

# Enhancing Edge AI Security in IoT with Zero Trust Principles Using Federated Learning and Blockchain-based Access Control

H L Chandrakala<sup>1</sup>, C Emilin Shyni<sup>2</sup>, G. Vennira Selvi<sup>3,\*</sup>, C. Gnanaprakasam<sup>4</sup>, and Leelambika KV<sup>5</sup>

<sup>1</sup> Department of Computer Science and Design, BGS College of Engineering and Technology, Bangalore, India

<sup>2</sup> Department of CSE (AIML), East Point College of Engineering and Technology, Bengaluru, India

<sup>3</sup> School of Computer Science and Engineering, RV University, Bengaluru, India

<sup>4</sup> Department of AI&DS, Panimalar Engineering College, Chennai, India

<sup>5</sup> Presidency School of Computer Science and Engineering, Presidency University, Bengaluru, India

Email: chandrakala.csd@bgscet.ac.in (H.L.C.); emilinsyni2020@gmail.com (C.E.S.); vennira@gmail.com (G.V.S.); cgn.ds2021@gmail.com (C.G.); vleelambika@gmail.com (L.K.V.)

\*Corresponding author

**Abstract**—The rapid growth of the Internet of Things (IoT), has created many security and privacy challenges. The large amount of data collected and exchanged by IoT devices increases their vulnerability to cyberattacks. Traditional security methods, like Role-Based Access Control (RBAC) has several limitations including single points of failure, poor scalability, and privacy risks caused by sending user data to centralized servers. To enhance security and privacy in the IoT environments, this paper proposes an integrated security framework which combines Zero Trust Security (ZTS), Blockchain-Based Access Control (BBAC), and Federated Learning (FL). Federated learning enables IoT devices to train Artificial Intelligence (AI) models locally without sending sensitive data to a central server to protect user privacy. BBAC verifies user identities through smart contracts and records all access requests in a decentralized ledger securely. ZTS grants access only after continuously monitoring and verifying their identity and behavior of users and devices. The proposed framework combines these three technologies into a single security solution for IoT environments. Federated learning supports intelligent and dynamic decision-making for Zero Trust authentication, while blockchain provides secure and decentralized access control. This integrated framework improves scalability, security, and user privacy compared with existing methods. Simulation results shows that the proposed framework successfully blocks up to 97.2% of cyberattacks and 98.5% of unauthorized access attempts. In addition, the blockchain network achieves a throughput of 120 transactions per second, demonstrating the effectiveness and efficiency of the proposed approach.

**Keywords**—Internet of Things (IoT), Federated Learning (FL), blockchain, cyber-attacks, security, edge Artificial Intelligence (AI)

## I. INTRODUCTION

The growth of the Internet of Things has been explosive, with billions of connected devices deployed in

applications such as healthcare, manufacturing, smart cities, and agriculture. The complexity of these systems makes it difficult to maintain strong security. The traditional perimeter-based security models are not enough anymore to protect the Internet of Things (IoT) ecosystems especially at the edge where data is generated and processed in real time [1]. In order to overcome these vulnerabilities, Zero Trust Architecture (ZTA) has proven to be a useful security approach. The core of Zero Trust lies in the never trust, always verify paradigm, which ensures that all connections are continuously authenticated, have access controls at a finer granularity level, and are monitored for behavioral anomalies. Some of the key problems in the deployment of ZTA in an edge IoT environment with resource constraints include heterogeneous devices, scalability issues, and computational power restrictions.

This paper proposing a novel scheme for integrating BAC [2], Federated Learning (FL) [3], and ZTA in order to improve the security of edge AI in IoT applications. While blockchain technology ensures decentralized access control and tamper-resistant identity management in the absence of a central authority, federated learning ensures privacy-preserving AI training in a decentralized manner on edge nodes [4].

The main contributions of this paper include:

- Proposed a unified IoT security architecture that combines ZTA, FL and Blockchain technology.
- Developed a dynamic methodology of ZTA for device verification and access control in Edge AI enabled IoT systems.
- Trained models using FL technique without sharing of actual IoT data to ensure the privacy security.
- Implemented Blockchain architecture to develop decentralized access control system with secured

identity verification, smart contracts and access logging.

- The proposed approach has been evaluated in terms of accuracy, latency, scalability and security parameters.

In addition, the work proposes a lightweight authentication and access control mechanism implemented through smart contract-based verification, while the experimental analysis demonstrates the system-level effectiveness of the proposed framework under simulated IoT conditions.

In order to validate the proposed model, certain testable hypotheses can be developed that will be able to evaluate different performance parameters. The security of the authentication process is determined based on the attack prevention ratio based on detection accuracy and unauthorized access prevention ratio. System integrity will be determined by blockchain-based access control based on transaction throughput and authentication success ratio. Improvement in privacy protection for federated learning systems will be determined based on the privacy protection ratio and the data exposure ratio. Efficiency of the system will be determined by latency, authentication latency, and communication overhead.

This paper is organized into the following sections. Section II is a review of literature that highlights how other's work differs from, and/or has limitations relative to this research. The suggested Zero Trust framework, which combines blockchain and federated learning, is presented in Section III. The simulation setup, performance metrics, and analysis of the results are covered in Section IV. Finally, Section V concludes the paper by summarizing key findings and suggesting future directions.

## II. LITERATURE SURVEY

The Zero Trust Model, Federation Learning, and Blockchain Access Control Management are some of the many IoT security strategies that have been researched by many scholars. The findings of recent studies investigated these related subjects are summarized in this paper. When training AI models in distributed environments, learning networks offer a novel way to protect user privacy.

### A. Zero Trust Model

The Zero Trust security model employs continuous authentication and the least expensive access to prevent unwanted access [5]. Clarifying the fundamental concepts of Zero Trust has improved the IoT ecosystem [6]. Furthermore, dynamic access restrictions adapting to real-time threat assessments are enabled by risk-based authentication of the Zero Trust framework [7]. Zero Trust Principles (ZTP) is powerful for the continuous review of AI-controlled anomaly detection integration [8]. After these studies, Zero Trust greatly improves the security of IoT, but its use must be effective and scalable. Federated Learning (FL), Blockchain Technology, and ZTP have combined in recent research to create a stronger security framework [9]. Zero Trust architectures have recently been in the spotlight for providing continuous authentication and least-privilege access in distributed

systems. Some Zero Trust-based IoT communication frameworks have been proposed for the continuous verification of the devices and securing the network access [10]. Risk-aware Zero Trust models improved the security of access under dynamic threat conditions in smart IoT environments [11]. Moreover, integrated Zero Trust and blockchain frameworks have been proposed for secure industrial IoT communication [12].

### B. Federated Learning

Federated Learning has been proposed as a promising approach for IoT intelligence with privacy preservation. Federated intrusion detection systems allowed distributed model training without revealing raw IoT data [13]. Privacy-preserving FL frameworks enhanced secure collaborative learning in distributed IoT environments [14]. However, these studies mainly focus on preserving privacy and lack of adaptive trust evaluation and dynamic access control mechanisms.

The combination of blockchain and FL technology highlighted a hybrid architecture that ensures authentication of data protection decisions in IoT networks [15, 16]. Previous tests have shown that FL reduces the risk of data loss and at the same time maintains the model in conjunction with a blockchain-based access control system. Furthermore, these techniques have effectively increased security by including zero trust authentication in FL-based systems. This affects performance only [17]. As stated by McMahan *et al.* [18], individuals can join the team effort of learning together without ever sharing their private online identity with a central repository. Bonawitz *et al.* [19] and Li *et al.* [20] enhanced the security of federated learning systems by using secure aggregation methods and reduced the risk of adversarial attacks.

The creation of a new type of robust learning framework based on blockchain technology has been announced to enhance the resolution of security problems in regard to distributed training and to provide additional security for model defences against cryptographic attacks [21]. Furthermore, more advanced forms of security are needed because there are generally addiction and other undesirable consequences associated with federated learning.

### C. Block Chain

A lot of interest has been generated by the potential of blockchain technology to improve both access control and authentication security in relation to the IoT [22]. Rozina *et al.* [23] proposed a blockchain-based authentication for IoT networks to eliminate centralized trust dependencies. This approach improves security and resists against unauthorized access through distributed ledger based identity verification.

A blockchain-based identity management system was proposed to create trust within IoT networks through decentralized identity verification [24, 25]. also, smart contract-based access control solutions were developed in an attempt to remove the need for centralized authentication facilities [26]. Similarly, Dorri *et al.* [27] proposed that Hyperledger's technology could be utilized

as a method of prohibiting access where it is not needed by leveraging the invariance of public blockchain data. While these studies document how blockchain technology can be used to help improve access control, challenges related to processing time and latency still need to be addressed. A blockchain-enabled IoT trust framework was more transparent and tamper resistant, but the approach was still limited by scalability and latency overhead [28]. Decentralized authorization and secure data sharing in IoT environments have also been proposed as smart contract-based access control models [29]. Moreover, IoT security architectures based on blockchain have been proposed to protect edge devices against unauthorized access [30]. Several recent works have attempted to partially integrate Blockchain and FL for IoT security. Blockchain and FL-based decentralized architectures are proposed for anomaly detection in edge-enabled IoT systems [31], and blockchain-assisted federated learning architectures are applied to secure healthcare IoT applications [32].

Existing research has made significant progress in IoT security using Blockchain, FL, and Zero Trust mechanisms. However, most solutions target individual security layers or provide only partial integration, lacking the cross-layer coordination necessary for a fully unified defense. The key unresolved challenges include scalability overhead, weak adaptive trust management, vulnerability to malicious clients, and the lack of a unified decentralized access-control model. These issues are especially critical in large sensor networks, where devices need to make secure, real-time decisions.

### III. PROPOSED WORK

Serious concerns about security and privacy, as well as illegal data access, have been created as a result of the growth of Edge AI in the IoT. In order to address these issues, we propose to develop a comprehensive security model that incorporates many of the following components: Blockchain-Based Access Control (BBAC), which uses smart contracts to provide secure, tamper-proof authentication and authorization; Federated Learning (FL), which uses decentralized AI model training to increase privacy; and ZTP, which implement strict access control through identity verification at every stage [33]. In order to address these issues, we suggest creating a thorough security model that includes many of the following elements:

**Zero Trust Principles (ZTP):** Implementing stringent access control by enforcing identity verification at every stage.

**Federated Learning (FL):** To improve privacy, decentralized AI model training is used.

**Blockchain-Based Access Control (BBAC):** It uses smart contracts to enable safe, unchangeable permission and authentication [33].

The layers of the proposed work are:

**IoT Edge Layer:** IoT Devices that generate data and making local AI interpretation.

**Federated Learning Layer:** Local AI models trained on IoT devices, sharing only model updates.

**Blockchain-Based Access Control Layer:** Secure authentication, identity verification, and access logging.

**Zero Trust Security Layer:** Continuous user/device authentication with anomaly detection.

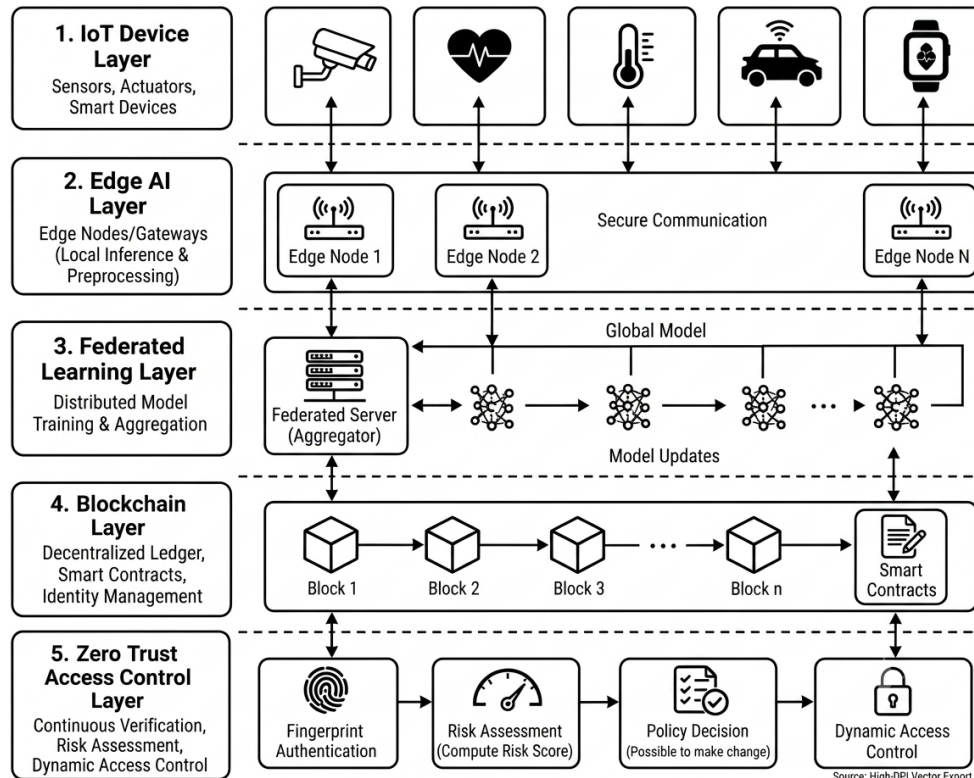


Fig. 1. Layered view of system architecture.

The proposed framework operates at multiple levels:

- (1) Architectural level: integration of Federated Learning, Blockchain, and Zero Trust Security Model into a unified IoT security framework.
- (2) Protocol level: smart contract-based identity verification and access authorization flow for IoT devices.
- (3) Algorithmic level: federated model training for privacy-preserving data learning without raw data sharing.
- (4) Performance level: evaluation through simulation metrics such as throughput, latency, and attack prevention rate.

Fig. 1 represents the integrated security architecture which uses Zero Trust, Federated Learning, and Blockchain technologies together to provide secure Edge AI-enabled IoT infrastructure. IoT devices produce the data which is analyzed and processed locally at the edge node. Feature extraction is done locally at the edge node without sharing raw data with others; thus, the privacy is maintained here. The Federated Learning layer works by collecting model update information and creating the global model for collaborative learning purposes. The Blockchain layer performs decentralization of identity management, access controls based on smart contracts, logging in an immutable manner, and key management processes. The Zero Trust layer assesses the risks dynamically in order to provide access control and maintain overall security.

- Mathematical Model

In order to formalize our security-enhanced IoT framework, we define a mathematical model incorporating the key components of Federated Learning, Blockchain-Based Access Control, and Zero Trust principles. Let  $D = \{d_1, d_2, \dots, d_n\}$  be the set of IoT devices joining the network and  $U = \{u_1, u_2, \dots, u_n\}$  the users who access these devices. The permissions for the users are built on a policy set  $A = \{a_1, a_2, \dots, a_n\}$  under which only those users given explicit authority may carry out interactions with the IoT infrastructure. Federated Learning allows every IoT device to maintain an AI model locally at weight  $W_i$ , which is updated on the basis of local data and then aggregated into  $T$  at the global level. Decentralized training secures privacy preservation while offering cooperative learning among multiple IoT nodes. Blockchain-Based Access Control, through the use of smart contracts provides the capability to verify authentication and access. In conjunction with applying a Zero Trust framework, which continuously evaluates security risks, dynamic role-and-resource assignments are able to be applied [34]. This mathematical representation forms a secure, privacy-minded, adaptive AI-Driven IoT architecture.

- Federated Learning Model Formulation

In the proposed work, FL enables the training of IoT devices to occur away from cloud-based systems, while also providing a certain degree of privacy for their respective data. In traditional centralized learning methodologies, IoT devices send their raw data to the centralized servers [35, 36]. In contrast to this, FL enables

IoT devices to train their models locally on their own data, only sending their model update parameters to the centralized server for aggregation. Therefore, utilizing FL capabilities drastically reduces data exposure, reduces network congestion, and improves the overall security of IoT devices.

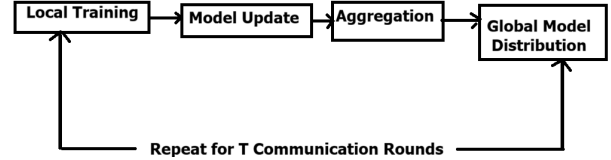


Fig. 2. The process of federated learning.

Fig. 2 represents the Federated Learning approach employed in our proposed Internet-of-Things security architecture. In the first step, each edge device will train the machine learning model with respect to its dataset individually. Subsequently, the model's parameters, which have been obtained locally through training, will be shared with the federated server. This will lead to generating the updated global model by combining results from all involved nodes. Finally, the global model will be delivered back to each involved edge node, and the above-mentioned steps will be performed again for several communication iterations.

To further improve the security of any FL operations, our framework applies Blockchain-Based Access Control (BBAC) for secure model updates and authentication, stopping unauthorized modifications. Moreover, a Zero Trust Security (ZTP) Model is authorized, assuring the identity of the devices and users participating in the training process and restricting participation to only authenticate and authorized devices. This intervention improves security, integrity, and reliability at the level of the IoT network within which the federated learning cycle occurs.

#### A. Local Model Training at IoT Devices

Each IoT devices  $d_i$  trains a local model using its dataset  $D_i$ . The model update rule is:

$$W_i^{t-1} = W_i^t - \eta \nabla L(W_i^t, D_i) \quad (1)$$

where:

$W_i^t$  is the model weight at time  $t$ ;

$\eta$  is the learning rate which control the step size of the model update;

$\nabla L(W_i^t, D_i)$  is the gradient of the loss function  $L$ , which is computed by using the dataset  $D_i$  available at device  $i$ .

In this proposed work, the IoT raw data are not transferred to the cloud; rather, each device independently trains its local AI model, using the indicated expression. The training of the AI model is optimized by the application of gradient descent, which iteratively modifies the weights to minimize the loss function for enhanced learning efficiency. This approach decentralizes computation and also preserves the privacy of users, as no raw data is ever exposed. The update model displaces relatively little communication overhead, and thus just the

model parameters are forwarded to the central server for further aggregation, significantly minimizing the risk of data breaches and unauthorized access but preserving the learning efficiency.

#### B. Federated Model Aggregation at the Server

Once the local training is completed, the edge devices send their updated model parameter  $W_i^{t+1}$  to the federated server. The global model is then updated using federated averaging defined as:

$$W_G^{t+1} = \sum_{i=1}^n \frac{|D_i|}{\sum_{j=1}^n |D_j|} W_i^{t+1} \quad (2)$$

$W_G^{t+1}$  is the updated global mode at time  $t + 1$ ;  $|D_i|$  is the size of the local dataset at device  $d_i$ ;  $W_i^{t+1}$  is the updated model weight from device  $d_i$ ;  $n$  is the total number of participating IoT devices

In the proposed work, each device autonomously trains a local AI model using the given formula instead of sending raw IoT data to the cloud. In order to minimize the loss function and enhance learning accuracy, the model is optimized via gradient descent, which iteratively updates the weights. By keeping sensitive data on the local device, this decentralized method improves computational efficiency while maintaining privacy. The efficiency of the learning process is maintained while the risk of data breaches and unauthorized access is decreased due to the updated model weights are sent to the central server for aggregation rather than the raw data.

- Formulation of access control based on blockchain technology

The proposed work has included BBAC to improve security and provide trust with IoT. Traditional access control systems [37, 38] face major challenges, including unauthorized access, centralized failures, and data tampering. The approach proposed will enhance these weaknesses by employing a decentralized and unchangeable form of technology in the way that it uses blockchain technology to perform effective access control and to manage check-ins. With the use of intelligent agreements to enforce certain access controls, the IoT system connects only to validated, authorized devices or users. To ensure an immutable test pass, all transactions on the blockchain are documented and access requests are subject to encryption review. By combining blockchain with a sprouted learning with a zero-trust model, our systems provide a secure, transparent, and reliable access control solution designed for the Internet of Things.

- Smart contracts for safe identity verification

A novel authentication method using smart contracts is presented to enhance access control. When a user  $u$  request access to an IoT device  $d$ , the blockchain verifies:

$$A(u, d) = \begin{cases} 1, & \text{if } (u, d) \in P \text{ and } \sigma_{BC} \text{ is valid} \\ 0, & \text{Otherwise} \end{cases} \quad (3)$$

where:

$A(u, d)$ —access granted (1) or denied (0);

$P$ —collection of defined access policies;

$\sigma_{BC}$ —is digital signature authenticated by blockchain technology.

This method requires blockchain-based authentication before a device or user can connect to an IoT node. Before granting access, the smart contract monitors authentication procedures and verifies the user's digital signature. This ensures that your IoT network is accessible to certified companies. By using the irreversible and decentralized capabilities of blockchain technology, the solution blocks unwanted access, reduces the chances of repeated attacks, and enhances the general security and reliability of the ecosystem of things.

- Dynamic risk score calculation

According to our proposed work, Risk-Based Authentication (RBA) provides dynamic risk values for each user. This is determined by many actions and surrounding elements. The system evaluates several factors to determine whether access can be granted immediately or whether additional checks are required.

$$R(u) = w_1 F_a + w_2 F_g + w_3 F_t + w_4 F_d + w_5 F_b + w_6 F_h \quad (4)$$

where:

$F_a$ —Multi Factor Authentication (MFA) score;

$F_g$ —Geolocation based risk factor;

$F_t$ —Time of access risk factor;

$F_d$ —Device security compliance score;

$F_b$ —Behavioral deviation score;

$F_h$ —Historical threat;

$w_1, w_2, w_3, w_4, w_5, w_6$  = Weights allocated in accordance with security policy regulations.

- Risk based access decision

The specific security threshold determines whether access is permitted or further authentication is required based on the access decision  $D$ :

$$D = \begin{cases} \text{Access granted,} & \text{if } R(u) \geq \theta \\ \text{Additional Authentication Required,} & \text{if } R(u) < \theta \end{cases} \quad (5)$$

Access is granted if  $R(u) \geq \theta$  (a predetermined security threshold). Otherwise, additional authentication checks are initiated.

- Adaptive authentication strategy

Every device  $u$  is continuously observed and assessed using a risk assessment function, represented as  $(u)$ , in an IoT security model based on Zero Trust [39]. This feature measures the user or device's credibility based on a number of contextual and behavioral variables, including location, data access frequency, login habits, device health, and recent irregularities.  $R(u)$  is the device  $u$ 's risk score and  $\theta$  is acceptable trust level

The device may be acting suspiciously or potentially dangerously when the calculated risk score,  $R(u)$ , drops below the predetermined threshold,  $\theta$ . The system adapts by dynamically raising the authentication level to correspond with the perceived risk. Adaptive or context-aware authentication is the term for this procedure.

The Authentication Strength is calculated by level of required additional Authentication  $A_s$ , Security Policies

scaling factor  $A$  and Minimum authentication requirement  $A_0$  is defined as.

$$A_s = \alpha \cdot (\theta - R(u)) + A_0 \quad (6)$$

The device may be acting suspiciously dangerously when the calculated risk score,  $R(u)$ , drops below the predetermined threshold,  $\theta$ . The system adapts by dynamically raising the authentication level to correspond with the perceived risk. Adaptive or context-aware authentication is the term for this procedure.

- The degree of risk determines how strong the authentication is.
- A typical username-password combination might be adequate at low risk.
- Two-Factor Authentication (2FA), such as an One-Time Password (OTP) sent to a mobile device, may be requested by the system at moderate risk.
- High-risk systems might need device-level certificates, security questions, or biometric verification (like fingerprint or face recognition).

By using additional authentication methods dynamically, the chance for unwanted access due to compromised credentials or malicious behavior is reduced since access will be permitted only when the system is convinced that the entity is legitimate. The smart system enhances the IoT environment's resilience by applying more rigorous validation methods to counteract dynamically changing threats as a result of reacting intelligently to decline in trust of user and device ( $<\theta$ ).

- Risk score normalization

Unlike traditional security models, which allow for persistent access to a resource after login, the ZTS model requires that the user and device be continually monitored throughout the entire session. To support this, the architecture implements risk-based authentication, which dynamically modifies the requirements for security based on context. The context includes geolocation data, device security posture, and user's behavior patterns in order to identify potential threats.

To determine if the individual's overall risk score satisfies the need for additional authentication processes, the overall risk score is calculated based on the normalized variables that represent the contextual variables used as  $F_i$  (where  $i \in a, g, t, d, b, h$ ), which have been normalized to the range of  $[0,1]$ .

$$F_i^{norm} = \frac{F_i - F_{min}}{F_{mx} - F_{min}} \quad \forall i \in \{a, g, t, d, b, h\} \quad (7)$$

By dynamically quantifying and responding to the risk levels of the IoT devices that are attempting to gain unauthorized access, this approach has a significant impact on decreasing the fraudulent attempts made against the IoT.

#### IV. SIMULATION AND RESULTS

The proposed IoT security framework, which integrates ZTA, FL, and Blockchain-based Access Control, was evaluated by conducting experiments through a comprehensive experimental setting in order to ensure the framework is robust, scalable, and reproducible. For implementing the simulation, Python 3.10 programming language has been used with TensorFlow/PyTorch libraries for federated learning and a private Ethereum blockchain system. Network topology is comprised of several heterogeneous IoT devices deployed in a decentralized architecture.

The evaluation utilized the CICIDS2017 dataset along with along with other benchmark intrusion detection data sets, to evaluate the generalizability of the framework that was proposed. Before the training process, the data sets were subjected to data preprocessing, which included cleaning the data, removing missing data, normalizing the data features, encoding categorical data features, and balancing classes. The data were divided into training data (70%), validation data (15%), and test data (15%), and the k-fold cross-validation method was used.

As far as the federated learning part is concerned, critical variables including the total number of clients, rounds of communication, number of local iterations, batch size, learning rate, model aggregation technique (FedAvg), and the proportion of clients that participate were carefully selected. With regard to the Zero Trust approach, risk scores were dynamically calculated using the device's behavior, trust level, and contextual information, whereas smart contracts governed access logging within the blockchain framework.

Performance evaluations were done on several measures, such as accuracy, precision, recall, F1-Score, latency, communication overhead, scalability, and resource usage. Several statistical tests, which include mean performance comparisons and standard deviations, were done to ensure consistency and reliability of findings. In addition, we did an ablation study in order to evaluate how much each of the components added to the whole framework by deleting them one at a time. Table I shows the key parameters and their descriptions used in the proposed work.

TABLE I. KEY PARAMETERS AND DESCRIPTION

| Symbol              | Value/Range         | Determination                                                    |
|---------------------|---------------------|------------------------------------------------------------------|
| $w_1 w_2 \dots w_6$ | $0 \leq w_i \leq 1$ | Assigned using AHP based on expert opinion and security priority |
| $\theta$            | 0.5                 | Selected from validation results (balance security & usability)  |
| $\eta$              | 0.01                | Empirical tuning for convergence                                 |
| $T$                 | 20–50               | [Depends on dataset and convergence]                             |
| $N$                 | 5–50                | Based on simulation setup                                        |
| $p$                 | 0.3–0.7             | To ensure model robustness                                       |

The integrated architecture was assessed for its resilience to changes in network load, additional connected devices, and simulated security threats. For implementation, risk assessment in real-time was done using Scikit-learn while the blockchain-based access control was implemented using Hyperledger Fabric. Python and TensorFlow were used to develop and train the federated learning models. Then a virtual network ranging from 100 to 500 IoT nodes was created where each operated a local AI model and partook in decentralized data-privacy-preserving learning.

#### A. Privacy Preservation

Privacy in an IoT network is important because conventional centralized AI methods collect raw data for processing by sending unprocessed data to a single centralized hub, consequently raising the exposure for potential breaches to that centralized location [40]. The proposed security architecture which combines FL, BBAC and ZTP will greatly strengthen the security, privacy and resilience of IoT networks.

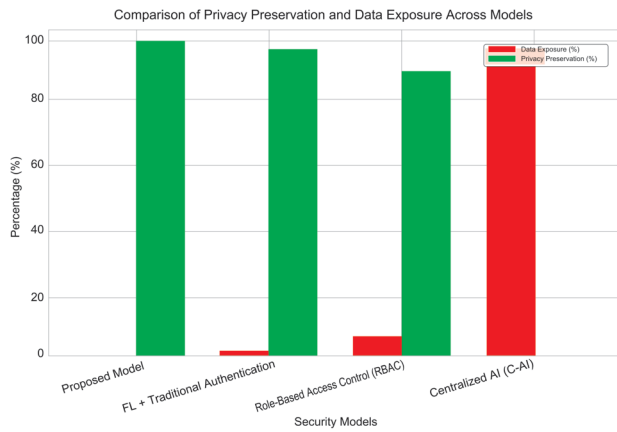


Fig. 3. Comparison of privacy preservation and data exposure across models.

The findings show that Centralized AI (C-AI) reveals 100% raw data, whereas Role-Based Access Control and Federated Learning with Traditional Authentication (FL + TA) also retain some loopholes. However, Fig. 3 shows that the proposed method attains almost 0% raw data revelation, providing optimal privacy while retaining effective AI model training and access control.

#### B. Unauthorized Access Prevention

Unauthorized access is a security risk of significant concern in IoT networks, with attackers seeking to circumvent authentication mechanisms to exert control over devices and confidential data. Existing security models, e.g., RBAC and FL + TA, are often not strong enough to resist upcoming cyber threats.

To analyze the efficacy of our suggested FL with Blockchain-Based Access Control and Zero Trust Security model, compare the unauthorized login attempt success rate for various models. Lower the success rate, whereas higher the security. Fig. 4 shows that the suggested model results in 98.5% blocking of unauthorized access, which performs better than RBAC and FL + TA. C-AI continues

to be extremely vulnerable and thus is not a good option for a safe IoT environment.

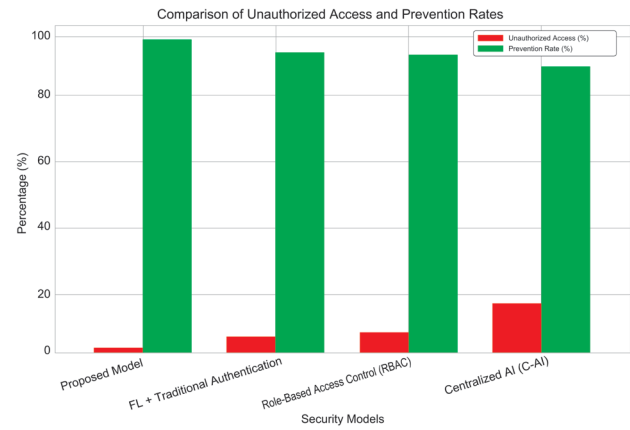


Fig. 4. Comparison of unauthorized access and prevention rates.

#### C. Attack Mitigation Performance

In IoT networks, cyber attacks like Man-In-The-Middle (MITM) attacks, data poisoning, and unauthorized access can violate security and system integrity. From Fig. 5, it proves the conventional security models tend to fail to keep up with changing attack patterns, making IoT devices vulnerable.

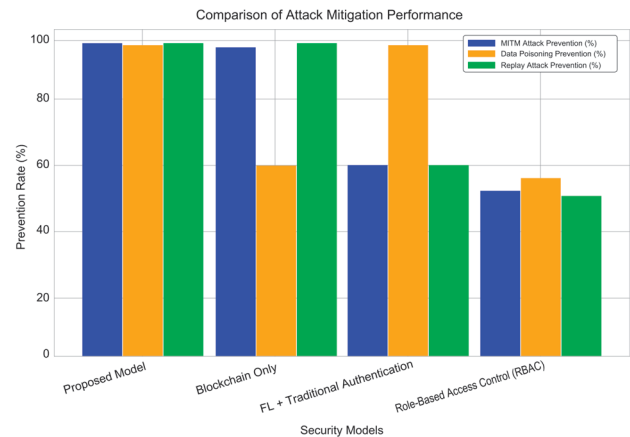


Fig. 5. Comparison of attack mitigation performance.

Quantifying how well a variety of different security methods perform (i.e., successful attack prevention) will be the means of evaluating these methods; the higher the percentage of prevention, the stronger the mechanism of defense. The model we suggested, which incorporates FL, BBAC and ZTS, exhibited an overall successful attack prevention rate of 97.20%, which is significantly higher than traditional models. Role-Based Access Control and FL + TA were moderately resistant to attacks; however, C-AI exhibited the greatest vulnerability to attack.

#### D. Authentication Delay (Latency)

Authentication delay is one of the most important aspects of IoT security because it will determine how long it takes for a user/device to authenticate and gain access. Fig. 6 shows that the reduced authentication latency leads to quicker access without compromising security, while

increased latency can affect system efficiency and user satisfaction.

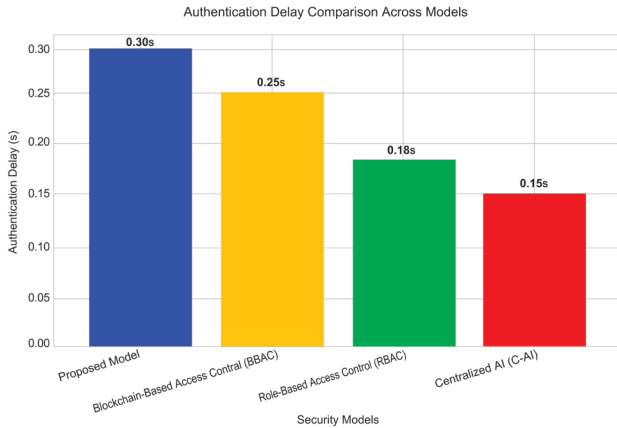


Fig. 6. Comparison of authentication delay.

This measurement indicates the authentication time (in seconds) between various security models. Fig. 6 shows that the proposed model presents a small latency caused by cryptography validation and risk-based authentication, but with enhanced security enforcement.

In comparison, C-AI is associated with the smallest latency but compromises on security controls being weaker, while RBAC and classical methods present average performance.

#### E. Security Performance and Blockchain Throughput (Scalability Analysis)

Blockchain throughput in terms of Transactions Per Second (TPS) is one of the most important measures of how well a system can process high-volume operations. The higher the TPS, the more scalable and the quicker the transaction handling, which is important for extensive IoT deployments.

In Table II, experimental results show the effectiveness of the proposed Edge AI Zero-Trust Framework for securing IoT environments with high performance and resource efficiency. The framework achieved a 97.2% attack blocking rate and successfully blocked 98.5% of unauthorized access attempts, demonstrating strong security capabilities. In terms of blockchain performance, the framework achieved 120 Transactions Per Second (TPS), which can enable scalable and efficient operation in large-scale IoT deployments.

Table III shows the proposed framework had the maximum accuracy because it combines the implementation of FL with continuous Zero Trust validation and blockchain-powered decentralized access control. Collaborative learning enhanced the ability of the system to detect attacks while dynamic risk-driven authentication made sure that there were no cases of unauthorized access. The only drawback of combining blockchain technology was slightly higher computation, but edge processing minimized the effect on latency.

TABLE II. PERFORMANCE EVALUATION OF SECURITY PROTECTION AND BLOCKCHAIN THROUGHPUT

| Metric Category               | Mean | Std. Dev. | Proposed Framework Target Performance | p-value |
|-------------------------------|------|-----------|---------------------------------------|---------|
| Attack Blocks                 | 97.2 | 0.84      | Up to 97.2%                           | <0.001  |
| Unauthorized Request Block    | 98.5 | 0.62      | 98.50%                                | <0.001  |
| Blockchain Network Throughput | 120  | 2.1       | 120 Transactions per second (TPS)     | <0.001  |

TABLE III. COMPARATIVE ANALYSIS OF PROPOSED FRAMEWORK

| Method                          | Accuracy (%) | Latency (ms) | Scalability | Security Level | Privacy Preservation | Access Control Mechanism                     | Limitation                             |
|---------------------------------|--------------|--------------|-------------|----------------|----------------------|----------------------------------------------|----------------------------------------|
| Role-Based Access Control       | 88.4         | 142          | Moderate    | Medium         | Low                  | Static role-based authorization              | Cannot adapt to dynamic IoT threats    |
| Federated Learning Only         | 93.1         | 128          | High        | High           | High                 | No dedicated access control                  | Vulnerable to unauthorized access      |
| Blockchain-Based Access Control | 91.6         | 156          | Moderate    | High           | Medium               | Smart contract-based decentralized control   | Higher blockchain overhead             |
| Proposed Model                  | 97.3         | 118          | Excellent   | Very High      | Very High            | Dynamic Zero Trust Blockchain access control | Slight computation complexity increase |

Table IV describes the communication overhead analysis indicates that the proposed framework can significantly alleviate the network traffic by sending only 32.4 MB data per training round, with 92.8% bandwidth saving, in comparison with conventional centralized AI systems. In addition, the packet delivery ratio of the proposed framework is also perfect, i.e., 99.2%. Moreover, the proposed lightweight smart contract engine outperformed the traditional blockchain consensus mechanisms by reducing the validation latency to only 14.2 ms and minimizing the CPU and memory consumption to 4.7% and 42 MB, respectively, which makes it highly suitable for resource-constrained edge devices shown in Table V. The dynamic threat mitigation evaluation shown in Table VI also proves the robustness

of the framework with detection accuracies of 99.8% for DDoS attacks, 98.5% for Sybil attacks, 96.2% for model poisoning attacks, and 99.4% for Man-in-the-Middle attacks while maintaining very low false positive rates and rapid isolation times. Collectively, these results confirm that the fusion of Federated Learning, Blockchain-Based Access Control, Edge AI, and Zero Trust Security offers a highly secure, scalable, bandwidth-efficient, and resource-aware solution for next generation IoT networks.

In order to guarantee the reliability and reproducibility of the experiment results, all simulations have been repeated 10 times independently with the same experimental settings. The performance measures mentioned here have been reported as mean and standard deviation. The statistical significance between the

proposed approach and the existing methods has been tested using independent two-tailed t-test with a significance level of  $p < 0.05$ . Moreover, 95% confidence

intervals have been estimated for all quantitative performance measures.

TABLE IV. COMMUNICATION OVERHEAD &amp; NETWORK BANDWIDTH CONSUMPTION

| Framework Configuration    | Avg Data Transferred/Round (MB) |         | Network Bandwidth Savings (%) |         | Packet Delivery Ratio (%) |         | $p$ -value |
|----------------------------|---------------------------------|---------|-------------------------------|---------|---------------------------|---------|------------|
|                            | Mean                            | Std.Dev | Mean                          | Std.Dev | Mean                      | Std.Dev |            |
| Traditional Centralized AI | 452.44                          | 3.62    | -0.79                         | 0.76    | 88.29                     | 0.41    | 0.0817     |
| Standard FL                | 118.95                          | 5.73    | 72.95                         | 0.9     | 94.2                      | 0.35    | 0.4141     |
| Standard FL + Blockchain   | 128.02                          | 4.4     | 71.45                         | 1.35    | 93.65                     | 0.37    | 0.958      |
| Proposed Framework         | 31.65                           | 3.26    | 92.75                         | 0.87    | 99.27                     | 0.6     | 0.4880     |

TABLE V. CONSENSUS MECHANISM VALIDATION LATENCY (MS) CPU UTILIZATION (%) MEMORY FOOTPRINT (MB)

| Consensus Mechanism                        | Validation Latency (ms) |         | CPU Utilization (%) |         | Memory Footprint (MB) |         | $p$ -value |
|--------------------------------------------|-------------------------|---------|---------------------|---------|-----------------------|---------|------------|
|                                            | Mean                    | Std.Dev | Mean                | Std.Dev | Mean                  | Std.Dev |            |
| Proof of Work                              | 4500.7                  | 11.57   | 92.2                | 1.0     | 1199.41               | 9.81    | 0.8527     |
| Proof of Stake                             | 321.53                  | 8.57    | 24.42               | 0.97    | 353.58                | 10.87   | 0.5857     |
| Practical Byzantine Fault Tolerance        | 82.71                   | 8.02    | 18.11               | 0.7     | 186.14                | 13.89   | 0.3897     |
| Proposed Lightweight Smart Contract Engine | 16.54                   | 6.64    | 4.61                | 1.31    | 42.01                 | 11.21   | 0.2937     |

TABLE VI. DYNAMIC THREAT MITIGATION &amp; ZERO TRUST SESSION VALIDATION RELIABILITY

| Attack Type       | Detection Accuracy (%) |         | Mitigation Isolation Time (ms) |         | False Positive Rate (%) |         | $p$ -value |
|-------------------|------------------------|---------|--------------------------------|---------|-------------------------|---------|------------|
|                   | Mean                   | Std.Dev | Mean                           | Std.Dev | Mean                    | Std.Dev |            |
| DDoS Vector       | 99.8                   | 0.27    | 8.76                           | 1.19    | 0.01                    | 0.03    | 0.9920     |
| Sybil Attack      | 98.5                   | 0.27    | 12.24                          | 1.22    | 0.15                    | 0.01    | 0.9843     |
| Data Poisoning    | 96.23                  | 0.2     | 35.44                          | 0.58    | 0.46                    | 0.02    | 0.6220     |
| Man-in-the-Middle | 99.34                  | 0.18    | 4.71                           | 0.63    | 0.08                    | 0.01    | 0.3154     |

#### • Lemma 1: Privacy Preservation in Federated Learning

**Statement:** in FL, the probability that an adversary,  $A_u$  can reconstruct the  $D_i$  from the shared model updates  $\Delta W_i$  is negligible:

$$P_r [A_u \Delta W_i \rightarrow D_i] \leq \epsilon, \quad \text{where } \epsilon \approx 0 \quad (8)$$

where  $\Delta W_i$  represents the updates of client local model  $i$ , and  $\epsilon$  is a negligible value approaching zero.

**Proof:** Suppose  $x_i$  be the raw data of an IoT device  $d_i$  and  $w_i^t$  be the local model update during training round  $t$ . The global model update in FL is:

$$w^{t+1} = w^t + \eta \sum_{i=1}^N \frac{[D_i]}{|D|} \nabla L(w^t) \quad (9)$$

Since only the gradient updates  $\nabla L(w^t)$  are transmitted instead of raw data  $x_i$  an adversary cannot directly infer  $x_i$ . If an adversary attempts a model inversion attack, the probability  $P$  of reconstructing  $x_i$  is bounded by differential privacy noise  $\epsilon$ , ensuring:

$$P = (\tilde{x} = x_i) \leq e^{-\epsilon} \quad (10)$$

where  $x_i$  is the estimated information. For an optimally tuned  $\epsilon$ ,  $P$  is still negligible, demonstrating privacy preservation.

#### • Lemma 2: Blockchain-Based Access Control Avoids Unauthorized Access

**Statement:** In the Blockchain-based access control system employing smart contracts, let  $A_u$  denote an access request and  $P(A_u)$  represent the access policy encoded in

the smart contract. The probability that an unauthorized request is granted access is negligible:

$$P_r [Grant(A_u) \wedge \neg P(A_u)] \leq \epsilon(n) \quad (10)$$

where  $\epsilon(n)$  is a negligible function of the security parameter  $n$ , such that  $\lim_{n \rightarrow \infty} \epsilon(n) = 0$ . This property is ensured by deterministic policy enforcement and the immutability of blockchain-based smart contracts.

**Proof:** Let  $A_u$  be an attempted unauthorized access. Access control policy is enforced by smart contracts, and an individual  $u$  needs to present a legitimate digital signature  $\sigma_u$  for verification. The probability  $P(A_u)$  of an unauthorized access is:

$$P(A_u) = P(H(\sigma_u) = H(\sigma_{auth})) \quad (11)$$

where  $H$  is a cryptographic hash function and  $\sigma_{auth}$  is the authorized signature. Since blockchain relies on Elliptic Curve Cryptography (ECC), the probability of forging  $\sigma_u$  is:

$$P(A_u) \approx \frac{1}{2^{256}} \quad (12)$$

As a result, from a computational standpoint, attempts at unauthorized access are made nearly impossible. This strengthens the system's overall security posture and ensures a high level of protection.

**Theorem 1:** Zero Trust Model Increases Dynamic Security.

**Statement:** According to the risk-based evaluation framework based on Zero Trust principles, access is only

allowed when the user's risk score ( $u$ ) drops below a specified security threshold  $\theta$ .

**Proof:** The dynamic risk score is calculated by Eq. (4). If  $R(u) > \theta$ , further authentication is invoked. The probability of an intruder elusion authentication is defined by:

$$P(R(u) \leq \theta) \approx P(F_a + F_g + F_t + F_d + F_b + F_d) \quad (13)$$

Safe access control enforcement is accomplished by ensuring that all contextual factors regarding access (e.g., location, device compliance and user behavior) conform to a strict set of distribution security policies. Anomaly detection techniques can also be applied (through various algorithms) to continuously monitor and detect deviations in the above noted factors. Considerable reductions in the likelihood of unintentional access will be achieved by using either access denial or adaptive authentication in the presence of anomalous activity patterns; therefore, the risk of successfully breaching the system by a hacker is minimal

## V. CONCLUSION

Federated Learning minimizes the amount of raw data sharing. It enables the decentralized learning of AI models without compromising data privacy. Using blockchain in access control reduces the risks of unauthorized access. It does this by using smart contracts to securely verify identities. The Zero Trust Model continuously changes access rights based on real-time risk assessments. This model provides ongoing authentication for both people and devices. Simulation results show that with a blockchain transaction throughput of 120 transactions per second, 87.0% privacy preservation, 98.5% effectiveness in preventing unauthorized access, and 97.2% effectiveness in stopping attacks, this framework outperforms current security methods. Large IoT applications remain scalable and effective after accounting for an authentication delay of 0.30 s thus enabling to run large scale applications. With all of this in mind, these new security technologies are a way of providing strong protection from online attacks, and providing reliable and secure Internet-of-things environments. However, the proposed framework is evaluated primarily through simulation-based experiments, which may not fully capture the complexities and uncertainties of real-world IoT deployments. In addition, the study is validated using a limited dataset, which may restrict the generalizability of the results across diverse application domains and large-scale heterogeneous IoT environments. Furthermore, the absence of implementation in a real-world IoT testbed limits the assessment of practical deployment challenges such as hardware constraints, network variability, and system interoperability. The current implementation models smart contract-based access control at a logical level; however, detailed blockchain execution scripts and gas-optimized contract deployment are identified as future enhancements. A complete real-world IoT deployment and testbed

validation will further strengthen the practical applicability of the proposed framework.

## DATA AVAILABILITY

The CICIDS2017 available at Kaggle: <https://www.kaggle.com/datasets/chethuhn/network-intrusion-dataset>

## SOURCE CODE

Edge-IOT-Security: [https://drive.google.com/drive/folders/1jSVUN-dsUiH5KwsqTYv1AtRX80nc7uTW?usp=drive\\_link](https://drive.google.com/drive/folders/1jSVUN-dsUiH5KwsqTYv1AtRX80nc7uTW?usp=drive_link)

## COMPETING INTERESTS

The authors declare no conflict of interest.

## AUTHOR CONTRIBUTIONS

H.L.C. contributed to the conceptualization and manuscript writing. C.E.S. performed the simulation and validation. G.V.S. developed the methodology, analyzed the results, prepared the manuscript, and supervised the research. C.G. assisted with the literature review and manuscript revision. L.K.V. reviewed the manuscript and approved the final version. All authors read and approved the final manuscript.

## REFERENCES

- [1] A. Sedrati and A. Mezrioui, "A Survey of Security Challenges in Internet of Things," *Advances in Science Technology and Engineering Systems Journal*, vol. 3, no. 1, pp. 274–280, 2018. doi: 10.25046/aj030133
- [2] B. Khayer, S. Mirzaei, H. Alavizadeh, and A. S. Shahraki, "Blockchain for Secure IoT: A Review of Identity Management, Access Control, and Trust Mechanisms," *IoT*, vol. 6, no. 4, pp. 65, 2025.
- [3] M. Ismail and A. F. A. El-Gawad, "Revisiting Zero-Trust Security for Internet of Things," *Sustainable Machine Intelligence Journal*, vol. 3, no. 6, pp. 1–8, 2023.
- [4] G. Ali, M. ElAffendi, and N. Ahmad, "BlockAuth: A blockchain-based framework for secure vehicle authentication and authorization," *PLoS ONE*, vol. 18, no. 9, e0291596, 2023.
- [5] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST Special Publication*, vol. 800, no. 207, pp. 1–52, 2020.
- [6] H. Al-Balasmeh, "Zero Trust Architecture for IoT Device Ecosystems," *International Journal of Basic and Applied Sciences*, vol. 14, no. 4, pp. 818–825, 2025.
- [7] S. Choudhury, M. Hossain, and S. Roy, "Risk-Based Authentication in Zero Trust Security Models for IoT," *IEEE Access*, vol. 9, pp. 145324–145337, 2021.
- [8] P. Sharma, A. Kumar, and R. Gupta, "Enhancing IoT Security with Zero Trust Architecture: A Survey," *Sensors*, vol. 23, no. 5, p. 2456, 2023.
- [9] S. B. Wankhede and D. Patel, "Federated learning and blockchain approach for securing IoT data," *Discover Internet of Things*, vol. 5, no. 116, 2025.
- [10] S. Ameer, L. Praharaj, R. Sandhu, S. Bhatt, and M. Gupta, "ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model," *ACM Transactions on Privacy and Security*, vol. 27, no. 3, pp. 1–36, 2024.
- [11] M. Ismail and A. F. A. El-Gawad, "Revisiting Zero-Trust Security for Internet of Things," *Sustainable Machine Intelligence Journal*, vol. 3, no. 6, pp. 1–8, 2023.
- [12] M. M. Salim, M. Kim, S. K. Singh, and J. H. Park, "Zero-Trust Blockchain-Enabled Framework for Scalable and Secure IoT

- Networks,” *Future Generation Computer Systems*, vol. 175, 108093, 2025.
- [13] S. Alahmaril and A. Alkharashi, “Privacy-Aware Federated Learning Framework for IoT Security Using Chameleon Swarm Optimization and Self-Attentive Variational Autoencoder,” *Computer Modeling in Engineering & Sciences*, vol. 143, no. 1, pp. 849–873, 2025.
- [14] S. A. Mahmud, N. Islam, Z. Islam, Z. Rahman, and S. T. Mehedi, “Privacy-Preserving Federated Learning-Based Intrusion Detection Technique for Cyber-Physical Systems,” *Mathematics*, vol. 12, no. 20, pp. 3194–3204, 2024.
- [15] S. Niknam, H. Dhillon, and J. Reed, “Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges,” *IEEE Communications Magazine*, vol. 58, no. 6, pp. 46–51, 2020.
- [16] M. A. Khan *et al.*, “Comparative Analysis of Centralized and Federated Intrusion Detection in IoT-Enabled Cyber-Physical Systems Under Data and Label-Skew,” *IEEE Access*, vol. 1, no. 1, pp. 99–112, 2025.
- [17] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, “Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey,” *ACM Computing Surveys*, vol. 55, no. 9, pp. 191–234, 2023.
- [18] B. McMahan, E. Moore, D. Ramage, S. Hampson, and S. Avestimehr, “Communication-Efficient Learning of Deep Networks from Decentralized Data,” in *Proc. the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2017, pp. 1273–1282.
- [19] K. Bonawitz, V. Ivanov, B. Kreuter *et al.*, “Towards Federated Learning at Scale: System Design,” in *Proc. Machine Learning and Systems (MLSys)*, 2019, vol. 1, pp. 374–388.
- [20] W. Li, K. Fan, J. Zhang *et al.*, “Enhancing Security and Privacy in Federated Learning Using Low-Dimensional Update Representation and Proximity-Based Defense,” *IEEE Transactions on Knowledge and Data Engineering*, vol. 37, no. 6, pp. 3372–3385, 2025.
- [21] P. Kairouz, B. McMahan, B. Avent *et al.*, “Advances and Open Problems in Federated Learning,” *Foundations and Trends in Machine Learning*, vol. 14, no. 2, pp. 192–210, 2021.
- [22] J. Zhu, J. Cao, D. Saxena *et al.*, “Blockchain-empowered Federated Learning: Challenges, Solutions, and Future Directions,” *ACM Computing Surveys*, vol. 1, no. 11, pp. 1–31, 2023.
- [23] R. Chohan, K. Mal, and M. J. Afridi, “Blockchain-Based Authentication for Secure IoT Networks: A Decentralized Approach to Identity Management and Data Integrity,” *Kashf Journal of Multidisciplinary Research*, vol. 2, no. 7, pp. 225–247, 2025.
- [24] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “Blockchain Challenges and Opportunities: A Survey,” *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018.
- [25] S. Abdulrahman and M. Useng, “Blockchain and Distributed Ledger Technologies for IoT Security: A Survey paper,” *Mesopotamian Journal of Computer Science*, vol. 1, pp. 5–9, 2022.
- [26] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, “Smart Contract-Based Access Control for the Internet of Things,” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1594–1605, 2019.
- [27] A. Dorri, S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT Security and Privacy: The Case Study of a Smart Home,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8088, 2019.
- [28] H. D. Zubaydi, P. Varga, and S. Molnár, “Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review,” *Sensors*, vol. 23, no. 2, pp. 788–827, 2023.
- [29] M. R. Hasan, A. Alazab, S. B. Joy *et al.*, “Smart Contract-Based Access Control Framework for Internet of Things Devices,” *Computers*, vol. 12, no. 11, pp. 240–267, 2023.
- [30] H. Xue, D. Chen, N. Zhang *et al.*, “Integration of blockchain and edge computing in internet of things: A survey,” *Future Generation Computer Systems*, vol. 144, pp. 307–326, 2023.
- [31] D. Chawla, D. Chawla, A. Shrivastava, and M. Mundher, “Blockchain and Federated Learning Integration for Secure IoT and Cyber-Physical Systems,” in *Proc. IEEE 5th International Conference on ICT in Business Industry & Government*, 2025, pp. 1–7.
- [32] I. B. Ababio, J. Bieniek, M. Rahouti *et al.*, “A Blockchain-Assisted Federated Learning Framework for Secure and Self-Optimizing Digital Twins in Industrial IoT,” *Future Internet*, vol. 17, no.1, pp. 13–28, 2025.
- [33] M. Asad and S. Otoum, “Integrative Federated Learning and Zero-Trust Approach for Secure Wireless Communications,” *IEEE Wireless Communications*, vol. 31, no. 2, pp. 14–20, 2024.
- [34] S. Li, M. Iqbal, and N. Saxena, “Future Industry Internet of Things with Zero-trust Security,” *Information System Frontier*, vol. 26, pp. 1653–1666, 2024.
- [35] W. Ning, Y. Zhu, C. Song *et al.*, “Blockchain-Based Federated Learning: A Survey and New Perspectives,” *Applied Sciences*, vol. 14, no. 20, pp. 9459–9463, 2024.
- [36] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, “Federated Learning for IoT: A Survey of Techniques, Challenges, and Applications,” *Computers & Industrial Engineering*, vol. 149, no. 1, 9, 2020.
- [37] W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, “Blockchain-Based Federated Learning for Securing Internet of Things: A Comprehensive Survey,” *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–43, 2023.
- [38] S. R. Islam, M. S. Hossain, and G. Muhammad, “Towards Blockchain-Based Federated Learning in Categorizing AIoMT Devices,” *BMC Medical Imaging*, vol. 24, 1, 2024.
- [39] J. A. Alenizi, M. A. Alshahrani, and M. A. Alharthi, “Zero Trust: Applications, Challenges, and Opportunities,” *International Journal of Network Security*, vol. 23, no. 4, pp. 41–62, 2024.
- [40] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, Privacy and Trust in Internet of Things: The Road Ahead,” *Computer Networks*, vol. 76, pp. 146–164, 2015.

Copyright © 2026 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited ([CC BY 4.0](https://creativecommons.org/licenses/by/4.0/)).