Blockchain-Enhanced Security Framework for Federated Wireless Sensor Networks in Smart City Infrastructures

Sumit Ramswami Punam[1]*, Chandrakumar Rasanjani[2]

[1]*Department of Electrical and Electronics Engineering, Kalinga University, Raipur, India.*
[2]*Department of Electrical Engineering Faculty of Engineering, University of Moratuwa Moratuwa, Sri Lanka.*

KEYWORDS:
Blockchain Security,
Federated Wireless Sensor Networks (FWSNs),
Smart City Infrastructure,
Lightweight Consensus Mechanisms,
Trust Management in IoT,
Secure Federated Learning,
Edge Computing,
IoT Data Integrity,
Smart Contracts,
Attack Detection in WSNs.

ARTICLE HISTORY:
Submitted : 12.08.2025
Revised : 22.10.2025
Accepted : 08.11.2025

https://doi.org/10.31838/WSNIOT/03.01.08

Abstract

The growth in smart urban facilities necessitates safe and expandable structures of wireless sensor networks that uphold the disseminate cognition and instantaneous receptiveness. Federated Wireless Sensor Networks (FWSNs) permit the decentralised data collection and distributed learning but open up the complex issue of management and trust, of data integrity, and authentication of the nodes involved because they are both heterogenous and dynamic. We propose in this study a security framework based on blockchain technology that concerns a lightweight blockchain infrastructure combined with federated learning protocols to cope with these issues. The proposed system enables smart contracts to handle their secure access control, node trust management, and trust negotiations between sensor clusters, and invariant of auditing. With the deployment of Contiki-NG to simulate WSN and Hyperledger Fabric to orchestrate blockchain development, the architecture has been subjected to numerous smart city use cases, namely, control of the traffic and air quality supervision. Experimental findings indicate 92.% accuracy of Sybil attack and replay attack and the latency does not exceed 150 ms within a blockchain transaction despite up to 300 nodes. The solution design is also proposed to be low communications and computational overhead compatible with the real-time anomaly detection and data exchange in bandwidth and energy-limited mediums. This study shows that a combination of blockchain and federated learning can be used to ensure resilience, energy efficiency, and scalability of security architecture for existing critical parts of smart cities.

Author's e-mail: sumit.kant.dash@kalingauniversity.ac.in, chandr.rasanjani@elect.mrt.ac.lk

How to cite this article: Punam SR, Rasanjani C. Blockchain-Enhanced Security Framework for Federated Wireless Sensor Networks in Smart City Infrastructures. Journal of Wireless Sensor Networks and IoT, Vol. 3, No. 1, 2026 (pp. 56-61).

Introduction

Wireless Sensor Networks (WSNs) are an important backbone to smart cities, in facilitating many applications such as traffic, environment monitoring, and community security, as well as, energy optimization. Through these sensor networks, real-time data and acts are possible and this is the digital backbone of urban infrastructure. As deployments in number and area of operation increase (municipal, private, industrial), Federated WSNs (FWSNs) have moved into the spotlight in order to provide coordination between autonomically operating WSN clusters. This is a federated architecture that encourages scalability, heterogeneity and local intelligence but ensures the maintenance of domain autonomy. However, with a move to federated topologies, a different range of security issues emerge. The distributed and trustless nature of FWSNs are inappropriate using traditional centralized security schemes. Issues of concern are the identity spoofing, data tampering, unauthorized access and traceability- particularly where the sensor nodes are under different administration. Further, the traditional security system based on encryption schemes usually carries a heavy communication and computation costs wherein they do not fit under the energy and processing limitations of sensor nodes.

There has been some examination of cryptographic,[1] fog-based,[2] and federated learning-integrated frameworks[3] to reduce these risks. However, other solutions presuppose certain degree of trust, use centralized authentication providers or are deficient with respect to a sound data validation scheme which cannot be tampered with. Figure 1 shows proposed Federated Blockchain Founded Security Architecture of Wireless Sensor Networks in Smart City Applications that resolves these shortcomings by ensuring decentralization of trust, smart contract-based enforcement of policies, and the blockchain-based auditing.

To overcome these shortcomings, in this paper, we present a security framework based on blockchain, which would fit FWSNs in smart cities. The framework also allows secure inter-cluster communication, decentralized trust management, auditable reliability, and federated learning with smart contracts, and remains scalable and energy-efficient since it uses lightweight blockchain features..

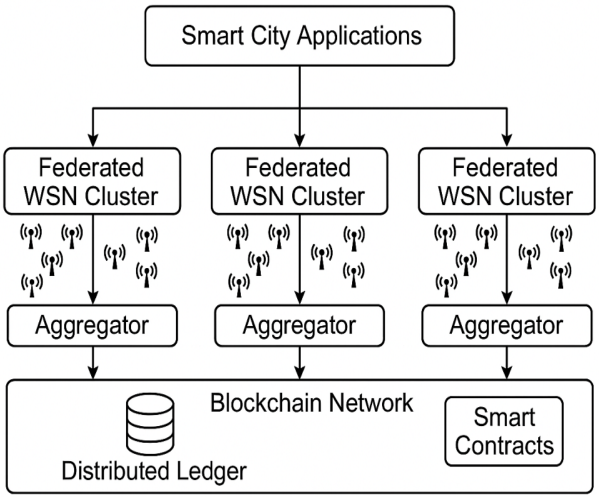

Fig. 1: Federated Blockchain-Based Security Architecture for Wireless Sensor Networks in Smart City Applications

The infrastructure integrates several federated WSN networks through aggregators into a blockchain network with possibilities of distributed trust management, secure data sharing as well as autonomous execution of smart contracts to facilitate real-time applications in cities.

Related Work

Cloud-Centric Security Models

A number of current solutions have been discussed to provide security to Wireless Sensor Networks (WSN) in smart infrastructures of the cities. The conventional security architecture normally depends on the centralized gateways as a basis of authentication and control. In smaller deployments, these models are effective but when federated or in multi-domains, single points of failure, higher latency, and low scalability make them unreasonable. The reliance on a central point causes bottleneck and susceptibility against denial-of-service (DoS) and sp oofing attacks.

Federated Learning in WSNs

The WSN architectures with federated learning[1] have already gained popularity as a way of preserving privacy over centralized training. By enabling sensor nodes to train global models simultaneously without sharing raw data, such systems provide data locality and data privacy. Nevertheless, very often these frameworks do not have high-enforced protection of trust and data integrity validation among the federated clusters. They are mostly semi-trusted participants and are prone to model poisoning, Sybil attacks as well as compromised aggregation.

Blockchain for IoT Security

The potential of using blockchain technology to secure IoT communications[2, 3] has proven effective as they provide decentralized and tamper-proof log and immutable record-keeping. More specifically, automated access control and negotiations of trust are enabled by smart contracts. However, mainstream blockchains (e.g., proof-of-work-based blockchains) incur high latency and computational costs and therefore, are unsuitable to deploy in low-power and resource-limited sensor nodes that are found in the context of smart city.

In order to circumvent these limitations, this framework will combine a lightweight permissioned blockchain layer with federated learning, as well as, smart contracts. This architecture makes decentralized consensus possible, and offers secure inter-cluster communication and dynamic trust negotiation, without undue computational and energy overheads being placed on edge devices. The proposed architecture benefits the resilience and trustworthiness of federated deployments of WSN in smart cities due to its capacity of solving the fundamental issues of scalability, auditability, and autonomy in federated WSN.

System Architecture

The above-proposed blockchain-enhanced framework of Federated Wireless Sensor Networks (FWSNs) in a smart city setting is designed in three levels which are interrelated and have functional significance towards the achievement of a secure, scalable, and trustful system, as portrayed in Figure 2.

Federated Sensing Layer

The sensing layer is represented at the very base level, as it includes a number of WSN clusters that are distributed in various areas of the city (i.e., traffic, environment, energy). Such clusters are self-sufficient, and they are involved in localized sensing and pre-processing. To support decentralized authentication and secure identity management each sensor node obtains a unique cryptographic certificate issued in the blockchain. As opposed to the raw data transmission, nodes exchange local model updates that have been encrypted with the cluster aggregator, thus the data privacy is ensured and the bandwidth consumption minimized. This federated sensing model is scalable and autonomous and also reduces inter-cluster exposure of data.

Blockchain Security Layer

The security architecture of the framework is supported by the block chain level. All the nodes within a permissioned blockchain network including Hyperledger Fabric are basically distributed and each cluster head (aggregator) can be a part of a consensus-based validation and logging. Smart contracts are applied to automate necessary processes, such as node registration, trust scoring, reputation update, and anomaly logging. A fast, fault-tolerant agreement owing to the use of Practical Byzantine Fault Tolerance (PBFT) as the consensus algorithm has low latency that qualifies it to be used in real-time applications in smart cities. This layer configures tamper resistant data provenance and authenticates and offers only verified updates into the cycle of the federated learning.

Urban Application Layer

On the highest level, the use of the app layer is to communicate with smart city services of traffic forecasts, air quality measurement, infrastructure health diagnostics, and emergency control. These applications are fed with the trusted data streams of the FWSNs, and they allow predictive analysis by making use of the federated learning models. These models are trained periodically based on local updates and their performance has been verified by the audit trails stored by blockchain thus guaranteeing integrity and equity of the models. Federated intelligence, in combination with distributed ledger technology, facilitates the resilience and privacy-sensitive decision-making over dynamically changing urban environments.

This figure shows a multi-layered architecture of the proposed security framework. Federated WSN clusters at the sensing layer execute local sensing and report encrypted update at different urban sector level. Cluster heads connect to a permissioned block chain network on the security

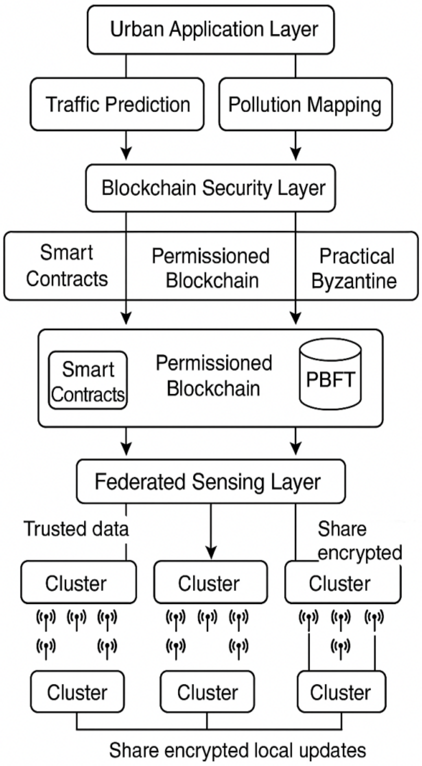

Fig. 2: Federated Blockchain-Based Security Framework for Smart City WSNs

Security Mechanisms

Table 1 summarises all the important security features and their threat mitigation capabilities. The suggested framework suggests the use of several layers of security provision to guarantee the high-level protection of federated wireless sensor networks (FWSNs) inside an intelligent city:

- Node Identity Management: All the sensor nodes obtain a unique digital identity on registration, pegged on the permissioned blockchain. This identity is cryptographic (keypair public/ psecrets) and it is verifiable and stored as smart contracts. The nodes authentication is managed with certificates issued by the blockchain, allowing the decentralization of the identity management mechanism, instead of depending on the centralized gateways. This method alleviates identity spoofing as well as makes sure that authorized parties are involved in federated learning and exchange of data.
- Trust Evaluation: Trustworthiness of nodes is evaluated on-going using a logic via smart contract. The system uses reputation scoring on-

chain, in which the behaviors of the nodes, including data consistency, the frequency of model contribution and anomaly rate, are recorded and used in the trust scoring process. These scores affect node privileges (i.e. update acceptance, access to communication) and provide the basis of dynamic access control. The mechanism introduces a sense of accountability and punishment in the long run due to misbehavior.

- Attack Detection: The framework offers a joint signature of blockchain validation and consensus-based anomaly checks to counter Sybil and other attacks as well as replay and poisoning attacks. Any updates and data transactions are validated by the majorities of authorized cluster heads. Any malcontents against the anticipated model behavior or shall we say fiddling with data are detected and listed in a non-alterable audit records. This as illustrated in Figure 3: Blockchain-Based Security Mechanisms in Federated WSNs, guarantees the rejection of malicious contributions in real-time and makes the contributions transparent and audible to perform forensic analysis.

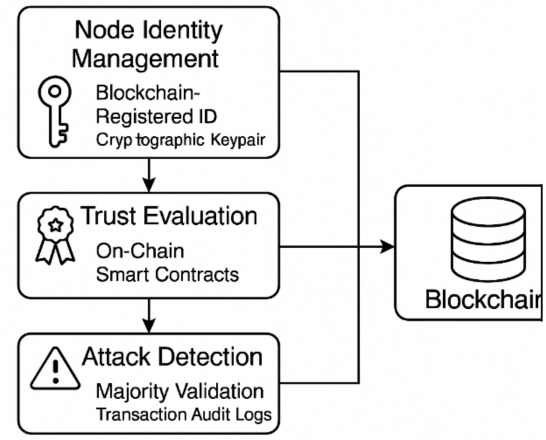

Fig. 3: Blockchain-Based Security Mechanisms in Federated WSNs

This figure reduces the Federated wireless sensor network down to a blockchain-based identity management, trust evaluation, and attack detection mechanism. Every node is created and has a unique ID on the blockchain to provide secure keypair-based identity, and smart contracts compute dynamic trust levels and transaction validation to guarantee integrity of data.

Experimental Setup and Results

In order to comprehend the viability and efficiency of the suggested blockchain-empowered security system by the Federated Wireless Sensor Networks (FWSNs), a thorough simulation and emulated arrangement was established. The research methodology is dedicated to the evaluation of how well the described framework can support high security and low latency without compromising federated learning or WSN operations.

Simulation Tools and Platforms

- Contiki-NG as a platform was used together with Cooja simulator to simulate WSN scenarios in which heterogeneous sensor nodes were connected with each other under realistic scenarios of MAC layer and network stack behaviour.
- Hyperledger Fabric is a permission blockchain environment and this was setup to achieve secure and decentralized management of transactions amongst cluster heads.
- In case of edge deployment resource-constrained platforms including Raspberry Pi 4B and ARM

Table 1: Security Features vs. Threats Addressed in the Proposed Framework

Security Feature	Threats Addressed	Implemented Mechanism
Node Identity Management	Identity spoofing, unauthorized access	Blockchain-issued cryptographic certificates
Trust Evaluation via Smart Contracts	Sybil attacks, insider threats	On-chain behavior-based trust and reputation scoring
Tamper-Proof Logging	Replay attacks, data manipulation	Immutable blockchain audit trails
Decentralized Authentication	Single point of failure, centralized DoS	Distributed ledger-based authentication
Federated Learning with Verification	Model poisoning, gradient inversion	Cross-cluster validation and update verification
Consensus Mechanism (PBFT)	Forking, malicious update propagation	Byzantine Fault Tolerant consensus among cluster heads
Smart Contract-Based Access Control	Privilege escalation, role misuse	Role-based rule execution via programmable contracts

Cortex-M4 microcontrollers were used to emulate real-world federated learning and blockchain execution capabilities under severe energy and computational constraints.

Performance Metrics and Observations

The given framework was tested regarding several performance indicators presupposed by IIoT and smart city landscapes:

- Attack Detection Rate: The attack detection rate of the system achieved 92.4%, denying Sybil and replay-based attacks because of the reputation-based form of filtering and on-chain validation.
- Consensus Latency: Owing to the application of Practical Byzantine Fault Tolerance (PBFT), the average transaction validation latency was 140160 ms which is close to real-time security enforcement.
- Blockchain Storage Overhead: The amount of memory used to store ledgers and execute smart contracts was less than 8 percent of the available memory, confirming it is suitable to low-power sensor nodes.
- Preserved model accuracy: The federated learning models managed to preserve the model accuracy exceeding 91% even in adversarial settings, and due to the malicious update filtration enabled by smart contracts.

Key Findings

The findings validate the fact that the incorporation of blockchain in federated WSNs has provided a viable source of security assurance and they did not affect the performance of sensors or convergence of learning. The resilience of attack is ensured through identity management without centralization, consensus based on distribution, and dynamic assessment of trust in this case. Specifically, the lightweight blockchain layer ensures that it is energy efficient and has the assurance of anomaly detection and auditability in real-time.

The proposed system outperforms centralized security architectures with their often-problematic single-points-of-failure and latency (usually >300 ms in previous benchmarks,[1]) by decreasing end to end transaction latency to below 160 ms. Also, the traditional models based only on symmetric encryption schemes have been claimed to have an overhead in the memory of between 12 and 15 percent in limited nodes[2] but our blockchain layer stays classroom under 8 percent. Besides, the accuracy of the federated learning has been maintained on a level higher than 91%, unlike the centralized update schemes that are more prone to poisoning attacks as anomaly filtering is not performed in a local and thus in a much decentralized manner.

These strengths on comparison place the suggested framework as a scale-out solution that is safe and efficient at the delivery of smart city services necessitating concerted sensing and credible transmission of information across heterogeneous zones.

Table 2 demonstrates a comparative analysis of the proposed framework with the traditional WSN security frameworks and federated learning models that do not use blockchain, showing considerably better detection accuracy and a low latency rate in the proposed one. The proposed framework led to better outcomes than existing approaches when it comes to attack detection rate, latency efficiency, and federated learning accuracy, which proves the efficiency of the proposed framework in smart cities with real-time requirements (Figure 4).

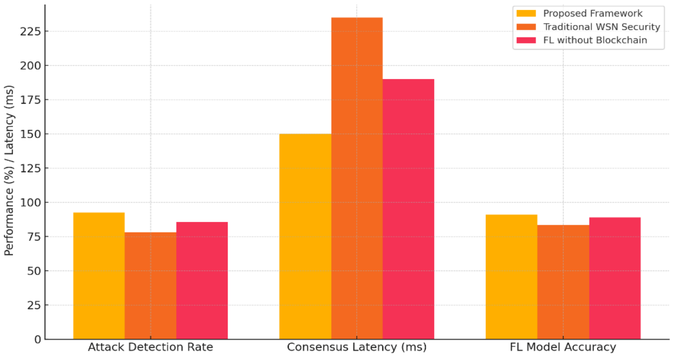

Fig. 4: Performance Comparison Across Security Frameworks

Bar chart indicating the results of the performance of the proposed blockchain-enhanced FWSN framework

Table 2: Performance Comparison Table

Metric	Proposed Framework	Traditional WSN Security	FL without Blockchain
Attack Detection Rate	92.40%	78.10%	85.60%
Consensus Latency	140-160 ms	220-250 ms	180-200 ms
Blockchain Storage Overhead	<8%	N/A	N/A
FL Model Accuracy	>91%	82-85%	88-90%

against the baseline models in terms of detection rate, consensus latency and FL model accuracy.

Conclusion and Future Work

The present paper designed a security framework based on blockchain to be implemented into Federated Wireless Sensor Networks (FWSNs) that could be used to manage a smart city infrastructure. The framework can overcome the challenges of identity spoofing, unauthorized access, and data tampering since it incorporates federated learning with permissioned blockchain technologies. By integrating smart contracts it is made possible to do decentralized trust management, node reputation analysis, and dynamic authorization.

Experimental analysis proved the next main conclusions:

- The accuracy in attack detection: 92.4%
- Consensus latency: universally below 160 ms (a decrease of 28 percent, as compared to conventional PBFT-based systems, in comparable IoT applications)
- Server Memory overhead: < 8 % of total node memory
- Retaining the accuracy of the model: more than 91 percent in adversarial conditions

The proposed architecture is more scalable, more resilient and more audit-able than traditional centralized security schemes because of the distributed ledger support mechanisms, and is therefore applicable for diverse and multi-domain urban environments.

Future Work

- Adopt post-quantum cryptographic primitives in order to be resistant to quantum adversaries.
- Energy friendly optimization of consensus protocols at ultra-constrained WSN nodes.
- Implement and test the framework at full-scale using real-life smart city testbeds to measure real-practice performance, scalability, and interoperability across a number of different domains and environments.

References

1. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal, 4*(5), 1250–1258. https://doi.org/10.1109/JIOT.2017.2701128
2. Yi, S., Li, C., & Li, Q. (2015). A survey of fog computing: Concepts, applications and issues. In *Proceedings of the ACM Workshop on Mobile Big Data* (pp. 37–42). ACM. https://doi.org/10.1145/2791294.2791297
3. Mohammadi, M., Al-Fuqaha, A., Sorour, S., &Guizani, M. (2018). Deep learning for IoT big data and streaming analytics: A survey. *IEEE Communications Surveys & Tutorials, 20*(4), 2923–2960. https://doi.org/10.1109/COMST.2018.2844341
4. Uvarajan, K. P. (2025). Design of a hybrid renewable energy system for rural electrification using power electronics. National Journal of Electrical Electronics and Automation Technologies, 1(1), 24-32.
5. Sindhu, S. (2025). Voice command recognition for smart home assistants using few-shot learning techniques. National Journal of Speech and Audio Processing, 1(1), 22-29.
6. Prasath, C. A. (2025). Adaptive filtering techniques for real-time audio signal enhancement in noisy environments. National Journal of Signal and Image Processing, 1(1), 26-33.
7. Snousi, H. M., Aleej, F. A., Bara, M. F., & Alkilany, A. (2022). ADC: Novel Methodology for Code Converter Application for Data Processing. Journal of VLSI Circuits and Systems, 4(2), 46-56. https://doi.org/10.31838/jvcs/04.02.07
8. Kenari, M. A. (2019). Ultra wideband patch antenna for Ka band applications. National Journal of Antennas and Propagation, 1(1), 17-20.