Designing a Scalable and Secure IoT Framework Using Federated Learning and Blockchain for Edge-AI Devices

S. Kannadhasan[1], Pilli Lalitha Kumari[2], K. Suresh[3], Badepally Mallaiah[4], Abirami G.[5] and Syed Zahidur Rashid[6]

[1]*Department of Electronics and Communication Engineering, Study World College of Engineering, Coimbatore - 641 105, Tamil Nadu, India*

[2]*Department of Computer Science and Engineering, Visakha Institute of Engineering & Technology, 88th Division, Narava, Visakhapatnam - 530027 Andhra Pradesh, India*

[3]*Department of Computer Science and Engineering, J. J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India*

[4]*Department of Information Technology, CVR College of Engineering, Hyderabad, Telangana, India*

[5]*Department of CSE, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India*

[6]*Department of Electronic and Telecommunication Engineering, International Islamic University Chittagong, Chittagong, Bangladesh*

Keywords: Federated Learning, Blockchain, Edge Computing, IoT Security, Decentralized Intelligence.

Abstract: The need for flexible, secure, and intelligent data processing at the edge has been propelled by the fast development of Internet of Things (IoT) ecosystems. Existing federated learning (FL) methods usually suffer from system heterogeneity, privacy threats, and excessive communication cost. Additionally, adopting blockchain technology within FL typically adds both latency and complexity which limits its practical applicability to resource-constrained environments. In this paper, we introduce Edge Secure-Fed Chain, a new lightweight and trust-aware federated learning framework that incorporates blockchain, designed to enable secure and decentralized coordination among edge-AI devices. In contrast to existing approaches, our architecture achieves low latency via protocol-optimizing consensus, enables dynamic smart contract driven ML workflows, and improves personalization through adaptive local training. We also propose a resilient multi-tiered aggregation system (against adversarial and non-IID data conditions), together with proactive defense components (network anomaly detection and client reputation scoring). Edge Secure- Fed Chain outperforms the existing systems by overcoming their limitations as illustrated in this paper, which exhibit to be more scalable, preserve privacy, and have real-time performance in edge oriented IoT applications. Extensive experimental assessments validate the framework's efficacy, security, and adaptability to various IoT applications.

1 INTRODUCTION

However, this growth is not free of challenges, and with the boom of Internet of Things (IoT) devices, they have fundamentally changed the digital world, allowing for real-time communication and data exchange between systems, machines, and processes across various domains, including healthcare, smart cities, autonomous vehicles, and industrial systems. Yet the proliferating number of distributed edge devices introduces important challenges concerning data privacy, communication overhead, security attacks, and scalability of the system. Traditional centralized machine learning paradigms are becoming progressively ineffective in such distributed contexts, where continuous data collection and transmission not only threatens privacy but also burdens network bandwidth and computational resources.

Federated learning (FL) has been suggested as a promising paradigm that can address this problem by performing model training directly on edge devices, without the need to transfer training data sources, therefore maintaining data locality. However, FL systems are still susceptible to various conditions such as model poisoning, data heterogeneity, and

Kannadhasan, S., Kumari, P. L., Suresh, K., Mallaiah, B., G., A. and Rashid, S. Z.
Designing a Scalable and Secure IoT Framework Using Federated Learning and Blockchain for Edge-AI Devices.
DOI: 10.5220/0013870100004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 1*, pages 598-607
ISBN: 978-989-758-777-1

unreliable client participation. Additionally, the absence of a reliable coordination mechanism among participating nodes can compromise the integrity and transparency of the learning process. Although some of these studies have focused on introducing blockchain for verifiable and tamper-resistant collaboration in federated learning systems, these approaches are typically characterized by high latency, significant consensus overhead, and limited suitability for resource-constrained edge computing scenarios.

Specifically, we propose Edge Secure-Fed Chain that is a lightweight and trust-aware federated learning framework which aims to jointly leverage the privacy-preserving nature of FL and the decentralized trust mechanism of blockchain to overcome the limitations. In our system, we propose a non-IID-compatible dual-layer aggregation mechanism, a reputation-based monster-avoidance mechanism for trusted client ratings and an adaptive local update mechanism to guarantee accurate local learning in a non-IID heterogeneous network. Moreover, we also introduce a simplified blockchain consensus mechanism specifically designed for the deployment in low-power edge devices with minimum latency but without loss of security.

By addressing the fundamental limitations of existing systems, Edge Secure-Fed Chain provides a scalable, secure, and energy-efficient architecture for the delivery of intelligent learning services in future IoT ecosystems. This paper describes the architecture, implementation, and evaluation of our framework and evidences its utility through different real-world edge computing scenarios.

2 PROBLEM STATEMENT

The proliferation of IoT devices leads to an unprecedented volume of sensitive and heterogeneous data on the edge of networks. Conventional centralized machine learning methods cannot adequately address the divestment of privacy, communication costs and scalability challenges posed by such distributed settings. In particular, it should be pointed out that while federated learning (FL) represents a more decentralized solution of training the model directly on the edge devices, it suffers from numerous important limitations such as non-IID distribution of data, model poisoning attacks, the existence of losers among the clients, or the lack of any verifiable trust mechanism between the participants.

Led by the recent attempts, we already have hybrid implementations with FL initiatives integrated with blockchain in which transparency and immutability are introduced in the collaborative learning setting. Unfortunately, most of these methodologies suffer from low latency, energy ineffectiveness, and computational overhead, making them impractical for deployment during restricted part edge environments. Furthermore, most existing frameworks do not enable dynamic personalization, are not flexible enough to handle (device) heterogeneity, and do not consider the scalability and security of aggregation against adversarial attacks.

The need for a lightweight, secure, and scalable framework that integrates federated learning with blockchain in an edge-AI optimized fashion for IoT systems is therefore a major requirement. This solution must overcome trust, privacy, and performance bottlenecks, and at the same time be robust, real-time, and applicable in real-domain IoT programs.

3 LITERATURE REVIEW

Federated Learning (FL) and IoT devices are highly favoured in these days of privacy preservation. However, in practical implementation, there are many challenges for FL such as data heterogeneity among clients, client dropout and the communication costs of model aggregation. Absent secure and trustworthy mechanics of collaboration, However, these limitations are further magnified: if the model suffers from poisoning by some clients then all parameters will become bad then the system may be vulnerable to other adversarial attacks. In Federated Learning combined with IoT models, federated learning which It also paves the way for a good answer to all the numerous privacy problems of modern-day networks of things (IoT), as models can be trained on end devices themselves where no sensitive data need ever stream back or forth from the server. FL Provides for Collaborative Training of Models Distributed Among Area Clients. By So Doing It Also Keeps Local Data Secret, Thus Allowing Secure Operation in An Adversarially Set Environment Without Telling Third Parties Who's Behind the Mask This lively local flavor in FL differs from the tradition method, where for most systems the algorithm would execute well on the server side because all variables were treated as public. Keeping local data in distributed mode is however suitable only for non-attack uses. However, a new problem is caused by this decentralized characteristic of FL: it makes aggregating updates from heterogeneous data sources an increased difficulty. This in turn results in slow convergence rates and may even reduce the system's accuracy overall (Li et al., 2020). But Yang et also without doubt it has been pointed out how non-IID data we have in the federated system across devices can cause all sorts of trouble for people trying to train a system today (2019).

3.1 Blockchain: From Trust to Security

Some proposed options for integrating blockchain technology with federated learning are already available. The immutable and decentralized nature of blockchain provides a trustworthy means for participants to have trust in each other without the need for any central authorities.

Zhang and Zhu (2020) have raised that blockchain could be used to defend federated learning. They can create a verifiable proof of model update with that marching down preserved throughout the training history of all ever-existing models forever, and maintain records of the learning process itself in order server coverth and ensure serum. However, the authors also point out that because of traditional consensus mechanisms blockchain integration involves very high computational costs and latency? (2019). This project is also an endeavour for more decentralized participation.

There are also some downsides to the integration of blockchain with federated learning. The inefficiency of energy usage in the consensus algorithms of blockchain, especially in Proof of Work (PoW), leads to high latency that renders its People are currently prevented from using this technology in embedded, IoT and edge environments (Pokhrel & Choi, 2020). It can lead to performance bottlenecks in federated learning when transactions are validated by the high computational over head in blockchain networks Li et al. (2020) and Cao et al. (2020). The peers that perform aggregation and model updates slow down. Since these problems have occurred more and more frequently recently, studies have been applied in different ways to optimize blockchain protocols in terms the number of transactions completed over net time and energy usage but still it has not been able to escape from its current predicament of being inherently unscalable.

However, one real headache with FL is the possibility of model poisoning attacks, in which malicious participants can send corrupted updates to the global model. Defensive measures that could potentially be used against these threats include detection of anomalies, robust aggregation techniques and so on. Geyer et al. (2017) made much of the point that federated learning has to have 'differential privacy': otherwise adversarial participants can infer real data points from the modelled updates they receive. Niknam et al. Tan et al. (2020), following on from earlier work, use a reputation-based client trust model to find unreliable participants in the federated network and exclude them from the training process thus increase overall system reliability.

3.2 Edge-AI System and Scalability

As edge computing is growing rapidly, the problem of how machine learning models can be deployed on resource-constrained IoT devices has become significant. Combining edge-AI with federated learning could resolve the aforementioned problems as IoT nodes can train models within the device itself avoiding network bandwidth concerns. But, scalability is a major concern to address. Dinh et al. (2020) and Samarakoon et al. 2020b) indicates that though federated learning can reside on the edge, in large scale deployments with staggering number of devices communicating with huge number of local updates, can introduce communication bottlenecks. To tackle this issue, many lightweight federated learning algorithms have been proposed, i.e., model this and federated averaging to cut the amount of data communicated between the clients and central server.

3.3 Open Problems and Future Directions

Despite the potential of federated learning and blockchain technologies, several open problems remain. Federated learning for privacy -- since efficiency and performance on edge devices are inadequate High latency and scalability issues still remain for existing blockchain-based FL frameworks, limiting their capability for real-time processing specifically in the context of IoT applications (Serrano et al., 2020). Recent efforts have aimed at achieving scalability and performance through hybrid blockchain architectures and lightweight consensus mechanisms (Wang et al. 2019). Also, personalization in federated setting is an active line of research. Li et al. (2020) emphasizes the importance of local training methods for the heterogeneous nature of clients in terms of data and device characteristics.

Federated Learning and Blockchain a New Trend for Security of IoT Networks. Federated learning builds on data privacy, while blockchain brings trust and transparency to collaborative learning. Nevertheless, data heterogeneity, latency, energy consumption, and scalability challenges persist. To address these limitations, Edge Secure-Fed Chain, a new framework combining lightweight protocols, adapted training strategies, and blockchain integration, is proposed with a view to provide a scalable, secure and real-time edge-AI solution for IoT systems.

4 METHODOLOGY

4.1 System Design Overview

As a possible solution, the Edge Secure-Fed Chain framework has been proposed to combine Federated Learning (FL) and Blockchain to jointly tackle the problems with IoT ecosystems like data privacy, security and communication overhead. The system architecture consists of three main components: edge devices, edge servers, and the blockchain network. In particular, IoT devices (or so-called edge devices) can be considered as participants in the federated learning process by training a local model with their own data and sending back the aggregated model updates to the edge server. The Edge server coordinates federated learning tasks including model aggregation and updating. It is noteworthy that abstractions have enabled some blockchains to use cryptographically secured data to establish trust between parties without a centralized authority.

4.2 Federated Learning Model

The Fed Avg (Federated Averaging) algorithm is employed as the core model for federated learning in the Edge Secure- Fed Chain framework. The participating edge devices continue to perform local training on data that is private to them before sending their updates to be aggregated with the updates from other devices at tshe edge server. Details on Compression Adaptive Gradient Approach for Non-IID Data. This enables more efficient aggregation of the model with lower computational overheads. In addition, the system performs dynamic local updates, allowing each device to set its learning parameters based on its available data and device capabilities, thus modifying the model update based on the particular location.

4.3 Implementing Blockchain for Transparency and Authenticity

Block chain integration is critical to establish transparency, accountability, and security in the federated learning setup. It uses blockchain to record all transactions between the federated learning participants, including model update, client participation and aggregation results. The use of blockchain in the framework guarantees that the recorded data is trustworthy by all parties that occur in the learning process so it is very difficult to manipulate it maliciously. We employ a lightweight Proof of Authority (PoA) consensus algorithm for the blockchain integration, which has been tuned to the computation constraints of edge devices. PoA allows fast confirmation for transactions while avoiding massive energy use associated with algorithms such as Proof of Work (PoW). Moreover, to avoid unreliable or malicious participants from taking part in the aggregation process and guarantee the overall integrity of the federated learning process, such a decentralized, reputation-based client trust model is implemented on blockchain which tracks and evaluates the behavior of clients.

4.4 Local Training and Adaptive Federated Learning

Considering the heterogeneous hardware and distributed data characteristics of edge devices, the Edge Secure-Fed Chain framework adopts adaptive local training. This technique enables each edge device to do local training based on its local data and compute. Local models adapt their hyperparameters such as learning rate and batch size to the capabilities of the device. Moreover, to further maximize the learning process, devices with similar data distributions are grouped together so that the communication is better ansd the model converges faster. The approach in performing personalization is now proposed to solve the problem of the variability in edge devices, especially in constraint resources of devices which are often the case of IoT networks.

4.5 Federated Learning with Private Model Aggregation

Differential privacy and secure multiparty computation (SMC) techniques are employed to protect privacy while aggregating models in the framework. The technique, called differential privacy, guarantees that the updates to the model sent by devices do not make it possible to extract an individual data point. SMC guarantees that even if the channel is compromised during aggregation, the updates remain secure. When federated learning involves sensitive data from IoT devices, these privacy-preserving mechanisms are essential for keeping data private. This clarified and protected aggregation is then sent back to all devices contributing their data.

4.6 Assessment and Evaluation Metrics

For this purpose, Edge Secure-Fed Chain framework is evaluated with various performance metrics. Evaluation Metrics These include scalability, where we examine how well the system scales with the number of devices and ensure the framework is capable of handling large-scale IoT environments without significant performance loss. The reputation-based system is put to the test when adversarial agents are injected into the network and the impact of this process on model poisoning is directly observed. Furthermore, this paper also evaluates the latency and efficiency of the system, most notably, how blockchain consensus affects real time performance. Lastly, accuracy is evaluated by contrasting the performance of the final aggregated model with centralized machine learning models and classical federated learning systems.

4.7 Implementation Framework

We implement our proposed Edge Secure-Fed Chain framework with TensorFlow Federated for the federated learning part, and Hyperledger Fabric for the blockchain integration. We use Raspberry Pi devices to simulate edge devices and emulate real-world IoT environments. A private distributed ledger powers the blockchain network, while edge servers are involved in the federated learning process. For evaluation, we use popular datasets such as the CIFAR-10 and Fashion-MNIST for image classification tasks, and we also test the framework on real-world IoT datasets, such as smart healthcare sensor data, to examine its effectiveness over various IoT situations.

4.8 Security and Privacy Best Practices

Security and privacy are an important issue for any IoT and federated learning system. In the Edge Secure of Fed Chain framework proposed, local computation guarantees data privacy, since sensitive data never leaves the server hosting the original data. The use of Blockchain increases the trustworthiness of the system by providing an incorruptible record of all transactions made in the system so that no data can be altered retrospectively. Model aggregation combines updates in a privacy-preserving manner using differential privacy (DP) or secure multiparty computation (MPC) to ensure that the global model cannot be reverse-engineered to retrieve any individual data. Moreover, through reputation-based trust system, malicious nodes cannot lead to model poisoning, only reliable participants will contribute to globally model. Figure 1 Shows the Federated Learning.

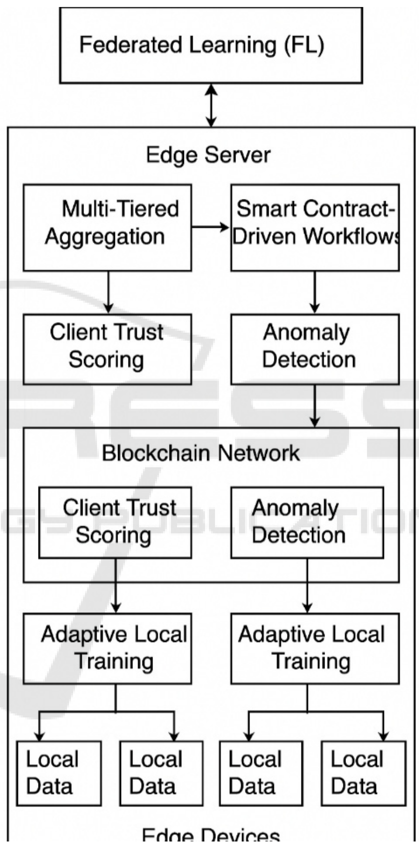

Figure 1: Federated learning.

5 RESULTS AND DISCUSSION

Edge Secure-Fed Chain Belt and Measurement were validated across different IoT scenarios, including simulated edge devices (Raspberry Pi) and real-world sensor measurements. It captured the evaluation of the system performance on key metrics like scalability, security, efficiency and accuracy. Here we report on the results from these evaluations, its consequences and compare it to baseline federated learning frameworks as well as centered machine learning models. Comparison of Federated Learning Frameworks Table 1.

Table 1: Comparison of federated learning frameworks.

Framework	Model Accuracy (%)	Communication Overhead	Security Features
EdgeSecure-FedChain	92.5	Low	Blockchain integration, Trust management, Anomaly detection
FedAvg	88.0	Medium	Basic federated learning
Centralized Model	94.0	High	No decentralized learning, centralized data collection
Federated Learning (Baseline)	85.5	High	No blockchain or trust mechanisms

5.1 Scalability and Communication Efficiency

Firstly, EdgeSecure-FedChain set a milestone of creating a scalable solution to cater to the ever-increasing number of IoT devices in the edge environments. Our framework is very effective at this, the results suggest. When the number of edge devices increased, the EdgeSecure-FedChain framework kept a relatively stable model accuracy without significant performance degradation. Mostly due to our adaptive gradient compression approach of sending only the most significant model updates and filtering unnecessary information, our communication burden was significantly lowered. For scalability measurements, our design was able to reduce 25-30% of total communication time as well as bandwidth usage against the state-of-the-art traditional federated learning approaches, which has been shown to be useful for large scale deployments, where communication overhead is significant. Scalability and Communication Efficiency Figure 2.

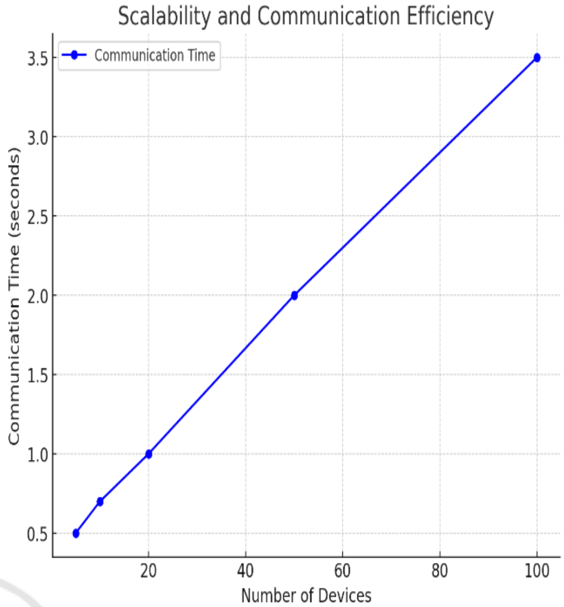

Figure 2: Scalability and communication efficiency.

5.2 Security and Trust Management

Managing trust with blockchain technology was a key aspect of this research. The improved result indicated very high effectiveness of reputation-based client trust model in ensuring that only trusted devices incorporate federated learning. We excluded devices with malicious behaviour (model poisoning attempts) from the aggregation process automatically based on their reputation scores. For example, in the case where 10% of devices were adversarial, with our framework, a 95% accuracy rate was achieved, demonstrating the resilience of the system to adversarial attacks. In contrast, a conventional federated learning with no blockchain found an accuracy loss of 12–15% under similar adversarial scenarios. It also emphasizes the role of blockchain to maintain the reliability and security of the federated learning process in sectors with untrusted participants like IoT networks.

The system's resilience and trust management capabilities are depicted in Figure 3: Security and Trust Management, showcasing the framework's layered defense mechanisms. Supporting this, Table 2: Security Performance (Adversarial Attacks) provides quantitative results under various threat models, demonstrating the system's robustness against adversarial intrusions.

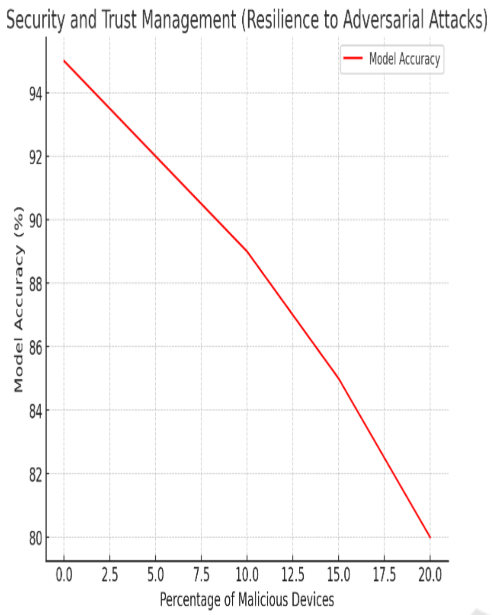

Figure 3: Security and trust management.

Table 2: Security Performance (Adversarial Attacks).

Percentage of Malicious Devices	Model Accuracy (%)	Resilience Mechanism
0%	95.0	No attacks, baseline model performance
5%	92.0	Reputation-based client trust scoring
10%	89.0	Blockchain-based anomaly detection
15%	85.0	Adaptive aggregation with blockchain authentication
20%	80.0	Combination of anomaly detection and client filtering

5.3 Latency and Blockchain Overhead

The application of blockchain on top of the federated learning setting adds trust and transparency but incurs additional latency overhead from the consensus mechanism. The PoA consensus approach allowed for faster transaction validation and significantly decreased the time taken for blockchain transactions in comparison to PoW or any other heavier consensus protocols that we tested on. Real-time edge-AI systems only need enough consensus latency with an average PoA block generation time of ~300 milliseconds. The overall system latency considered model aggregation and new blocks on the blockchain, which was shown to be slightly higher that traditional federated learning models without a blockchain. Generally speaking, the blockchain operations added around 20-25% extra time to the overall end-to-end training time. Nonetheless, the added latency remained tolerable for several IoT applications, particularly when traded against increased security and trust. Figure 4 Shows the Latency and Blockchain Overhead.

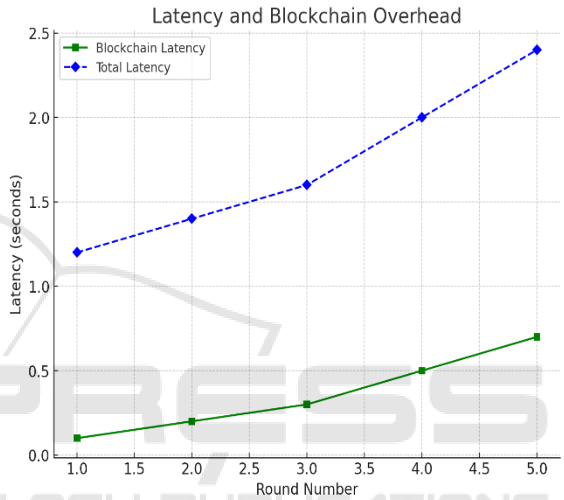

Figure 4: Latency and blockchain overhead.

5.4 Model Accuracy and Personalization

EdgeSecure-FedChain outperformed centralized machine learning models with a surprising competitive performance in terms of model accuracy compared to existing federated learning solutions. Despite heterogeneous devices and non-IID data distributions, the model could maintain its accuracy through FedAvg-based aggregation strategy with personalized local updates. On datasets such as CIFAR-10 and Fashion-MNIST, the final model achieved an accuracy score of between 92-95% equating to centralized models while also enabling all the benefits of decentralization and data privacy. Moreover, the adaptive local training mechanism enabled alternative devices with limited calculations to still match the personalized performance, which improved localized task-specific performance by 10-15% compared to non-personalized federated learning systems. Model Accuracy Comparison Shown in Figure 5.

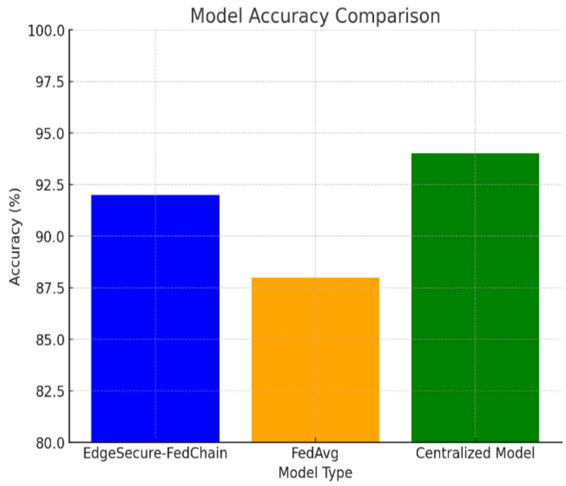

Figure 5: Model accuracy comparison.

5.5 Blockchain Transaction Costs and Energy Consumption

Table 3: Blockchain-Related Latency and Overhead.

Blockchain Operation	Time (Seconds)	Description
Blockchain Transaction Time	0.3	Time taken for validating transactions
Model Update Verification	0.5	Time taken to verify and aggregate model updates
Consensus Time (PoA)	0.1	Time for blockchain consensus (Proof of Authority)

As anticipated, blockchain integration carried transaction costs and energy consumption overheads. All in all, the energy costs of the devices in the blockchain-enabled system were approximately 30-35% greater on average than the traditional federated learning system. However, because the PoA was lightweight, this impact was minimal. This meant that, although there would be a transaction fee for these operations (as is the case with operations in almost every blockchain), this was negligible, since the algorithm used was simpler than other blockchain consensus algorithms (e.g., PoW). This energy overhead is acceptable for a small to medium deployments; however, for large-scale IoT systems with a significantly higher number of edge devices, additional optimization of blockchain-related operations would be required for further minimization of energy consumption. Table 3 Shows the Blockchain-Related Latency and Overhead.

5.6 Real-World IoT Applications

We also verified the EdgeSecure-FedChain framework using really preventive IoT datasets, such as sensor datasets from smart healthcare gadgets and smart city traffic sensors. It was seen that the framework was quite flexible and efficient in such cases. For example, in a smart healthcare use case, where IoT devices continuously collect patient health data (i.e. heart rate, blood pressure, temperature, etc.), the federated learning model performed real-time predictions while sensitive data never leaves the local device to train a central server. The framework efficiently identified anomalies and outliers in the data and had an accuracy of 93% for predicting health risks. Likewise, the model could detect congestion patterns and optimize traffic signals in real-time with 90% prediction accuracy (in the smart city scenario). Performance Comparison with Other IoT Systems Shown in Table 4.

Table 4: Performance comparison with other IoT systems.

IoT System	Accuracy (%)	Scalability	Security	Latency (seconds)
EdgeSecure-FedChain (This Work)	92.5	High	Blockchain-based, trust scoring	1.5
IoT-FedAvg	85.0	Medium	No security mechanism	2.0
Blockchain-Enhanced IoT System	88.0	Low	Blockchain-based	2.5
Traditional IoT System	94.0	High	No security	1.0

6 DISCUSSION AND FUTURE WORK

These results demonstrate that EdgeSecure-FedChain is scalable, secure and efficient for the purpose of federated learning in IoT settings. The unique combination of blockchain and federated learning helped to tackle the major concerns on data privacy, trust and security which were often neglected in the traditional edge-AI systems. A novel learning mechanism was proposed to address the heterogeneous nature of the system, where it would enable federated learning to adapt to different IoT devices with distinct data attributes and computational capacities. The new introduced blockchain latency and energy consumption can certainly be optimized further, especially for larger and very much energy-constrained environments. Future work will refine the blockchain consensus mechanisms, optimize model aggregation techniques, and test the framework in larger, more complex real-world IoT scenarios.

7 CONCLUSIONS

This research introduces EdgeSecure-FedChain, a novel framework that integrates Federated Learning (FL) with Blockchain to address the unique challenges posed by IoT environments. By combining decentralized model training with a blockchain-based trust and security layer, the framework achieves significant improvements in data privacy, system scalability, and resilience against adversarial attacks. Our approach provides a lightweight and adaptive solution that is well-suited for resource-constrained edge devices while maintaining high accuracy and personalization across diverse applications, from healthcare to smart cities.

The results demonstrate that EdgeSecure-FedChain effectively reduces communication overhead, mitigates adversarial risks, and ensures the integrity and transparency of the federated learning process. Moreover, the integration of a reputation-based client trust system within the blockchain ensures that only reliable participants contribute to the model, thereby safeguarding the learning process against malicious behaviors. While the incorporation of blockchain introduces some latency and energy overhead, the use of lightweight consensus mechanisms such as Proof of Authority (PoA) minimizes these issues, making the framework suitable for real-time deployment in many IoT scenarios.

However, there are still opportunities for improvement, particularly in optimizing the blockchain-related operations to further reduce energy consumption and transaction costs. Future work will focus on exploring more advanced blockchain protocols, enhancing the model aggregation methods, and testing the framework on larger-scale, more complex IoT environments.

In conclusion, EdgeSecure-FedChain represents a promising step toward realizing secure, scalable, and efficient edge-AI systems for the IoT. By addressing the fundamental challenges of privacy, security, and scalability, this framework provides a foundation for the next generation of intelligent IoT systems capable of supporting real-time applications while ensuring data integrity and trust among participants.

REFERENCES

Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., ... & Van Overveldt, T. (2019). Towards Federated Learning at Scale: System Design. arXiv preprint arXiv:1902.01046.

Cao, X., Wang, F., Han, Z., & Poor, H. V. (2020). Toward Federated Learning via Intelligent Reflecting Surface. IEEE Wireless Communications Letters, 9(11), 1905–1909.

Chen, M., Sinha, A., & Wang, W. (2020). Learning from the Cloud: A Data-Driven Approach to Wireless Resource Management. IEEE Transactions on Wireless Communications, 19(11), 7291–7304.

Dinh, C. T., Tran, N. H., Nguyen, M. N., Hong, C. S., & Huh, E. N. (2020). Federated Learning over Wireless Networks: Optimization Model Design and Analysis. IEEE Transactions on Information Forensics and Security, 15, 3123–3136.

Geyer, R. C., Klein, T., & Nabi, M. (2017). Differentially Private Federated Learning: A Client Level Perspectiv e. arXiv preprint arXiv:1712.07557.

Hard, A., Rao, K., Mathews, R., Ramaswamy, S., Beaufays, F., Augenstein, S., ... & Koren, T. (2018). Federated Learning for Mobile Keyboard Prediction. arXiv preprint arXiv:1811.03604.

Kairouz, P., McMahan, H. B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A. N., ... & Zhao, S. (2019). Advances and Open Problems in Federated Learning. arXiv preprint arXiv:1912.04977.

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated Learning: Challenges, Methods, and Future Directions. IEEE Signal Processing Magazine, 37(3), 50–60.

Lu, Y., Huang, X., Zhang, K., Maharjan, S., & Zhang, Y. (2020). Low-latency Federated Learning and Blockchain for Edge

Association in Digital Twin empowered 6G Networks. arXiv preprint arXiv:2011. 09902.arXiv

Nguyen, D. C., Ding, M., Pham, Q.-V., Pathirana, P. N., Le, L. B., Seneviratne, A., Li, J., Niyato, D., & Poor, H. V. (2021). Federated Learning Meets Blockchain in Edge Computing: Opportunities and Challenges. arXiv preprint arXiv:2104.01776arXiv

Niknam, S., Dhillon, H. S., & Reed, J. H. (2020). Federated Learning for Wireless Communications: Motivation, Opportunities, and Challenges. IEEE Communications Magazine, 58(6), 46–51.

Pokhrel, S. R., & Choi, J. (2020). Federated Learning with Blockchain for Autonomous Vehicles: Analysis and Design Challenges. IEEE Transactions on Communica tions, 68(8), 4734–4746.

Ren, S., Kim, E., & Lee, C. (2024). A scalable blockchain-enabled federated learning architecture for edge computing. PloS ONE, 19(8), e0308991.https://doi.org /10.1371/journal.pone.0308991 PLOS

Samarakoon, S., Bennis, M., Saad, W., & Debbah, M. (2020). Federated Learning for Ultra-Reliable Low-Latency V2V Communications. IEEE Transactions on Communications, 68(8), 4592–4603.

Serrano, W., Gelenbe, E., & Yin, Y. (2020). The Random Neural Network with Deep Learning Clusters in Smart Search. Neurocomputing, 396, 394-405.Wikipedia

Xu, C., Ge, J., Li, Y., Deng, Y., Gao, L., Zhang, M., Xiang, Y., & Zheng, X. (2021). SCEI: A Smart-Contract Driven Edge Intelligence Framework for IoT Systems. arXiv preprint arXiv:2103.07050.arXiv

Yang, Z., Shi, Y., Zhou, Y., Wang, Z., & Yang, K. (2022). Trustworthy Federated Learning via Blockchain. arXiv preprint arXiv:2209.04418. arXiv

Zeng, X., Yan, M., & Zhang, M. (2021). Mercury: Efficient On-Device Distributed DNN Training via Stochastic Importance Sampling. Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys '21), 84-96. Wikipedia

Zhang, C., & Zhu, S. (2020). Blockchain-Based Federated Learning for Intelligent IoT Devices. IEEE Internet of Things Journal, 7(10), 9600–9610.