Decentralized Edge Intelligence: A Big Picture on Integrating Blockchain and Federated Learning for IoT Security

Deepak Puthal[1], Pradip Kumar Sharma[2], Amit Kumar Mishra[3], Chan Yeob Yeun[4], Antonella Longo[5], and Saraju P. Mohanty[6]

[1, 4] Indian Institute of Management Bodh Gaya, India
[2] University of Aberdeen, UK
[3] Aberystwyth University, UK
[4] Khalifa University, UAE
[5] University of Salento, Italy
[6] University of North Texas, Denton, USA

Abstract

Compromising in cyber security, especially regarding data leaks and single points of failure, pose a problem to the rapid growth of the Internet of Things (IoT). A solution for these issues is Blockchain and Federated Learning (FL) integration, which offer a more private and decentralized method for ensuring the security of IoT devices. This integration improves the integrity of data autonomously, while authentication and secure model aggregation block any attempts to tamper. Moreover, FL allows Artificial Intelligence (AI) to be trained on devices, making the exposure of data less likely. This improves real-time threat response, cuts down on communication overhead, and boosts the resilience of IoT to cyber-attacks. At the same time, trade-offs in power expenditure or processing overhead must be carefully considered to maintain a balanced approach to energy use, infrastructure networking latency, and overall operational efficiency. In this paper, we analyze the attack surface and emerging vulnerabilities of Blockchain-FL based IoT systems while constructing a taxonomy of the threats posed. They focus on novel security frameworks aimed at constructing next generation IoT system infrastructure, which is scalable, robust, intelligent and above all, secure.

Keywords. Internet of Things, Federated Learning, machine learning, Edge Computing, Cyber Security, Cyber Threats.

1. Introduction

The adoption of the Internet of Things (IoT) has transformed multiple sectors, such as smart cities, healthcare, industrial automation, and autonomous systems [1]. While the benefits are commendable, the surge of interconnected IoT devices has caused worrying security and privacy concerns. Their traditional approach to cloud-based security is ineffective because of centralization, susceptibility to cyber-attacks, elevated latency speeds, and restricted bandwidth. IoT devices, generally characterized by low computing and energy capabilities, find it difficult to utilize advanced security features and are, therefore, exposed to unauthorized access, breaches, and hostile attacks [2]. These factors call for effective performance-preserving flexible, scalable, decentralized security frameworks that are needed to protect IoT ecosystems.

Security of the IoT ecosystem hinges on data privacy and integrity as a fundamental concern in IoT security. The incorporation of conventional machine learning (ML) techniques centered around data aggregation pose a risk of hacking and compliance issues like General Data Protection Regulation (GDPR) and Digital Personal Data Protection Act (DPDP Act) 2023. Furthermore, single points of failure (SPOF) existent in cloud based security frameworks enable distributed denial of service (DDoS) attacks, data manipulation, and unauthorized intrusion. These issues necessitate the design of autonomous, trustless, and tamper-proof security solutions which ensure data confidentiality, integrity, and real-time threat detection in IoT networks.

Of late, Blockchain technology and Federated Learning (FL) have come forth as disruptive technologies to resolve IoT security issues. Through Blockchain, secure identity management and access control is possible along with transparent data exchange because it provides a decentralized, immutable, and tamper-proof ledger [3]. In addition, smart contracts in IoT devices automation of security policies gives additional IoT protection by verifying the identity of devices and enforcing proper access control policies. At the same time, FL stands for privacy-preserving AI model training, which permits the training of an ML model on an IoT device without the need to move the raw data to a centralized server. By this means, the user data does not need to be exposed and can easily be hidden in IoT devices while exposing strong AIdriven security enforcement [4].

The combination of Blockchain and FL brings forth a new approach for edge intelligence under IoT security. On one hand, Blockchain ensures trust, data integrity, and decentralized identity management, on the other side FL provides real-time adaptive security capabilities with the help of distributed artificial intelligence (AI) models. Collectively, these technologies enable IoT networks to function securely, independently, and efficiently positing threats of adversarial attacks, model poisoning, or unauthorized access to devices. Nevertheless, the integration of Blockchain and FL in IoT Security brought forward challenges such as scalability, computation efficiency, and interoperability issues which must be resolved in order to mainstream next generation networks [5].

This paper investigates the integration of Blockchain and FL in IoT security, particularly looking at their synergy, implementation architectures, and tradeoff in performance. The combination of Blockchain and FL can shift the paradigm of IoT security to a trustless and privacy preserving intelligent defense systems that safeguards critical infrastructure, and consumer IoT devices in the age of next-gen computing.

2. IoT Security Challenges

2.1 IoT Cyber Risks

An instance of the breach of IoT security is the Mirai botnet attack, where hackers took advantage of people's lax security precaution in IoT devices to generate a large subnet of bots. This caused a lot of internet services to disrupt. In the same way, a type of cyber attack known as man-in-the-middle (MitM) enables infringers to capture and alter communications between IoT devices. This can lead to exposure of confidential information [6]. Besides, IoT devices are used in mixed environments where many different communication protocols, device vendors, and software platforms are used. By not having a single set standard, there are weak security measures put into place which increases the chances of breaching data. With such complexities, most traditional integrated security systems do not work, along with a shift towards the use of Blockchain technology and FL, decentralized trust based security systems will be needed. A fair comparison between the Traditional IoT security and Blockchain and FL integration is shown in Table 1.

2.2 Centralized System Vulnerabilities

Considerable personal, financial, and medical information is simultaneously collected and sent over by IoT devices making them an easy target for cybercriminals. The conventional IoT secutity model depends on centralized online nfrastructures, which capture information from peripheral devices and sends it over for processing where it is stored in a single central location [7]. This model certainly eases the analysis and subsequent decision steps, however, it brings along a number of privacy and security challenges:

- Centralized cloud servers serve as main data stores which makes them susceptible to potential attacks. These attacks result in massive data breaches and subsequent identity theft, financial frauds, and blatant disregard of laws and regulations.
- Cloud service providers have direct control on their data centers and, as a result, users have very little control on how their data is managed or processes raising concerns on independence of the data.

2.3 Real-Time Security at the Edge

IoT systems run on several real-time environments, such as, autonomous vehicles or smart healthcare systems which are considered critical areas where security threats can be dangerous [8]. In these circumstances, the ability to detect threats and act upon them to avoid disasters is of a key importance.

Conventional security paradigms depend on cloud-based threat intelligence systems, which suffer from latency and bandwidth constraints. Security can be improved and response times significantly shortened with edge computing which processes information closest to the source [2, 6]. Nonetheless, protecting these edge environments call for a different set of challenges:

- Constrained Computational Capabilities: Many IoT edge devices have extremely low processing capabilities and memory, rendering the implementation of sophisticated encryption methods and security protocols impossible.
- Proactive Threat Neutralization: Edge devices need to have autonomous security responses that can detect, understand, and respond to malicious attacks without human or cloud intervention.
- Trust and Scalability Challenges: Providing secure communications for thousands of IoT edge devices poses the challenge of developing light-weight authentication protocols and trust management systems.

Table 1: Comparison of Traditional IoT Security Models with Blockchain-FL integration

Security Feature	**Traditional IoT Security**	**Blockchain-FL Security**
Data Integrity	Prone to tampering	Blockchain ensures immutability
Authentication	Centralized identity verification	Decentralized identity via DID
Threat Detection	Cloud-based AI	FL-based on-device anomaly detection
Latency	High due to centralized processing	Low due to local model execution
Scalability	Limited by cloud resource constraints	Decentralized, distributed learning
Data Privacy	Low (Centralized data storage)	High (No raw data sharing)
Security & Trust	Medium (Cloud-based security)	High (Tamper-proof blockchain)
Computational Cost	Low	Moderate (Optimized blockchain)

3. Blockchain for Secure and Transparent IoT

Because decentralization, transparency, and security are so important, the integration of Blockchain technology into IoT security frameworks is receiving greater attention. IoT devices need to ensure vast data access control, data integrity, and confidentiality. The use of blockchain makes possible the efficient IoT ecosystems through automated security policies, enhanced data integrity, and immutable, distributed trustless ledger systems [3, 9].

3.1 Blockchain based Environment

The application of Blockchain technology through an IoT ecosystem results in a trustless and decentralized framework, eliminating the need for central authorities [3].

The application of Blockchains in IoT Security and their Key Benefits:

1. Immutable: Every transaction recorded in a Blockchain ledger is stored cryptographically, meaning that they are unable to be deleted or modified resulting in tamper free data storage.
2. Decentralization: By fracturing trust across different nodes, the Blockchain eliminates the need to depend on a single authority which minimizes single point of failures.
3. Data Integrity: The unauthorized alterations of IoT transactions are ensured to be uncovered with the shift to Blockchain because the data becomes transparent and accountable verifiably.

As an illustration, consider smart healthcare systems. With IoT devices for medical care, patient information can be protected using Blockchain technology. Every health record can be hashed to ensure data integrity, and the hashes along with relevant meta-data can be stored in a public Blockchain ledger where no one can modify it.

3.2 Consensus Mechanisms for IoT Transactions

The specific consensus mechanism determines the recording of legitimate transactions to a Blockchain which is the essence or heart of the protocol. Due to IoT devices' scope limitations, a good compromise on the consensus mechanism that maintains the balance between security, speed and scalability has to be made [10].

Common Consensus Mechanisms for IoT Security:

1. Proof of Work (PoW): Offer High Security at Great Expense

PoW is in use for Bitcoin and for its use, a complex cryptographic puzzle must be solved to achieve the goal, thereby making PoW very secure. Unfortunately, the high energy usage and low speed make PoW unworkable under IoT conditions.

2. Proof of Stake (PoS): Low Power Consumption Substitute

PoS chooses a certain number of validators per round depending upon stake ownership and hence power usage is less compared to PoW. It's easier to scale and more appropriate for IoT networks where energy consumption is an issue.

3. Proof of Authentication (PoAh): Very Scalable and Lightweight

PoAh is dedicatedly design for resource constraint devices. This is the most appropriate for smart sensors and other low power industrial IoT devices.

Fraudulent transactions and unauthorized interactions with devices can take place if proper consensus mechanisms are not put in place. When ensuring the security of the IoT devices, it is important to safeguard the device interaction from and towards it’s ecosystem. To accomplish it, the interaction of fraudulent and non-fraudulent data streams with IoT devices must be controlled in real time. It can be argued that security attributes of decentralized IoT applications can be improved by removing the centralized security point which results in reduced trust on the third party security service providers [11]. The dependability and overall security package of IoT networks can be enhanced with the use of consensus mechanisms which make them a prospective candidate for making the IoT environment safe and secure.

4. FL for Privacy-Preserving Intelligence

The use of AI in IoT networks automation, decision making, and real-time analytics has greatly improved over the years. However, centralized data collection though useful for traditional AI models, raises issues in data privacy, security, and even regulatory compliance [12]. With data privacy concerns on the rise, FL becomes quite handy as it enables model training and requires no transfer of raw data to a server.

4.1 FL Enables AI Training

Standard AI models typically need extensive amounts of data to train efficient ML models. Within IoT ecosystems, smart sensors, medical devices, industrial controllers, and self-driving vehicles are constantly creating critical data [4, 13]. Unfortunately, transferring this information to centralized cloud servers for training comes with various obstacles.

1. Privacy Threats: Sensitive user information needs to be exposed to third party cloud services, which heightens the chances of data leaks.
2. Expensive Bandwidth: The data streams created by IoT devices are huge, which makes their transmission costly and inefficient.
3. Compliance Violations: Regulations like GDPR and DPDP Act. come with stringent constraints on data storage and movement.

FL removes the requirement for centralized data gathering by offering the option of local IoT edge device AI model training. Instead of transmitting data to the cloud, FL permits IoT devices to:

- Train AI models on localized data sets.
- Send only model change (gradients or parameters) to a central aggregator.
- The aggregator integrates model updates received from multiple devices to enhance the global AI model without the need to harvest raw data.

This approach allows for data to remain local while still profiting from global collaborative learning. An example of this would be Google's FL system used in predictive text and auto-correction in Android devices.

4.2 Role of FL in Securing IoT-Edge Devices

Due to limited computational power, edge devices often lack adequate security features which makes them susceptible to attacks [14]. Because of the following reasons, threats are augmented with FL:

1. Reducing Risk of Data Breach: The fact that data never leaves the IoT device mitigates the risk of interception, MitM attacks, and unauthorized access.
2. Achieving Localized Anomaly Detection: AI models for real-time anomaly detection can be trained and deployed directly on edge devices, thanks to FL.
3. Decreasing Dependency on Encrypted Cloud Security: Encrypted data transfer to centralized cloud servers has to be done with traditional AI systems, FL eliminates this dependency by processing data locally.

Integrating FL with AI powered Intrusion Detection Systems (IDS) to trace security breaches in IoT networks is possible. Every device is capable of developing a security model relative to its own network traffic, receiving and sending model parameters, as opposed to raw logs, thus limiting the chances of cyberattacks [14].

4.3 Preserving Privacy with Decentralized Learning

The AI powered models that need training from a central point present a significant void for privacy issues, which include:

1. Data Leakage: With the storrage of IoT data in the could, cyberattacks are more likely.
2. Control Deficiency: There is little to no control for users and organizations over how their data is handled after leaving the IoT device.
3. Compliance Violation: Privacy laws for sensitive data gathering and storing can be hard to achieve for global IoT systems and networks.

Differential privacy techniques are included in FL by adding random noise before applying model updates. It is ensured the model updates cannot be traced back to specific users as they are in no position to get to a single user. For each individual, there is sufficient guarantee of privacy, while still remaining statistically useful for AI training.

The Semi-Private Multi-Party Computation (SMPC) is a form of cryptography that allows individuals to compute functions over shared data without revealing the data itself. In conjunction with FL, SMPC guarantees the private information is not leaked when IoT devices train AI models collaboratively. Sensitive information is shielded during the process of aggregation because FL model updates are encrypted.

The integration of FL with Blockchain technology enhances the capability of model update retention within an immutable ledger. The level of transparency and auditability in the training of AI models. The protection against model poisoning attacks, where an attacker attempts to compromise AI models by offering false updates.

5. Integrating Blockchain and Federated Learning for IoT Security

5.1 How Blockchain and FL Complement Each Other

Like many technologies, Blockchain is quite new, and its applications do not only apply to currencies such as Bitcoin and Ethereum. Its intersection with FL is an example where Blockchain can increase privacy, security, and trust within the Federated framework. Most AI-driven functionalities require data to be aggregated at a central server which poses the danger of identity theft and leakage of sensitive information. FL resolves this issue of data privacy by keeping data on edge devices. At the same time, Blockchain ensures data integrity is maintained because there are no unauthorized alterations made to the model updates before aggregation [11].

One of the problems of trust in FL is the putative trust in participants and their model contributions. Malicious clients can implement so-called data poisoning attacks are used to manipulate the values of model parameters (for example, upload bad models). By take a verifiable hash of the FL update, Blockchain strengthens this issue by making it possible to record information that can be verified to exist without being able to alter it. Furthermore, countless devices that comprise the IoT still need to be authenticated. Most of these devices depend on an identity provider which introduces a single point of failure. Managed Access Control Lists based on the tamper-proof systems replace traditional authentication methods and improve security and resilience.

Incentive participation is another tricky problem while using FL as edge devices may be hesitant to participate owing to resource cost. Through smart contracts, Blockchain can employ token-based incentive methods where participating devices are compensated through cryptocurrency or credit them for their efforts. Merging Blockchain with FL will enable organizations to create an AI-infused ecosystem that is more secure, decentralized, and reliable, especially for IoT solutions countries [9, 11]. The complementary strengths of Blockchain and FL in IoT security is thoroughly summarized in the table 2.

Table 2: the complementary strengths of Blockchain and FL in IoT security

Feature	**Blockchain**	**Federated Learning**	**Synergy**
Privacy	Not inherently private	Localized training keeps data on the device	FL ensures privacy while Blockchain secures updates
Security	Tamper-proof and immutable ledger	AI model may be vulnerable to adversarial attacks	Blockchain secures model integrity
Decentralization	Fully decentralized trust model	Distributed learning with multiple edge devices	FL and Blockchain both reduce reliance on central authorities
Scalability	Can be computationally expensive	Reduces cloud dependency	Optimized Blockchain protocols enhance FL efficiency

5.2 Architecture for Decentralized Edge Intelligence

A clear architectural framework design is essential if Blockchain and FL are going to be combined for IoT security. This architecture provides secure, decentralized, and privacy-preserving intelligence at the edge of IoT networks. The developed framework is composed of main elements which, when put together, aim at improving trust, security, and efficiency in decentralized AI-driven IoT systems. The key components of the architecture are detailed as follows.

5.2.1 IoT Edge Nodes (Data Sources)

Devices like sensors, smart wearables, smart cameras, and industrial controllers form IoT Edge nodes and are main data sources. The devices filter and analyze the raw data on the device level. Unlike the typical paradigm where data is sent to a centralized cloud, FL allows every node to perform a Machine Learning (ML) model training on its local data. The identity and transaction of the devices is secured using Blockchain that guarantees data integrity and access secrecy [6].

5.2.2 Local Model Training and Secure Aggregation

IoT devices utilize FL frameworks such as TFF and PySyft for on-device training [15]. Model updates are not directly shared; rather, they are verified through Blockchain technology. The results of local training are hashed and stored onto the Blockchain, allowing only legitimate updates to be included into the global model aggregation. This system helps to mitigate adversarial attacks, for example, model poisoning attacks.

5.2.3 Blockchain-Based Smart Contracts for Model Aggregation

As with every contract, a smart contract autonomously enforces consensus and trust during the FL model aggregation process. They delineate the processes that validate the model updates prior to the aggregation. Model aggregation servers, also known as decentralized coordinators of FL, improve the global model with Blockchain-enabled updates. In doing so, they mitigate the problems caused by centralized aggregation servers, which increases the security and transparency of the system [15].

5.2.4 Decentralized Identity and Access Control

Another important security component in the framework is decentralized identity management. The IoT devices issue Blockchain-based self-sovereign unique digital identities, which lead to trustless authentication and access control capabilities [15]. Through the smart contracts implemented on the Blockchain, FL training access is provisioned or revoked without relying on the centralized identity provider. This leads to highly resilient and tamper-proof authentication systems, greatly minimizing the chances of identity theft and unauthorized access.

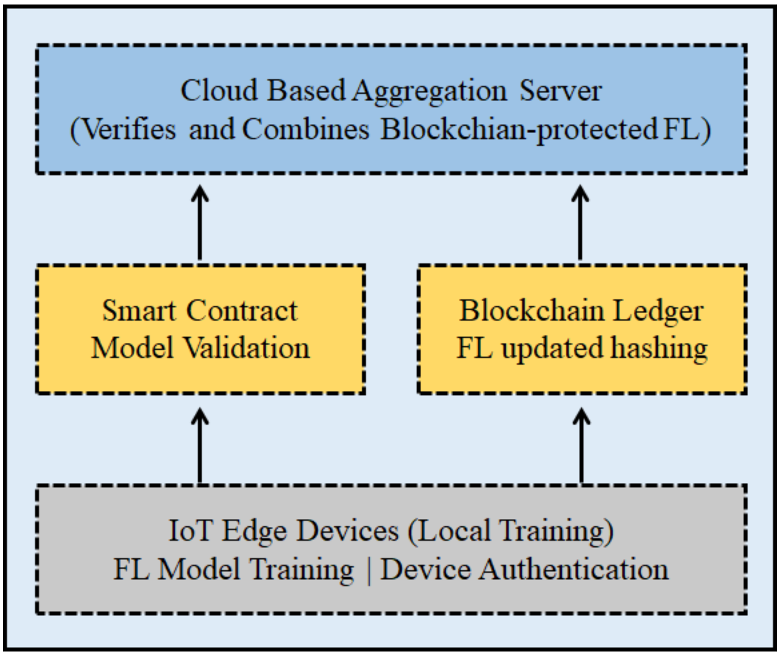
Cloud Based Aggregation Server
(Verifies and Combines Blockchian-protected FL)
Smart Contract
Model Validation
Blockchain Ledger
FL updated hashing
IoT Edge Devices (Local Training)
FL Model Training | Device Authentication

Figure 1: Layered architecture diagram for Blockchain-FL-based IoT security

The integrating Blockchain with FL architecture diagram is as shown in Figure 1; and the details of the steps are as follows.

1. **Data remains local** – IoT devices utilize FL methodologies to independently train local models.
2. **Model updates are logged on the Blockchain** – The hashes of the FL updates are logged on the Blockchain for FL to verify them.
3. **Consensus validation** – The updates are authenticated and verified through smart contracts for model poisoning attacks.
4. **Secure model aggregation** – Only authenticated and validated updates are included in the global AI model.
5. **Decentralized AI deployment** - The enhanced AI model is sent back to the IoT edge devices.

6. Performance Analysis and Comparative Evaluation

6.1 Security and Efficiency Trade-Offs

The adoption of Blockchain and FL for IoT security creates a binary value of trade-off for security and efficacy of the system in relation to the available resources. Despite these innovations supporting trust, privacy, and cyber resiliency, they come at the cost of additional computation, communication, and energy expenses [11, 14, 15]. Addressing these issues is a prerequisite for any IoT security architecture to be useful and implementable.

6.1.1. Security Benefits vs. Computational Overhead

The FL and blockchain technologies come with an additional computational cost, but at the same time, these cost outweigh due to the benefits provided in terms of security. In Blockchains, integrity is tampered with and trust is also decentralized through the use of consensus algorithms like the PoW method and the less expensive PoS and PoAh method. These mechanisms make it easier to compute, however, require resources in plenty on the computing side, particularly in IoT settings which are low on energy. In addition, angry smart contracts that need to be executed to make sure that security policies are executed also cause system delays in processing time.

Alternatively, FL keeps raw data on the IoT edge devices which ensures protection from central servers thereby FL means of lowering privacy. This, however, makes the computational requirement to aggregate and validate securely much higher due to the frequent remote model updates called weights, and gradients. This conflict captures the essence of the need for the development of better optimized consensus algorithm and more performant industrial FL training methods. A detailed comparison between the security and performance is given as in the table 3.

6.1.2. Privacy Guarantee vs. Communication Overhead

As with all techniques, there is a cost associated with decentralization with AI model training for privacy, and in this case, it is considerable communication overhead. The model updates in FL are the most common type of change passed between edge devices to the aggregator. These changes and additions claims resources bandwidth for IoT networks that are already thin. Moreover, transactions in Blockchain also need to undergo validation via a consensus which makes the whole process slow and may hinder critical applications such as real-time monitoring of anomalies in IoT.

In an effort to tackle these challenges, methods like Secure Aggregation paired with a unique compression strategy decreases the data transmission frequency along with its size while retaining promised privacy. These methods can be implemented without affecting the security systems in place.

6.1.3. Security Strength versus Energy Consumption

As with many modern technologies, one of the greatest challenges when implementing Blockchain and FL in the IoT ecosystem is energy consumption. Sensors operating on batteries do not have sufficient resources available for Blockchain-based security frameworks which need consistent cryptographic validation and transaction verification. Likewise, FL consumes additional energy on-device AI training, especially for deep learning networks that use extensive resources.

Newer mechanisms for achieving consensus, such as PoAh enhance energy efficacy by lessening the likelihood of computing abuse while still maintaining some level of security. Other energy-efficient approaches are offered by lightweight FL models like AI inference and training with TinyML on low-power devices. It is imperative to find methods that strengthen security while lowering energy expenditure to foster sustainable IoT systems.

Table 3. Performance Analysis of Blockchian and FL in security and privacy

Parameter	**Blockchain**	**Federated Learning**	**Combined Blockchain-FL Approach**
Security	High (Immutable Ledger)	Medium (Privacy-Preserving AI)	High (Decentralized AI Security)
Latency	Medium-High (Consensus Overhead)	Medium (Gradient Updates)	High (Combined Overhead)
Computational Cost	High (Cryptographic Operations)	Medium (On-Device AI Training)	High (Combined AI + Blockchain Processing)
Scalability	Limited (Throughput Bottleneck)	High (Parallel Edge Training)	Medium (Blockchain Scalability Issues)

6.2 Comparison with Traditional IoT Security Mechanisms

The use of Blockchain and FL for IoT security is a paradigm shift from existing traditional deployed models. Most conventional IoT security mechanisms are based on centralized models which, for all their strengths, create very harmful weaknesses like single points of failure, latency, and data privacy concerns. On the other hand, security based on Blockchain coupled with FL advanced decentralized models offer better strength towards IoT system support, real time threat response and improved data privacy.

6.2.1. Security Models Centralized versus Decentralized Blockchain-FL Security

The security of IoT systems relies heavily on cloud-based security models whereby cloud servers are trusted parties for authentication, access, and data verification. The following concerns still persist with this approach:

- Single Point of Failure: Centralized cloud servers can become targets of cybercriminals and the downfall of a centralized cloud server can lead to the entire IoT network becoming insecure. This becomes a target because it becomes a target for malefactors.
- High Latency: The SPOF model requires cloud processing in order to respond to threats, so IDS and anomaly detection that utilize artificial intelligence require additional time to respond to risks.
- Data Privacy Risks: The centralization of IoT data presents the greatest risk regarding privacy. Sensitive information is not only at risk from being accessed, but can also be leaked via external databases.

On the contrary, Blockchain and FL eliminates these concerns by decentralizing the enforcement of security policies and removing the need for a centralized authority. In doing so, these technologies reduce the time required to enforce security measures, and sensitive data is kept on edge devices as opposed to central servers. A comparative analysis of centralized security models vs. decentralized blockchain-FL security is given in Table 4(a).

6.2.2. Blockchain-FL and Cloud-Based AI Security

AI security solutions that depend on the cloud take advantage of centralized data processing systems, where IoT security information is sent to the cloud infrastructure for processing. While employing these methods makes cyber threat detection and authentication easier, they also come with grave security issues and inefficiencies. On the other hand, Blockchain-FL has an edge over its peers due to the following reasons:

- Privacy-Preserving Model Training: FL does not require sending raw data to central servers. Due to this, the chances of data breaches drastically increase. In this case, model training is performed within IoT edge devices.
- Tamper-Proof Model Updates: With Blockchain, model updates stay tamper-proof as the cryptographic hashes are stored, protecting against data poisoning from malicious actors.
- Dynamic Threat Detection: Blockchain FL permits AI decision making to happen on the periphery, which means that Blockchain-FL does not depend on cloud computing, allowing abnormal signal detection to happen at the edge – boosting security levels.

Because of these considerations, Blockchain-FL has proven to be more effective than the solution offerings provided by cloud-based AI security perpetuated in constantly changing and senstive IoT contexts. A comparative analysis of Blockchain-FL vs. cloud-based AI security is given in Table 4(b).

6.2.3. Access Control and Management

Conventional IoT Security commonly applies Role Based Access Control (RBAC) or Attribute Based Access Control (ABAC) in order to manage permissions and limit access to information comparatively easier. Nonetheless, these models have significant challenges:

- Centralized Identity Management: RBAC relies on a central identity provider which can lead to credential abuse and identity theft through privilege escalation attacks.
- Manual Policy Enforcement: Continuous manual updates corresponding to changes in user roles and their permissions is a requirement for both RBAC and ABAC, which adds to the administrative burden.

Smart Contracts based on Blockchain technology provide a different approach: they manage access control policies in a fully automated self-enforcing way. Unlike RBAC, which needs reliance on a trusted third party, smart contracts operate with zero trust – authentication is given based on cryptographic proof, not user claims. This change makes the system more secure and minimizes the risks posed by insiders as well as credential and token abuse. A comparative analysis of smart contract-based security vs. role-based access control is given in Table 4(c).

Table 4: Comparative study of the traditional Security with Blockchain and FL Integration

Feature	Traditional Centralized Security	Blockchain-FL Security
Trust Model	Centralized Cloud-Based Security	Decentralized Peer-to-Peer Security
Data Integrity	Vulnerable to Tampering	Immutable Blockchain Transactions
AI Training	Centralized Data Collection	Privacy-Preserving Federated Learning
Resilience	SPOF Risks	Distributed, Attack-Resistant Framework

(a) Centralized Security Models vs. Decentralized Blockchain-FL Security

Comparison Metric	Cloud-Based AI Security	Blockchain-FL Security
Latency	High (Data Transmission to Cloud)	Low (On-Device Processing)
Privacy Risks	High (Centralized Data Processing)	Low (Local Training in FL)
Computational Cost	Medium (Centralized AI Training)	High (Distributed AI & Blockchain)
Security	Medium (Cloud Security Measures)	High (Blockchain Encryption & Trustless AI)

(b) Blockchain-FL vs. Cloud-Based AI Security

Feature	RBAC/ABAC Security Models	Blockchain Smart Contract Security
Authentication	Centralized User Verification	Decentralized Identity Verification
Access Control	Predefined Role-Based Permissions	Dynamic, Rule-Based Smart Contracts
Scalability	Medium (Limited to Enterprise Use)	High (Decentralized, Trustless Model)

(c) Smart Contract-Based Security vs. Role-Based Access Control (RBAC)

7. Conclusion

Blockchain technology coupled with FL is a paradigm shift in IoT security by supporting the features of trustless operation, privacy-preserving AI, data exchange, and eliminating the need for central authority security controls. This paper examined Blockchain and FL convergence, architectural integration, and their applications in smart cities, health care, and industrial IoT contexts. Also, we investigated the balance of security and efficiency, the gaps in scalability, interoperability, and possible approaches for effective large-scale implementation.

References

[1] I. S Udoh, and G. Kotonya. "Developing IoT applications: challenges and frameworks." *IET Cyber-Physical Systems: Theory & Applications* 3, no. 2 (2018): 65-72.

[2] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller. "Landscape of IoT security." Computer Science Review 44 (2022): 100467.

[3] V. Maurya, V. Rishiwal, M. Yadav, M. Shiblee, P. Yadav, U. Agarwal, and R. Chaudhry. "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions." *Peer-to-Peer Networking and Applications* 18, no. 1 (2025): 1-35.

[4] P. Qi, D. Chiaro, A. Guzzo, M. Ianni, G. Fortino, and F. Piccialli. "Model aggregation techniques in federated learning: A comprehensive survey." *Future Generation Computer Systems* 150 (2024): 272-293.

[5] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. V. Poor. "Federated learning for internet of things: A comprehensive survey." *IEEE Communications Surveys & Tutorials* 23, no. 3 (2021): 1622-1658.

[6] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani. "A survey of machine and deep learning methods for internet of things (IoT) security." IEEE communications surveys & tutorials 22, no. 3 (2020): 1646-1685.

[7] J. Li, J. Li, D. Xie, and Z. Cai. "Secure auditing and deduplicating data in cloud." *IEEE Transactions on Computers* 65, no. 8 (2015): 2386-2396.

[8] Y. B. Zikria, H. Yu, M. K.l Afzal, M. H. Rehmani, and O. Hahm. "Internet of things (IoT): Operating system, applications and protocols design, and validation techniques." *Future Generation Computer Systems* 88 (2018): 699-706.

[9] A. M. Saleh. "Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review." *Blockchain: Research and Applications* (2024): 100193.

[10] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang. "A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling." *ACM Computing Surveys (CSUR)* 53, no. 1 (2020): 1-32.

[11] S. Kayikci, and T. M. Khoshgoftaar. "Blockchain meets machine learning: a survey." *Journal of Big Data* 11, no. 1 (2024): 9.

[12] L. Li, Y. Fan, M. Tse, and K-Y. Lin. "A review of applications in federated learning." *Computers & Industrial Engineering* 149 (2020): 106854.

[13] F. Foukalas, and A. Tziouvaras. "Federated learning protocols for IoT edge computing." *IEEE Internet of Things Journal* 9, no. 15 (2022): 13570-13581.

[14] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha, and G. Srivastava. "Federated-learning-based anomaly detection for IoT security attacks." *IEEE Internet of Things Journal* 9, no. 4 (2021): 2545-2554.

[15] Y. Qu, M. P. Uddin, C. Gan, Y. Xiang, L. Gao, and J. Yearwood. "Blockchain-enabled federated learning: A survey." *ACM Computing Surveys* 55, no. 4 (2022): 1-35.