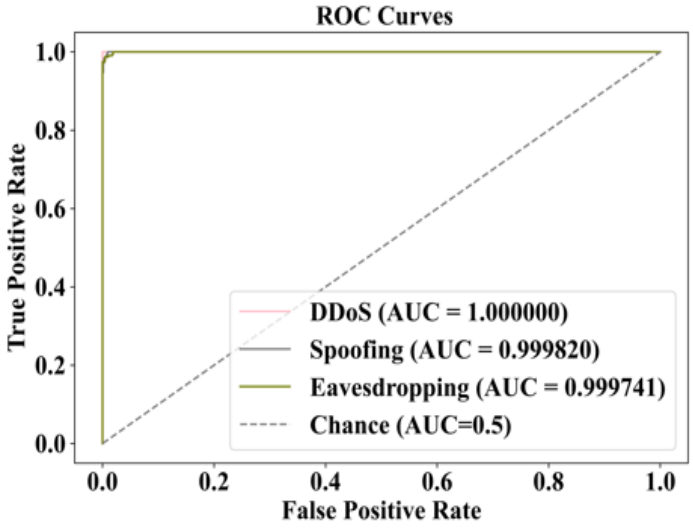

Figure 10. ROC Curves

Every curve represents the discrimination of the model between the positive and negative classes, and the closer a curve is to the top-left, the better is the classification performance. Area Under the Curve provides a scalar score capturing the model's discriminative capability—higher AUC indicates better generalization and classification performance. ROC curves validate the resilience of the model to correctly recognize attack types or class labels in secure 6G network slice detection, testifying to the effectiveness of federated training and privacy-preserving methods in achieving high detection rates among scattered clients. Figure 10 shows ROC Curves.

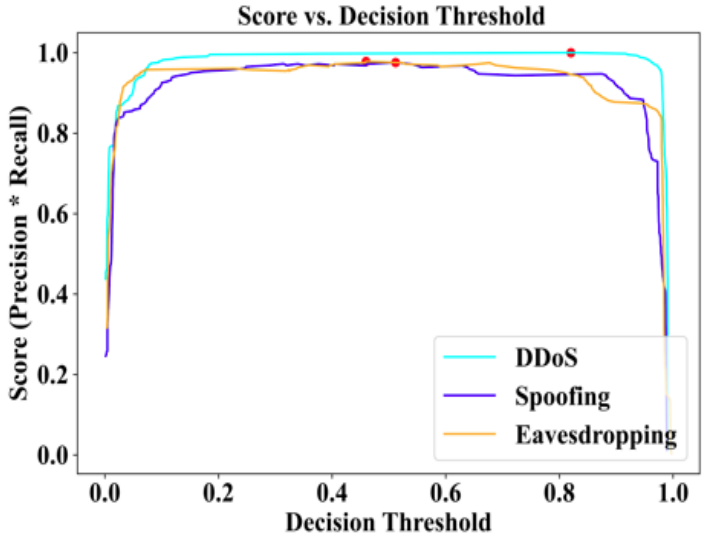

Figure 11. Score vs Decision Threshold

This graph plots the relation between class scores and various decision thresholds used by the federated learning model in determining class membership. With different values of threshold, the graph shows the precision-recall curve along with how sure the model is of the class membership at varying score values. This curve is invaluable in model performance tuning, particularly in cases where the cost of false positives and false negatives hugely varies, e.g., secure 6G network slice security detection. With a glance at the graph, the optimal value of the threshold for balancing specificity and sensitivity resulting in reliable decision-making without violating privacy and precision in federated environments can be identified. Figure 11 shows Score vs Decision Threshold.

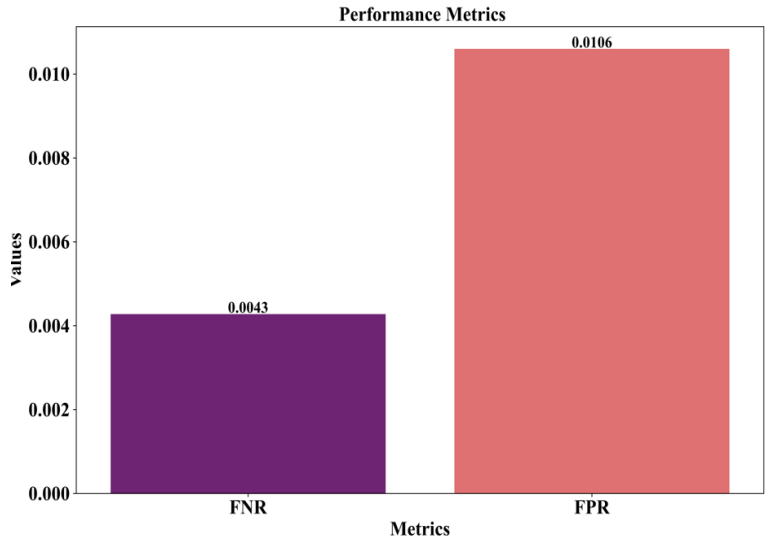

Figure 12. Performance Metrices of Two Primary Error Metrics – FNR and FPR

FNR and FPR are the two main error metrics shown in the bar chart. These metrics are essential for assessing the legitimacy of the federated learning-based anomalies detection method for 6G networking slice safety. The FNR, which stands at about 0.0043, is a very small percentage of real attacks that were mistakenly classified as regular traffic, indicating that the model is highly sensitive in identifying real threats. The FPR, on the other hand, is the ratio of harmless activities that are incorrectly classified as attacks, and it is approximately 0.0106. The FPR is comparatively low, although being somewhat higher than the FNR, demonstrating the accuracy and decreased risk of false alarms of the secure federated learning system that was put into place. The implemented secure federated learning framework's resilience and dependability in reducing the most significant categorization errors in upcoming wireless IoT environments are demonstrated overall by these performance measures. The performance metrics of the two main error measures, FNR and FPR, are displayed in Figure 12.

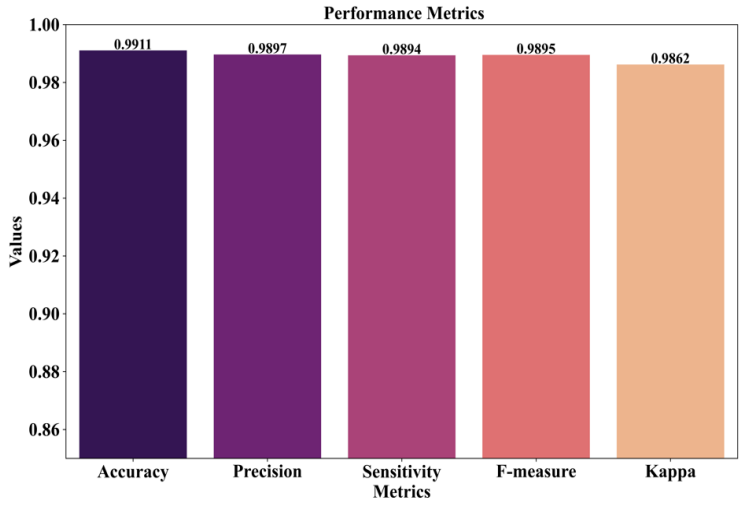

Figure 13. Performance Metrices of the Proposed Model

The bar chart indicates a comprehensive study of the performance of the model on five significant parameters: Accuracy, Precision, Sensitivity, F-measure, and Kappa score. The model was highly accurate at 0.9911, reflecting high overall correctness in prediction. Precision and sensitivity measures, which are strongly correlated at 0.9897 and 0.9894. The F-measure, harmonic mean of precision and recall, is 0.9895, further highlighting the model's highly balanced performance in detection and relevance. Furthermore, the Kappa score of 0.9862 indicates very high agreement between predicted and actual classifications even after adjusting for random chance. In total, these steps demonstrate the robustness, reliability, and suitability of the current architecture in delivering accurate and privacy-preserving anomaly detection in future generations of IoT-enabled wireless communication networks. Figure 13 shows Performance Metrices of the Proposed Model.

Table 6: Comparative Performance Analysis of Proposed Method with Existing Approaches

Method	Accuracy	Precision	Recall	F1-Score
Transfer Attention Learning [34]	92	88	90	89
KNN [35]	86	95	97	91
SVM [35]	89	95	91	93
Proposed Fed LSTM	99.1	98.9	98.9	98.9

For anomaly detection in 6G IoT network scenarios, Table 6 compares the performance of the suggested Federated LSTM model with popular machine learning techniques as Transfer Focused Learning, K-Nearest Neighbors, and Support Vector Machine. The results clearly demonstrate the suggested Fed LSTM model's better performance, with an F1-score of 98.9%, a remarkable accuracy of 99.1%, and precision and recall of 98.9%. When compared to the suggested approach, Transfer Attention Learning produces an accuracy of 92% with lower precision and recall values, whilst KNN and SVM, albeit having high precision 95% and recall, perform poorly overall. These findings support the privacy-preserving federated learning model's superiority in improving detection precision, reducing false positives and negatives, and promoting strong security against dispersed 6G IoT networks. The suggested method's comparison evaluation of performance with current methods is displayed in Table 6.

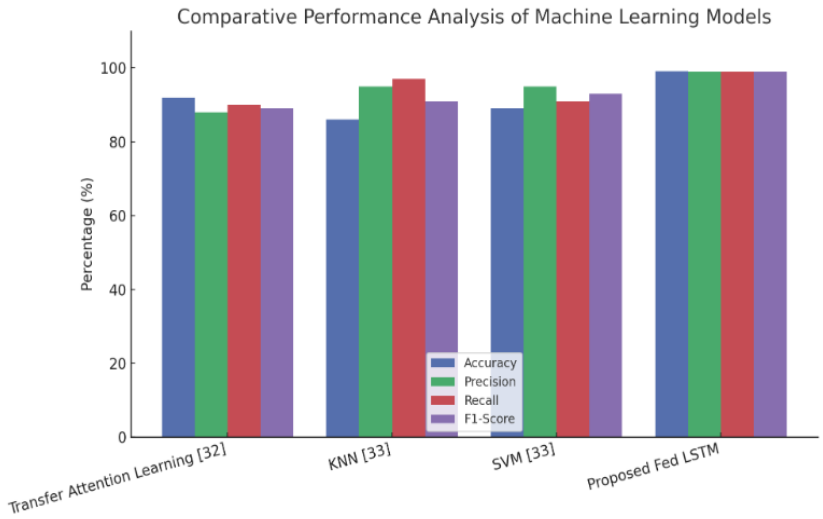

Figure 14. Comparative Performance Analysis of Machine Learning Models Based on Accuracy, Precision, Recall, and F1-Score

Transfer Attention Learning, K-Nearest Neighbors, Support Vector Machine, and the suggested Federated LSTM—based on four significant evaluation metrics: Accuracy, Precision, Recall, and F1-Score. Out of all the techniques, the proposed Federated LSTM model outperforms others with the best scores on all measures, accuracy of 99.1%, precision of 98.9%, recall of 98.9%, and F1-score of 98.9%. Transfer Attention Learning, on the other hand, has relatively moderate performance especially in precision and recall, while the performance of KNN and SVM is excellent in precision but lags behind in overall accuracy and recall. This difference highlights the superior efficiency and robustness of the proposed Federated LSTM approach for secure and privacy-preserving anomaly detection in 6G IoT network systems. Figure 14 shows Comparative Performance Analysis of Machine Learning Models Based on Accuracy, Precision, Recall, and F1-Score.

7. Discussion

The comparative performance analysis clearly indicates the superior efficiency of the proposed Federated LSTM method over traditional machine learning techniques in securing 6G network slice environments. While methods like Transfer Attention Learning [34], KNN [35] and SVM [35], exhibit respectable classification performance, they fall short in terms of attaining an equal balance. In particular, the Proposed Fed LSTM model also boasts a staggering accuracy rate of 99.1% with very close precision, recall, and F1-score values of 98.9%, indicating its consistency and robustness in recognizing both the attack and benign instances with minimal error. The inclusion of federated learning allows the model to harness decentralized data while maintaining users' privacy, while the temporal learning capability of LSTM enhances its performance in adapting to the dynamic properties of IoT network traffic. The high-performance profile also warrants the model's reliability to be utilized in real-world use cases in privacy-sensitive next-generation wireless communication networks, especially security threat mitigation at the edge in a decentralized 6G IoT network.

8. Conclusion and Future Work

By fusing blockchain technology with federated learning, the ChainGuard 6G+ architecture offers in next-generation IoT networks. The hybrid approach offers a strong foundation for anomaly detection with data confidentiality assured, thereby resolving the privacy and security issues. Strong accuracy, precision, and recall values demonstrate the model's strong performance and demonstrate its viability for efficient real-time threat detection in 6G network slices. By eliminating sensitive data from being continuously saved, federated learning enables the platform to mitigate potential dangers related to centralised storage of data. By enabling open and impenetrable logging of messages and actions, the use of blockchain enhances system safety. For future work, several areas of future development for the provided architecture are possible. Enhancing the performance of communication protocols in handling larger quantities of data in highly distributed environments is one area of development. Enabling the scalability of federated learning models to accommodate more IoT devices in 6G networks to be able to sustain performance as the network grows is also important. Further research could explore more advanced blockchain consensus algorithms and their integration with federated learning to increase system reliability and reduce latency. Finally, applying it to dynamic threat modeling and real-time adaptation against emerging attack vectors would further render it extremely flexible and effective in safeguarding next-generation wireless communication systems.

Acknowledgement: The author would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

Funding Statement: I would like to acknowledge the initial support received from Jadara University under grant number Jadara-SR-Full2023. This support played a vital role in facilitating this research.

Availability of Data and Materials: The author confirm that the data supporting the findings of this study is available within the article.

Conflicts of Interest: The author declare that they have no conflicts of interest to report regarding the present study.

References

[1] O. Friha, M. A. Ferrag, B. Kantarci, B. Cakmak, A. Ozgun, and N. Ghoualmi-Zine, "LLM-Based Edge Intelligence: A Comprehensive Survey on Architectures, Applications, Security and Trustworthiness," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 5799–5856, 2024, doi: 10.1109/OJCOMS.2024.3456549.

[2] S. Bhattacharya et al., "Blockchain for Internet of Underwater Things: State-of-the-Art, Applications, Challenges, and Future Directions," *Sustainability*, vol. 14, no. 23, Art. no. 23, Jan. 2022, doi: 10.3390/su142315659.

[3] S. Jamil, M. Rahman, and Fawad, "A Comprehensive Survey of Digital Twins and Federated Learning for Industrial Internet of Things (IIoT), Internet of Vehicles (IoV) and Internet of Drones (IoD)," *Appl. Syst. Innov.*, vol. 5, no. 3, Art. no. 3, Jun. 2022, doi: 10.3390/asi5030056.

[4] A. C. R., A. K. Pani, and P. Kumar, "Blockchain-enabled Smart Contracts and the Internet of Things: Advancing the research agenda through a narrative review," *Multimed. Tools Appl.*, vol. 84, no. 8, pp. 5097–5147, Mar. 2025, doi: 10.1007/s11042-024-18931-4.

[5] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "Blockchain Integration in the Era of Industrial Metaverse," *Appl. Sci.*, vol. 13, no. 3, Art. no. 3, Jan. 2023, doi: 10.3390/app13031353.

[6] S. Jain et al., "Blockchain and Autonomous Vehicles: Recent Advances and Future Directions," *IEEE Access*, vol. 9, pp. 130264–130328, 2021, doi: 10.1109/ACCESS.2021.3113649.

[7] P. Koukaras et al., "Integrating Blockchain in Smart Grids for Enhanced Demand Response: Challenges, Strategies, and Future Directions," *Energies*, vol. 17, no. 5, Art. no. 5, Jan. 2024, doi: 10.3390/en17051007.

[8] C. D. Morar and D. E. Popescu, "A Survey of Blockchain Applicability, Challenges, and Key Threats," *Computers*, vol. 13, no. 9, Art. no. 9, Sep. 2024, doi: 10.3390/computers13090223.

[9] N. Jin, K. Meng, J. Ding, L. Sun, H. Wu, and X. Chen, "Enhancing Privacy Preservation in Vehicular Trust Management Systems through Blockchain Technology," *Electronics*, vol. 12, no. 24, Art. no. 24, Jan. 2023, doi: 10.3390/electronics12244949.

[10] M. Balfaqih, Z. Balfagih, M. D. Lytras, K. M. Alfawaz, A. A. Alshdadi, and E. Alsolami, "A Blockchain-Enabled IoT Logistics System for Efficient Tracking and Management of High-Price Shipments: A Resilient, Scalable and Sustainable Approach to Smart Cities," *Sustainability*, vol. 15, no. 18, Art. no. 18, Jan. 2023, doi: 10.3390/su151813971.

[11] P. A. D. S. N. Wijesekara and S. Gunawardena, "A Review of Blockchain Technology in Knowledge-Defined Networking, Its Application, Benefits, and Challenges," *Network*, vol. 3, no. 3, Art. no. 3, Sep. 2023, doi: 10.3390/network3030017.

[12] A. M. Fadhil, "Next-Generation Urban Intelligence: Integrating 6G Communication and Blockchain Technology for Smart City Advancements," *Int. J. Comput. Sci. Mob. Comput.*, vol. 12, no. 11, pp. 29–35, Nov. 2023, doi: 10.47760/ijcsmc.2023.v12i11.003.

[13] Z. Zhou, O. Onireti, H. Xu, L. Zhang, and M. Imran, "AI and Blockchain Enabled Future Wireless Networks: A Survey And Outlook," *Distrib Ledger Technol.*, vol. 3, no. 3, p. 22:1-22:30, Sep. 2024, doi: 10.1145/3644369.

[14] A. Biswas and H.-C. Wang, "Autonomous Vehicles Enabled by the Integration of IoT, Edge Intelligence, 5G, and Blockchain," *Sensors*, vol. 23, no. 4, Art. no. 4, Jan. 2023, doi: 10.3390/s23041963.

[15] Y. Bobde, G. Narayanan, M. Jati, R. S. P. Raj, I. Cvitić, and D. Peraković, "Enhancing Industrial IoT Network Security through Blockchain Integration," *Electronics*, vol. 13, no. 4, Art. no. 4, Jan. 2024, doi: 10.3390/electronics13040687.

[16] T. Nguyen, H. Nguyen, and T. Nguyen Gia, "Exploring the integration of edge computing and blockchain IoT: Principles, architectures, security, and applications," *J. Netw. Comput. Appl.*, vol. 226, p. 103884, Jun. 2024, doi: 10.1016/j.jnca.2024.103884.

[17] Y. Bobde, G. Narayanan, M. Jati, R. Raj, I. Cvitić, and D. Peraković, "Enhancing Industrial IoT Network Security through Blockchain Integration," *Electronics*, vol. 13, no. 4, p. 687, Feb. 2024, doi: 10.3390/electronics13040687.

[18] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors*, vol. 24, no. 10, Art. no. 10, Jan. 2024, doi: 10.3390/s24103111.

[19] R. Shinde, S. Patil, K. Kotecha, V. Potdar, G. Selvachandran, and A. Abraham, "Securing AI-based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions," *Trans. Emerg. Telecommun. Technol.*, vol. 35, no. 1, p. e4884, 2024, doi: 10.1002/ett.4884.

[20] Q. Lin, X. Li, K. Cai, M. Prakash, and D. Paulraj, "Secure Internet of Medical Things (IoMT) based on ECMQV-MAC authentication protocol and EKMC-SCP blockchain networking," *Inf. Sci.*, vol. 654, p. 119783, Jan. 2024, doi: 10.1016/j.ins.2023.119783.

[21] K. Banti, M. Louta, and P. Baziana, "Data Quality in Human-Centric Sensing-Based Next-Generation IoT Systems: A Comprehensive Survey of Models, Issues, and Challenges," *IEEE Open J. Commun. Soc.*, vol. 4, pp. 2286–2317, 2023, doi: 10.1109/OJCOMS.2023.3316118.

[22] J. P. Queralta, F. Keramat, S. Salimi, L. Fu, X. Yu, and T. Westerlund, "Blockchain and Emerging Distributed Ledger Technologies for Decentralized Multi-Robot Systems," *Curr. Robot. Rep.*, vol. 4, no. 3, pp. 43–54, Sep. 2023, doi: 10.1007/s43154-023-00101-3.

[23] R. Pakrooh, A. Jabbari, and C. Fung, "Deep Learning-Assisted Security and Privacy Provisioning in the Internet of Medical Things Systems: A Survey on Recent Advances," *IEEE Access*, vol. 12, pp. 40610–40621, 2024, doi: 10.1109/ACCESS.2024.3377561.

[24] C. Yapa, C. de Alwis, and M. Liyanage, "Can Blockchain Strengthen the Energy Internet?," *Network*, vol. 1, no. 2, Art. no. 2, Sep. 2021, doi: 10.3390/network1020007.

[25] P. Majumdar and S. Mitra, "Blockchain technology for society 4.0: a comprehensive review of key applications, requirement analysis, research trends, challenges and future avenues," *Clust. Comput.*, vol. 27, no. 6, pp. 7059–7081, Sep. 2024, doi: 10.1007/s10586-024-04337-2.

[26] A. Rancea, I. Anghel, and T. Cioara, "Edge Computing in Healthcare: Innovations, Opportunities, and Challenges," *Future Internet*, vol. 16, no. 9, Art. no. 9, Sep. 2024, doi: 10.3390/fi16090329.

[27] P. B et al., "Toward Blockchain for Edge-of-Things: A New Paradigm, Opportunities, and Future Directions," *IEEE Internet Things Mag.*, vol. 4, no. 2, pp. 102–108, Jun. 2021, doi: 10.1109/IOTM.0001.2000191.

[28] S. K. Pattnaik et al., "Future Wireless Communication Technology towards 6G IoT: An Application-Based Analysis of IoT in Real-Time Location Monitoring of Employees Inside Underground Mines by Using BLE," *Sensors*, vol. 22, no. 9, Art. no. 9, Jan. 2022, doi: 10.3390/s22093438.

[29] S. Selvarajan and H. Mouratidis, "A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems," *Sci. Rep.*, vol. 13, no. 1, p. 7107, May 2023, doi: 10.1038/s41598-023-34354-x.

[30] R. Aluvalu, S. K. V. N, M. Thirumalaisamy, S. Basheer, E. A. Aldhahri, and S. Selvarajan, "Efficient data transmission on wireless communication through a privacy-enhanced blockchain process," *PeerJ Comput. Sci.*, vol. 9, p. e1308, Apr. 2023, doi: 10.7717/peerj-cs.1308.

[31] A. M. Hussein, S. A. Alomari, M. H. Almomani, and others, "A Smart IoT-Cloud Framework with Adaptive Deep Learning for Real-Time Epileptic Seizure Detection," *Circuits Syst Signal Process*, vol. 44, pp. 2113–2144, 2025, doi: 10.1007/s00034-024-02919-4.

[32] T. Benhmad, C. B. Rhaimi, S. Alomari, and L. Aljuhani, “Design and Implementation of an Integrated IoT and Artificial Intelligence System for Smart Irrigation Management,” *Int. J. Advance Soft Compu. Appl.*, vol. 16, no. 1, Mar. 2024, doi: 10.15849/IJASCA.240330.12.

[33] “6G Network Slice Security Attack Detection.” Accessed: Apr. 15, 2025. [Online]. Available: https://www.kaggle.com/datasets/ziya07/6g-network-slice-security-attack-detection.

[34] Government Arts and Science College, Chennai, India et al., “Securing Wireless Communication Using Novel Transfer Learning For Encryption In Wireless Networks,” *ICTACT J. Commun. Technol.*, vol. 14, no. 3, pp. 3005–3012, Sep. 2023, doi: 10.21917/ijct.2023.0447.

[35] A. Churcher et al., “An Experimental Analysis of Attack Classification Using Machine Learning in IoT Networks,” *Sensors*, vol. 21, no. 2, Art. no. 2, Jan. 2021, doi: 10.3390/s21020446.