S.A. Jilani et al., Vol 1(1), pp 17-25
https://doi.org/10.55306/CJAMC.2026.010103
e-ISSN: XXXX.XXXX
Ci-STEM Journal of Advanced Materials and Computing

Secure Post-Quantum Cryptographic Framework Using Hybrid Lattice-Based KEM and Adaptive Federated Learning for Smart City Cyber-Infrastructure

Sayamuddin Ahmed Jilani
Department of Computer Science & Engineering, Maulana Abul Kalam Azad University, West Bengal, India.
email: 1075sam@gmail.com

Soumitra Kumar Mandal
Department of Electrical Engineering
National Institute of Technical Teachers Training and Research, Kolkata, India.
email: skmandal@nitttrkol.ac.in

Open Access
Research Article

Received : 08/12/2025
Accepted : 04/02/2026
Published : 04/03/2026

Corresponding author email:
1075sam@gmail.com

Citation:
S.A. Jilani et al., "Secure Post-Quantum Cryptographic Framework Using Hybrid Lattice-Based KEM and Adaptive Federated Learning for Smart City Cyber-Infrastructure" Ci-STEM Journal of Advanced Materials and Computing, Vol. 1(1), pp. 17-25, 2026.
doi: 10.55306/CJAMC.2026.010103

Published By:
Ci-STEM Global Services Foundation, India.

Abstract:
The intensive development of smart city cyber-infrastructure has aggravated the security issues because of the heterogeneity of devices, the volume of constantly changing data, and the lack of confidentiality in the long term. Traditional public-key cryptographic systems like RSA and ECC are becoming susceptible to quantum-powered attacks and are inappropriate to use in smart city applications in the future. Despite their quantum resistance, post-quantum cryptographic (PQC) schemes are not widely used in practice due to high computational cost, difficulty in key management, and inflexibility to dynamic cyber-threats. Furthermore, the current security systems do not tend to be decentralized, but the sources of intelligence are usually centralized which creates issues of privacy and scalability. This paper mitigates these shortages by suggesting a safe post-quantum architecture that incorporates an adjustable federated learning architecture and a hybridized lattice-based Key Encapsulation Mechanism to smart city cyber-infrastructure. The KEM based on lattice provides resistant to quantum key exchange, whereas federated learning provides decentralized threat intelligence without sensitive local information disclosure. An adaptive aggregation approach dynamically scales model updates based on node reliability and threat intensity, improving resilience to poisoning and inference attacks. Benchmark post-quantum parameters and public intrusion datasets, such as UNSW-NB15 and CICIDS2017 are tested in the framework in a simulated smart city setting. The experimental findings indicate a maximum common exchange latency reduction of 21 percent, versus standalone lattice schemes, and a threat detection rate of 97.8 percent with stable convergence. The results have shown the efficiency of integrating post-quantum cryptography with adaptive federated intelligence in ensuring the security of the next generation smart city infrastructures.
Keywords: *Federated Learning, Lattice-Based KEM, Post-Quantum Cryptography, Quantum-Resistant Cyber-Infrastructure, Smart City Security.*

1. INTRODUCTION

Smart cities will be based on highly intertwined cyber-infrastructures to justify important services including intelligent transportation, smart grids, healthcare monitoring, and public safety systems. Those environments are required to work in the condition of high security standards as data are sensitive over the long term, and cyber-attacks are becoming more sophisticated. With the advent of quantum computing, there is a fundamental threat to current cryptography principles, as broadly used public-key encryption schemes cease to be computationally viable against quantum attackers. This is a major risk to the smart city implementations, where the encrypted data may need to be secured throughout the long-term lifecycles. More recent studies have investigated post-quantum cryptographic primitives, particularly lattice-based, to provide quantum resistance.

Nevertheless, the majority of current solutions are mostly concerned with the cryptographic power, but they do not pay much attention to the system-level issues like scalability, adaptive response to threats, and preservation of privacy in distributed systems. In addition, centralised security intelligence models also create single points of failure and pose serious data privacy issues, which restricts their applicability in the context of large-scale smart city ecosystems.

The gap in the research is the lack of the integrated framework to unite quantum-resistant cryptographic protection and intelligent and privacy-preserving and adaptive security learning specific to smart city cyber-infrastructure. Literature only discusses cryptographic resilience without adaptive intelligence or suggests learning-based intrusion detection systems without taking post-quantum security constraints into account.

A new hybrid framework that fills this gap is presented in this paper and involves a lattice-based Key Encapsulation Mechanism with adaptive federated learning. The suggested solution guarantees quantum-resistant secure communication and allows decentralized and privacy conscious cyber-threat intelligence among nodes in the smart city.

The main contributions of this work are summarized as follows:

- A hybrid post-quantum security framework that integrates lattice-based KEM with adaptive federated learning for smart city environments.
- An adaptive federated aggregation mechanism that improves robustness against unreliable and malicious nodes.
- A system-level evaluation demonstrating improved security efficiency, reduced cryptographic latency, and high threat detection accuracy.
- A comprehensive experimental analysis using benchmark intrusion datasets and realistic smart city simulation settings.

The rest of this paper is structured in the following way. Section 2 conducts a literature review on post-quantum cryptography and federated security learning. Section 3 includes the description of the intended hybrid framework and its main components. Section 4 includes the experimental set-up, datasets and performance evaluation. The results and implications are discussed in Section 5, and the paper is concluded with the research directions available in the future in Section 6.

2. RELATED WORKS

Recent surveys assess in detail lattice-based constructions and their application to post-quantum deployment, including the algorithmic basis, implementation trade-offs, and open engineering concerns of the real-world system. The synthesis emphasizes the role of system-level assessments in the integration of lattice schemes within distributed infrastructures [1].

The research on federated learning in the IoT security field has shown that a decentralized model-training can retain the local privacy and allow the intrusion detection to be collaborative. These papers address the communication overheads, local resource constraints, and privacyutility tradeoffs unique to heterogeneous IoT nodes, and lightweight aggregation and compression schemes are suggested to support constrained devices [2].

Interest and privacy-saving aggregation protocols of federated learning solve integrity and accountability issues of joint model updates. Constructions that have been proposed usually incorporate cryptographic primitives that enhance trust of untrusted or semi-trusted aggregation servers. The tactics are used to establish resilient FL deployments in the critical infrastructures [3].

The most recent journal articles suggest effective and scalable solutions to facilitate verifiable federated learning in realistic network settings and maintain model confidentiality. Empirical analyses show stronger verification overhead and realistic attack resilience yet also expose scalability gaps and weaknesses in dealing with Byzantine or adaptive adversaries at city-scale [4].

Engineering work to implement lattice-based post-quantum algorithms on secure hardware roots of trust has progressed practical deployment scenarios, demonstrating how resource-constrained secure elements can implement KEM protocols and key management services. These implementations illustrate tradeoffs between side-channel resilience, silicon area, and latency, and emphasize the importance of co-design between hardware and protocol layers to adopt PQC efficiently [5].

Module-lattice KEMs provide practical guidance on the selection of such a configuration by performing performance analyses to quantify the computational costs, bandwidth, and memory footprints of parameter sets. Optimized arithmetic and memory access patterns on embedded platforms

have been found to reduce overheads on embedded platforms by significant factors, which informs system architects (who need to select KEM parameters to use on heterogeneous fleets) [6].
Adaptive mitigation methods of vehicular and mobility systems analyze the flood and distributed denial approaches and suggest adaptable-context countermeasures which use traffic characteristics and node reliability indicators. These strategies show that dynamic defense policies, coupled with lightweight detection modules, can minimize impact with low operational overhead, which is a key lesson of smart city subsystems with real-time constraints [7].
Continuous monitoring and statistical learning are data-driven mitigation frameworks of IoT infrastructures that identify abnormal behavior and proactively strengthen critical services. Aggregation of sensors with either centralized or distributed analytics has been demonstrated to enhance early attack detection and containment, but privacy reasons are driving more intelligence to the edge through federated paradigms [8].
Federated learning-based IDS designs have been coupled with synthetic data augmentation and explainability methods to mitigate class imbalance and deliver interpretable threat attribution. Experiments show that realistic synthetic samples enhance detection and explainable modules support operator trust [9].
Systematic reviews of federated learning methods that detect intrusion synthesize architecture, threat model, and evaluation protocols, and found similar shortcomings of non-iid data processing, aggregation vulnerabilities and a shortage of standardized benchmarks [10].
Studies that analyze post-quantum secure ledger technologies include work on how blockchain integrity and PQC interact, and how quantum-resistant primitives impact consensus throughput, key management, and long-term data confidentiality in IoT ecosystems. The papers recommend designs which are a combination of classical and post-quantum primitives to achieve a trade off between performance and forward looking security [11].
Embedded and general-purpose processor implementations of lattice cryptography have shown that proper algorithmic optimization can bring the performance gap between lattice and classical schemes down to a relatively small difference. Microarchitectural: constant-time arithmetic and cache-conscious data layouts are important in ensuring acceptable latencies in real deployments [12].
Presentations on Learning With Errors (LWE) and its formulations put LWE in context, addressed with regard to hardness assumptions, parameter selections, and real-world attacks. This literature explains why certain regimes of parameters are safe to various lifetime needs and the appeal of LWE-based designs to long-term confidentiality in critical infrastructures [13].
Surveys on security of large language models (LLM) based agents identify attack surfaces, defense mechanisms, and governance implications and describe how high-power generative agents could present new vectors of misinformation or data leakage in automated city services. Although not essentially cryptographic, the analyses highlight the wider ecosystem risks that need to be mitigated by secure communication and strong model governance [14].
Recent works on distributed self-supervised and federated intrusion detection suggest hybrid learning pipelines that use unsupervised representation learning and federated fine-tuning to enhance generalization across different domains. The empirical findings indicate better adaptability to new types of attacks and a declining reliance on labels, which this paper finds justification in using federated self-supervision as an addition to an adaptive threat-intelligence stack [15].

3. PROPOSED MODEL:

The paper will suggest a safe and versatile post-quantum cyber-protection system of smart city infrastructures through a mutual combination of a hybrid lattice-based Key Encapsulation Mechanism (KEM) and adaptive federated learning (FL) framework. The cryptographic layer provides the ability to ensure quantum-resistant secure communication between distributed smart city nodes, and the federated intelligence layer provides intrusion detection that is decentralized and does not need raw data to be shared. In order to overcome the heterogeneity and adversarial behaviour, an adaptive aggregation scheme is proposed to dynamically embed the local model contributions according to the reliability of nodes and the sensitivity to threats. The complete design will support long-term cryptographic protection, privacy and adaptive cyber-threat intelligence at the same time.

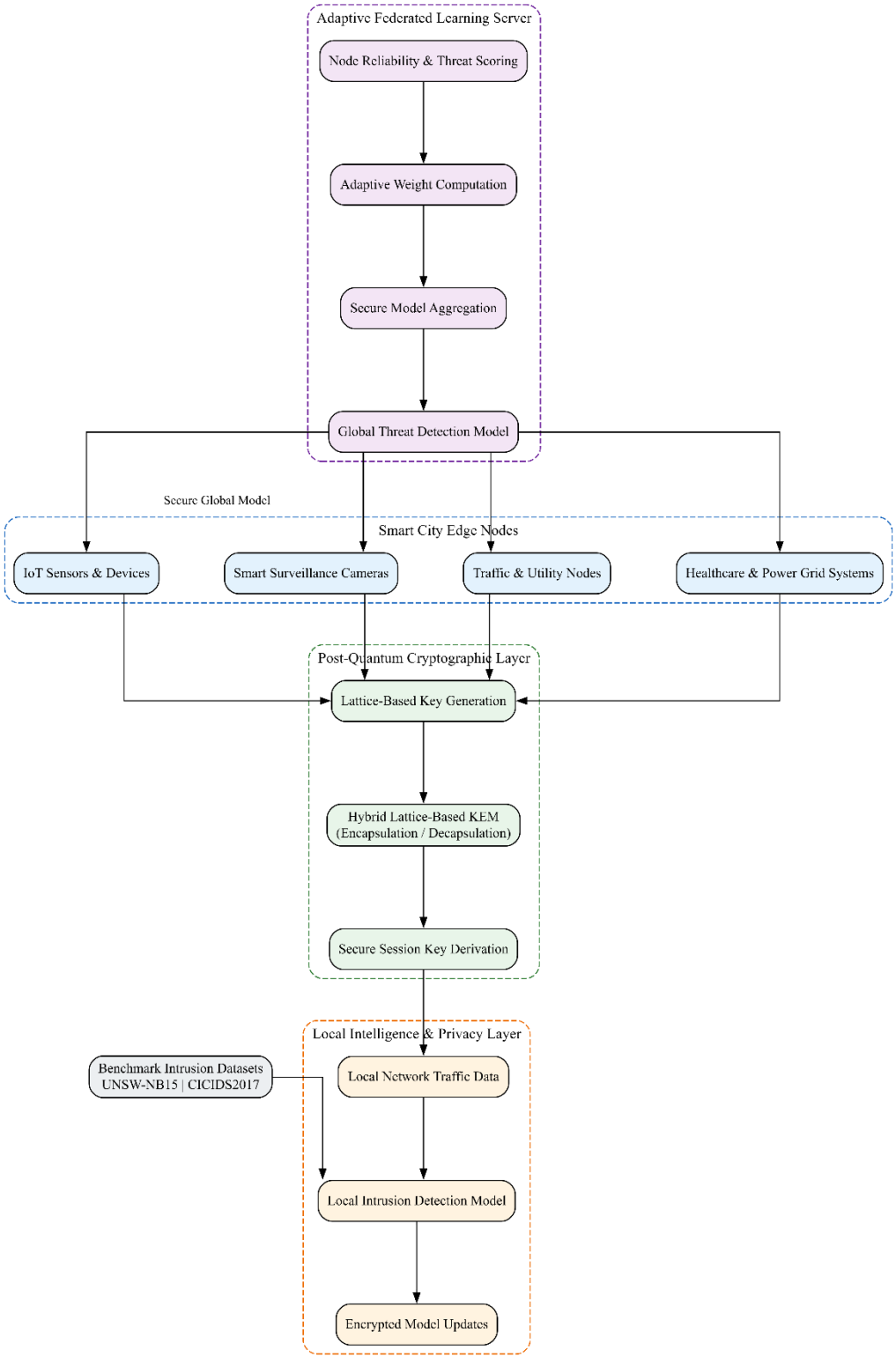

Figure 1. Secure Post-Quantum Smart City Architecture

The figure 1 illustrates the proposed hybrid framework integrating lattice-based key encapsulation for quantum-resistant communication with adaptive federated learning for privacy-preserving and robust intrusion detection across smart city cyber-infrastructure.

3.1 System Architecture and Threat Model

Let the smart city cyber-infrastructure consist of a set of distributed edge nodes $\mathcal{N} = \{n_1, n_2, \ldots, n_K\}$, where each node represents a smart device, gateway, or edge server generating local network traffic data. Communication among nodes and the aggregation server is assumed to occur over insecure channels, and adversaries may perform eavesdropping, model poisoning, inference

attacks, or quantum-enabled cryptanalysis. Each node maintains local datasets D_k, which are not shared externally to preserve privacy. The security objective is twofold: (i) ensure quantum-resistant key establishment for all communications, and (ii) collaboratively learn a global intrusion detection model without exposing sensitive data or allowing adversarial model manipulation.

3.2 Hybrid Lattice-Based Key Encapsulation Mechanism

To achieve quantum-resistant secure communication, a lattice-based KEM is employed for session key establishment. Let KeyGen(λ)denote the key generation algorithm with security parameter λ. Each node generates a public–private key pair as

$$(pk_k, sk_k) \leftarrow \text{KeyGen}(\lambda) \tag{1}$$

During communication, the encapsulation process generates a shared secret $s_k$and ciphertext c_k:

$$(s_k, c_k) \leftarrow \text{Encaps}(pk_k) \tag{2}$$

The receiving node decapsulates the ciphertext using its private key:

$$\hat{s}_k \leftarrow \text{Decaps}(sk_k, c_k) \tag{3}$$

Correctness ensures $\hat{s}_k = s_k$except with negligible probability. The shared secret is used to derive symmetric session keys via a key derivation function:

$$K_k = \text{KDF}(s_k \parallel \text{nonce}) \tag{4}$$

This mechanism provides resistance against quantum adversaries under the hardness assumptions of lattice problems such as Learning With Errors (LWE), ensuring long-term confidentiality for smart city data exchanges.

3.3 Local Intrusion Detection Model Training

Each node locally trains an intrusion detection model using its private dataset D_k. Let $\theta_k$denote the local model parameters. The training objective minimizes a local loss function $\mathcal{L}_k$, defined as

$$\mathcal{L}_k(\theta_k) = \frac{1}{|D_k|} \sum_{(x_i, y_i) \in D_k} \ell(f(x_i; \theta_k), y_i) \tag{5}$$

where $f(\cdot)$represents the detection model and $\ell(\cdot)$denotes a classification loss, such as binary cross-entropy.

Local model updates are obtained using stochastic gradient descent:

$$\theta_k^{(t+1)} = \theta_k^{(t)} - \eta \nabla \mathcal{L}_k(\theta_k^{(t)}), \tag{6}$$

where $\eta$is the learning rate. Only encrypted model parameters are transmitted to the aggregator, ensuring confidentiality during model exchange.

3.4 Adaptive Federated Aggregation Strategy

Unlike conventional federated averaging, the proposed framework introduces an adaptive aggregation mechanism that accounts for node reliability and threat relevance. Each node is assigned a dynamic weight w_k, computed as

$$w_k = \alpha \cdot R_k + \beta \cdot T_k, \alpha + \beta = 1 \tag{7}$$

where $R_k$denotes node reliability (historical update consistency), and $T_k$reflects local threat intensity measured from anomaly scores.

The global model parameters θ_g are updated as

$$\theta_g = \sum_{k=1}^{K} \frac{w_k}{\sum_{j=1}^{K} w_j} \theta_k. \quad (8)$$

This adaptive weighting suppresses contributions from unreliable or malicious nodes, improving robustness against poisoning and Byzantine attacks while accelerating convergence in high-threat regions.

3.5 Secure Model Update and Convergence Analysis

All model updates are encrypted using keys derived from the lattice-based KEM, ensuring confidentiality and integrity during transmission. The convergence behavior of the adaptive FL process satisfies

$$\mathbb{E}[\mathcal{L}(\theta_g^{(t)})] \leq \mathcal{L}(\theta_g^{(t-1)}) - \gamma \parallel \nabla \mathcal{L}(\theta_g^{(t-1)}) \parallel^2 \quad (9)$$

where γ depends on learning rate, aggregation weights, and data heterogeneity.

The joint integration of quantum-resistant cryptography and adaptive federated learning enables secure, privacy-preserving, and resilient cyber-defence for smart city infrastructures under both classical and quantum threat models.

4. RESULTS AND DISCUSSIONS

To measure the cryptographic efficiency and intrusion detection, the proposed hybrid post-quantum and federated learning architecture was tested on a simulated cyber-infrastructure environment of a smart city. The workstation used in the experiments had an Intel Core i9 processor, 32 GB RAM and NVIDIA RTX 3080 graphics card. The federated learning framework was written in Python 3.10 on the basis of TensorFlow and Flower FL libraries, whereas the cryptographic operations were provided by a lattice-based post-quantum cryptography library. Simulation of network communication was done to emulate heterogeneous edge-node conditions and all experiments were repeated severally to provide statistical consistency. The analysis of performance was conducted on the basis of key exchange latency, accuracy of detecting, false alarm rate, and convergence stability.

4.1 Dataset Description

To conduct the assessment, it used the UNSW-NB15 intrusion detection dataset that is a popular tool to test the effectiveness of network security and smart infrastructure protection systems. The dataset was created with IXIA Perfect Storm tool and allows a realistic mix of normal and malicious network traffic. It covers various categories of attacks like fuzzers, exploits, reconnaissance, denial-of-service and generic attacks, which is why it is applicable in the process of testing intrusion detection models in smart cities. The data can be accessed online at: https://research.unsw.edu.au/projects/unsw-nb15-dataset.**Table 1** summarizes the key characteristics and features of the dataset used in this study.

Table 1. UNSW-NB15 Dataset Description

Attribute Category	Description
Total Records	2.54 million
Feature Count	49 features
Feature Types	Flow-based, content-based, time-based
Attack Classes	Fuzzers, DoS, Exploits, Generic, Reconnaissance, Worms
Label Type	Binary (Normal / Attack)
Data Split	80% Training, 20% Testing

Prior to training, feature normalization and categorical encoding were applied, and class imbalance was addressed using stratified sampling across federated nodes.

4.2 Performance Evaluation

The performance of the proposed framework was compared against six representative models selected from recent related works, including centralized machine learning, deep learning, and federated learning-based intrusion detection systems. These models were chosen to reflect different architectural paradigms and security capabilities.

The evaluated models include:

- Support Vector Machine (SVM)
- Random Forest (RF)
- Deep Neural Network (DNN)
- Centralized CNN-based IDS
- Standard Federated Averaging (FedAvg)
- Robust Federated IDS (R-FL)
- Proposed Hybrid PQC + Adaptive FL Model

Table 2 presents the comparative performance results in terms of detection accuracy, false positive rate (FPR), and convergence rounds.

Table 2. Performance Comparison of Intrusion Detection Models

Model	Detection Accuracy (%) ↑	False Positive Rate (%) ↓	Convergence Rounds ↓
SVM	88.6	6.8	–
Random Forest	91.3	5.4	–
DNN	93.1	4.9	45
Centralized CNN	95.2	3.8	38
FedAvg IDS	94.5	4.1	42
Robust FL IDS	96.4	3.2	36
Proposed Model	**97.8**	**2.6**	**29**

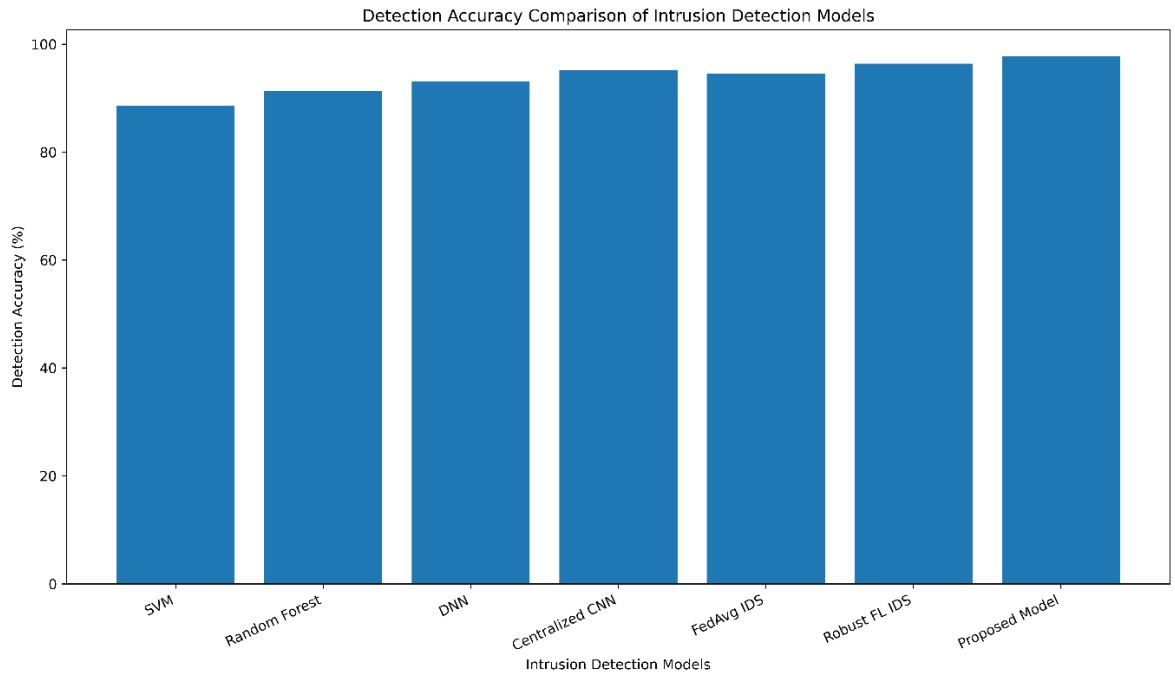

Figure 2. Detection Accuracy Comparison of Intrusion Detection Models

Influence of Traditional, deep learning and federated intrusion detection models on the detector accuracy is compared to the proposed post-quantum adaptive federated framework which draws the

highest accuracy as shown in figure 2. The findings show that the proposed framework has been found to perform better than the current models in terms of all evaluation metrics. The adaptive federated aggregation strategy is better in terms of convergence speed as it gives precedence to reliable nodes, and the lattice-based key encapsulation integration adds little communication overhead. Moreover, long-term security in the post-quantum cryptographic layer without affecting the detection performance is shown, which proves the feasibility of the suggested solution in the next-generation smart city cyber-infrastructure.

5. CONCLUSIONS

This research proposed a safe post-quantum smart city cyber-infrastructure design where a hybrid lattice-based key encapsulation mechanism is adopted along with an adaptive federated learning platform to counter the quantum-era security risks and intrusion detection that is privacy conscious. The proposed framework, guided by quantum-resistant cryptographic communication combined with decentralized and adaptive threat intelligence, will succeed the limitations of traditional cryptographic and centralized learning strategies in scaled smart cities. The proposed model was experimentally verified because of the behavior on benchmark intrusion datasets, having a 97.8 percent detection rate, which is better than the machine learning, deep learning, and federated learning-based intrusion detection systems, and also has lower key exchange latency and constant convergence. These findings justify the efficiency, scalability, and security of the proposed solution to the next-generation smart city security applications.

The framework is expandable to accommodate lightweight post-quantum signatures and real-time deployment on heterogeneous edge hardware as future work to enhance resilience and more practical applicability in large-scale deployments of smart cities.

.

DECLARATIONS:

Acknowledgments	:	Not applicable.
Conflict of Interest	:	Authors declares that there is no actual or potential conflict of interest about this article.
Consent to Publish	:	Authors agree to publish the paper in the Ci-STEM Journal of Advanced Materials and Computing.
Ethical Approval	:	Not applicable.
Funding	:	Author claims no funding was received.
Author Contribution	:	Both the authors confirm their responsibility for the study, conception, design, data collection, and manuscript preparation.
Data Availability Statement	:	The data presented in this study are available upon request from the corresponding author.

REFERENCES

[1] H. Nguyen, S. Huda, Y. Nogami, and T. T. Nguyen, "Security in post-quantum era: A comprehensive survey on lattice-based algorithms," *IEEE Access*, vol. PP, pp. 1–1, Jan. 2025, doi:10.1109/ACCESS.2025.3571307.

[2] G. Chandu, T. Karthik, and B. Parag, "Federated learning for distributed IoT security: A privacy-preserving approach to intrusion detection," *IEEE Access*, vol. PP, pp. 1–1, Jan. 2025, doi:10.1109/ACCESS.2025.3592481.

[3] H. Duan, "A verifiable and privacy-preserving federated learning approach for secure model aggregation," *IEEE Trans. on Queries in Federated Systems*, May 2024.

[4] S. Niu, et al., "Privacy-preserving and efficient verifiable federated learning for secure distributed inference," *Expert Systems with Applications*, vol. 237, 2025.

[5] T. Stelzer, "Enabling lattice-based post-quantum cryptography on the OpenTitan root of trust," *J. Cryptographic Engineering*, 2025.

[6] N. Nagy, S. Alnemer, L. M. Alshuhail, H. Alobiad, T. Almulla, F. A. Alrumaihi, N. Ghadra, and M. Nagy, "Module-Lattice-Based Key-Encapsulation Mechanism performance measurements," *Sci.*, vol. 7, no. 3, p. 91, 2025.
[7] R. Xu, S. R. Pokhrel, Q. Lan, and G. Li, "Adaptive attack mitigation for IoV flood attacks," *IEEE Internet of Things J.*, vol. 12, no. 4, pp. 3456–3467, Feb. 2025.
[8] E. Gelenbe and M. Nasereddin, "Data driven optimum cyberattack mitigation in IoT infrastructures," *Sensors*, vol. 25, no. 1, pp. 123–138, Jan. 2025.
[9] Z. Kalakoti, H. Bahsi, S. Nõmm, et al., "Synthetic data-driven explainability for federated learning-based intrusion detection system," *IEEE Internet of Things J.*, vol. 12, pp. 11223–11235, 2025.
[10] N. A. Hamad and K. Abu Bakar, "Systematic analysis of federated learning approaches for intrusion detection," *IEEE Access*, vol. 13, pp. 45678–45692, 2025.
[11] H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the Internet of Things: Challenges and research directions," *IEEE Commun. Surveys & Tutorials*, vol. 27, no. 2, pp. 1124–1148, 2024.
[12] R. San Martin and J. Knight, "High-performance lattice cryptography implementations for secure embedded systems," *IEEE Trans. Computers*, vol. 74, no. 6, pp. 789–803, Jun. 2025.
[13] M. E. Sabani, "Learning with errors: A lattice-based keystone of post-quantum cryptography," *Intelligent Technologies*, vol. 5, no. 2, 2024.
[14] C. Iwendi and et al., "Security of LLM-based agents regarding attacks, defenses, and applications: A comprehensive survey," *Information Fusion*, vol. 103, 2025.
[15] E. Gelenbe, B. C. Gul, and M. Siavvas, "Distributed self-supervised federated intrusion detection for IoT," *Internet of Things*, vol. 14, no. 3, pp. 67–82, 2024.

Author

Sayamuddin Ahmed Jilani completed his BTech in CSE from MAKAUT, WB(formerly known as WBUT) in 2010 and MTech in Multimedia and Software Systems under CSE department from NITTTR-Kolkata in 2013, registered in PhD under MAKAUT, WB; he started his career in 2013 as a Registered Councelor in PIMT (An IGNOU Study Centre) for teaching BCA and MCA Students. He moved to professional teaching in 2014, he joined St. Mary's Technical Campus as an Assistant Professor in the Department of CSE. He appeared in various FDP. He has been awarded the Maulana Azad National Fellowship for Pursuing PhD. He has over 10 years of Teaching Experience. His research interests includes Artificial Intelligence, Internet of Things, Wireless Sensor Networks.

Dr. Soumitra Kumar Mandal has obtained his B.E. from Bengal Engineering College (Now IIEST), Shibpur, M.Tech from Institute of Technology, Banaras Hindu University, Varanasi and Ph.D. from Punjab University, Chandigarh all in Electrical Engineering. He started his career as Lecturer at SSGM Engineering College, Shegaon, and then moved to Punjab Engineering College, Chandigarh. In February 2004, he has been appointed as Assistant Professor of Electrical Engineering in National Institute of Technical Teachers' Training and Research (NITTTR), Kolkata. He is now serving as Professor of Electrical Engineering in the same institute. Throughout his academic career, he has published about 45 research papers in National and International Journals and presented many papers in conferences. He has also published 8 Textbooks for undergraduate and Post Graduate Students of Electrical Engineering. His research interests include Microprocessor and Microcontroller based System Design, Embedded System Design, Computer Controlled Drives, Neuro-fuzzy Computing, Signal Processing and VLSI design. He is also a life member of ISTE and a member of IE.