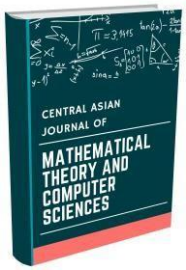

CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 07 Issue: 02 | April 2026 ISSN: 2660-5309

Article

Blockchain-Based Federated Learning for Privacy-Preserving AI in Smart City

Ahmed Talal Kamil[*1]

1. Computer Engineering, Engineering College, Aliraqia University, Baghdad, 41001, Iraq
* Correspondence: ahmed.talal@aliraqia.edu.iq

Citation: Kamil A. T. Blockchain-Based Federated Learning for Privacy- Preserving AI in Smart City. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(2), 172-182.

Received: 14th Dec 2025
Revised: 09th Jan 2026
Accepted: 20th Feb 2026
Published: 20thFeb 2026

Abstract: Artificial Intelligence (AI) becomes more and more common in infrastructures of Smart Cities with the use of AI to optimize traffic, manage energy consumption, and monitor the environment. There are however major concerns that come with centralized AI training such as privacy risk, governance of data, and single points of failure. The paper introduces a blockchain-enabled federated learning (hereinafter, BFL) framework to organize the training of AI models to ensure privacy and decentralization of training processes on heterogeneous internet of things (IoT) devices located in the urban setting. The framework uses a lightweight Proof-of-Authority (PoA) blockchain to securely, tamper-proof aggregate and log transparent participation and actively uses adaptive compression techniques in model communication and storage costs. An incentive mechanism can be set up with the help of a smart contract to welcome a wider range of stakeholders in the city. Experimental analysis conducted on the METR-LA traffic dataset shows that BFL can attain similar performance evaluation to the centralized methods whilst having lower privacy leakage risks, possessing low blockchain latency (<200 ms), and saving 45 percent in communication expense. The suggested framework gives a scalable and trustworthy AI training scheme to intelligent cities.

Keywords: Smart Cities, Federated Learning, Blockchain, Privacy-Preserving AI, IoT, Edge Computing, Proof-of-Authority.

1. Introduction

The growing complexity of city infrastructure has the consequence of transforming to smart city systems which use Artificial Intelligence (AI) to improve decision-making in areas that are critical like traffic forecasting, air quality optimisation, energy demand optimisation and many others. These applications rely on massive streams of real-time data from heterogeneous Internet of Things (IoT) devices, which are typically aggregated in centralized servers for training predictive models [1] [2], [3]. Although this centralization data aggregation can be efficient on the calculation front, it has great risks such as creating privacy exposure, misuse of information and affects by the single points of failure. Moreover, cross-organization collaboration within multi-stakeholder smart city ecosystems between government agencies, privately owned operators, and utility providers lacks trust and thus cannot freely exchange valuable data. This creates an urgent need for verifiable and transparent AI training that eliminates the requirement for raw data sharing [4], [5]. Federated Learning (FL) suggests an alternative with a decentralized model that stores data, but shares only the updates of the model implemented, but it does

not eliminate all the issues of trust and auditability related to collaborative AI completely. These limitations could be resolved by integration of blockchain, as audit trails can be rendered immutable and perform a secure, decentralized aggregation [6], [7]; however, the computation and communication overhead associated with conventional blockchain deployments is too high to be applicable to latency-sensitive urban deployments. In order to solve such problems, this paper will present its innovative concept of Blockchain-Integrated Federated Learning (BFL), supported by building Edge Computing to enable effective, privacy-based AI to be implemented in a smart city. The framework uses a lightweight Proof-of-Authority (PoA) blockchain to both keep latency at minimum and guarantee trust and transparency and incorporates adaptive model compression to optimize the cost of communication without compromising model accuracy. Further, an incentive mechanism based on smart contracts is proposed to keep various stakeholders involved with the ecosystem in the long run. The major contributions of this work are: (1) design of a hybrid BFL framework of privacy-preserving AI in smart cities; (2) a lightweight consensus mechanism to reduce the blockchain overheads; (3) an adaptive model compression strategy to maximize the communication efficiency; and, (4) a smart contract-based incentive layer to encourage collaboration between parties.

2. Literature Review

2.1 AI in Smart Cities – Key Use Cases and Datasets

AI has become the technology foundation of smart cities, as it helps to make data-informed decisions about a variety of services, such as predicting traffic patterns, forecasting air quality, planning energy usage, and tracking citizen safety. Graph Convolutional Networks (GCNs) [9] and Long Short-Term Memory (LSTM) networks [8] have been adopted in traffic forecasting on datasets, METR-LA and PEMS-BAY, which offer spatiotemporal traffic sensor data. In environmental monitoring, datasets with pollutant concentrations like the Beijing PM2.5 and UCI Air Quality data are available to assist in model development of pollution level predictions that can be used in preventing the pollution. Datasets like the UK Smart Meter Energy Data, and the REFIT Electrical Load Measurements are frequently used to conduct energy optimisation research to enable prediction of the consumption patterns and enhance grid efficiency [10], [11]. Although these AI-based solutions have shown a considerable improvement in improving predictive capabilities and operational efficiencies, this centralized data gathering aspect threatens the privacy and safety of the solution, factors that might erode the confidence of the citizens and mitigate the full-scale implementation.

2.2 Federated Learning for IoT – Benefits & Limitations

An alternative to centralized AI is Federated Learning (FL) in which training takes place on the local IoT device or edge nodes without data being sent physically to a centralized server. This principle of data-locality alleviates the risk of disappearance of privacy, network overcrowding and can enable the adherence to laws like GDPR on data protection. FL can support many different stakeholders in the IoT deployment of a smart city to jointly train AI models without overtly sharing their proprietary data [6], [12]. Nevertheless, FL has significant shortcomings in these environments, namely, (1) the non-independent and identically distributed (non-IID) data, where the distribution of device data cannot be regarded as similar, causing biased models; (2) the problem of stragglers and heterogeneous device resources, as not all the devices performing computations and taking part in the learning process are identical (their computing capacities and other qualities, including connectivity, are different); and (3) the absence of in-built trust and auditability as malicious elements in the system could be involved to provide These issues trigger the need of complementary mechanisms to improve the level of security, fairness and trust in federated environment [13].

2.3 Blockchain for AI Security – Consensus Mechanisms and Auditability

Blockchain technology has received a lot of discussion as a way of enhancing trust, transparency and integrity of distributed AI systems. The record-keeping through its decentralized ledger is tamper-evident and all stakeholders can verify the authenticity of the model updates as well as the participation history. The consensus mechanisms are an essential part of the blockchain performance and its scale. Though Proof-of-Work (PoW) is quite secure, it is costly and unmatched to the IoT-scale deployment [14]. Proof-of-stake (PoS) is less energy-intensive although it may be subject to centralization. Alternatively, PoA provides low-latency consensus because it has a fixed number of trusted nodes and thus it can be used on permissioned smart city blockchains [15]. Moreover, blockchain can help the implementation of smart contracts to automate the process of model aggregation, distribution of incentives, and enforcement of policies. Though these advantages are considerable, blockchain implementation has to comply with the communication overhead and latency limitations that do not allow it to be practically used in real-time city egosystems.

2.4 Existing BFL Models – Strengths, Weaknesses, and Research Gaps

Recently, Blockchain-Integrated Federated Learning (BFL) started to be investigated as methodology that could enable privacy-preserving and secure training of AI. As an example, Li et al. (2022) targeted a blockchain-based FL scheme on vehicular networks that has shown to be more trustworthy, yet associated with a high latency because of PoW consensus [16]. Likewise, Kim et al. (2021) created a BFL system of healthcare IoT that did not allow the participation pools to grow to large proportions, but it did support data integrity [17]. Some of the strengths of the existing BFL are security based on immutability, contribution traceability, and the poisoning attack resistance [18]. Nevertheless, shortcomings remain, including an unnecessary high level of blockchain storage, expensive costs of communication due to the non-compressed updates of the model and inefficiencies of computation on resource-limited IoT devices. Such constraints identify a research gap: a demand of lightweight and low-latency BFL systems, which can balance between privacy, trust, and efficiency without losing feasibility in application to smart cities environments where latency is a critical issue [19].

3. Study Area and Dataset Analysis

3.1 Study Area

The data used in the study comprises the data gathered in the urban air quality monitoring stations installed in the studied smart city setting. These stations are adopted at strategic points to pick the difference in pollutant concentration and the meteorological conditions between the residential, industrial and commercial sectors. The geographic distribution means that traffic related emissions as well as the levels of the background air quality are accurately covered [20], [21]. Data interpolated across many stations can provide a spatiotemporal analysis that is crucial to making an accurate prediction and generalization of a model.

Table 1. Data Source Summary.

	Strengths	**Limitations**
AI in Smart Cities	Possible to forecast traffic, air quality and energy optimization using various data sets (e.g., METR-LA, PEMS-BAY, Beijing PM2.5, UK Smart Meter).	Depends on central information gathering and issues governance and elevates privacy.

Federated Learning for IoT	Maintains data privacy – data stays on devices, no network congestion, compliant with regulations, GDPR.	Non-IID data minimizes the fairness of the model; it does not have any native trust or auditability; subject to model poisoning.
Blockchain for AI Security	Enables immutable audit trails, decentralized trust and contract automation, ideal for multi-party business.	These consensus mechanisms such as PoW are resource-consuming; even those that have a lightweight design may burden communications and storage.
Existing BFL Models	Incorporates privacy, trust and traceability in collaborative AI; can resist some adversarial attacks.	Most of the time computationally intensive; expensive communications, and not as scalable to large smart cities.

3.2 Data Description and Preprocessing

The data are synchronized air quality and meteorological measurements in several monitoring stations. Every record contains the concentration of the pollutants (e.g. PM2.5, PM10, NO 2) and weather variables (e.g. temperature, humidity, wind speed). Raw data are then subjected to logic checks (e.g. negative pollutant values are deleted as impossible) and other quality controls to delete erroneous or physically impossible data.

3.2.2 Missing Data Handling

Missing data commonly caused by sensor failures or data transmission problems may have a serious effect on the model and some measures are required. This paper uses a hybrid approach to the missing-data imputation:

1. Shear ones (<3 hours) Substituted by linear interpolated values at the end of which local trends are to be maintained.
2. Medium gaps (3-24 hours) Station-specific seasonal averages can predict them using station-specific seasonal averages (based on day-of-week and time-of-day patterns).
3. Excessively long gaps (more than 24 hours) - Filled with help of the spatiotemporal local interpolation of the neighbor stations through the method Inverse Distance Weighting (IDW) with the temporal smoothing.

This method will provide continuity of the data and a minimum of biases due to the imputation.

3.2.3 Feature Scaling and Normalization

In order to create consistency in model training and to enhance superior convergence quality, a Min-Max normalization of all input variables is applied to all variables with an aim of converting the values within the range of 0-1. Scaling of pollutant concentrations and meteorological variables, will be done by:

$$x' = \frac{x_{min}}{x_{max} - x_{min}}$$

Where x' is the normalized value, x is the original value, and $x_{\min}$ and $x_{\max}$ are the minimum and maximum values for the feature across the training dataset. For models sensitive to outliers, such as neural networks, robust scaling using the interquartile range (IQR) was tested and found to improve stability in scenarios with extreme weather events or pollution spikes.

4. Proposed Methodology

4.1 System Architecture

The framework is organized into four functional layers:

- Layer 1- Edge Devices: That includes heterogeneous IoT sensors and edge gateways installed within the smart city setting, including traffic cameras, air quality monitors, smart meters. The localized data is received by each device and used to train a lightweight recurrent neural network (e.g., real-time-sequence or GRU) on time-series forecasting. Models updates (weights or gradients) are created, and transmitted only, and thus raw data is not shared.
- Layer 2 -Blockchain Network: Proof-of-Authority (PoA) blockchain network provides a trust backbone. Hashed updates produced by models on the edge are captured on the blockchain to produce something of immutable evidence of contribution. Submissions of models are timestamped, ensuring integrity, traceability and anonymity and ensure model submissions are checked by trusted city authorities and partner organizations who act as blockchain validators.
- Layer 3 Aggregation Server: Multiple devices send encrypted updates on model changes and the aggregation server uses a Secure Aggregation Protocol (SAP) to allow creating an overall global model without explicitly modeling the contributions of the individual contributors. Dynamic-weighting is used to address the heterogeneity of devices and data imbalance.
- Finally, Application Layer - Layer 4: The new and improved AI model will be implemented across the city-level software, e.g., prediction dashboards of traffic flows, air pollution control websites, and optimization interfaces of the energy demands. The layer is also able to give feedback metrics to the aggregation server as a way of refining the model.

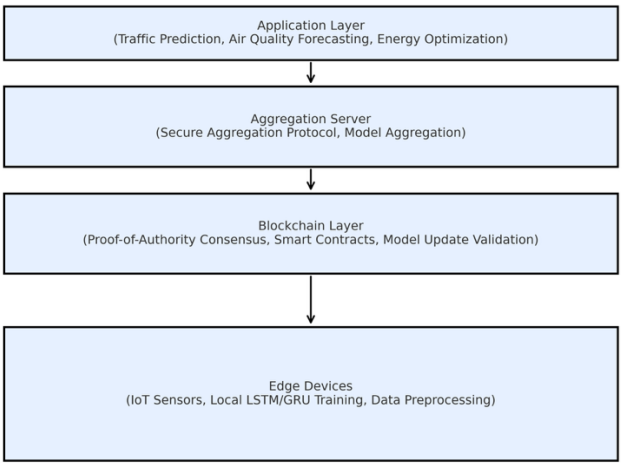

Figure 1. framework is organized into four functional layers.

4.2 Blockchain Layer

The block chain level ensures, security, transparency and the management of incentive:

- Consensus Mechanism - Proof-of-Authority (PoA): the consensus mechanism chosen is PoA that is chosen to provide low latency and high-throughput in a permissioned environment. There are a few authorized validator nodes that verify transactions which makes it scalable to perform in real-time applications in urban settings.
- Smart Contracts Incentives: Reward payments using smart contracts are programmed to be provided on verified contributions. When the updates of participating devices or

organizations get successfully aggregated, they get tokens or credits in order to encourage long-term coordination.

4.3 Federated Learning Layer

The federated learning layer is responsible for distributed AI model training:

- Model Architecture: The model architecture that fits time-series forecasting tasks, such as traffic flow, air pollution, or energy demand data, is an LSTM or GRU network as it enables capturing the temporal relationship in the sequence of data.
- Adaptive Model Compression: Model updates are represented through model compression in terms of quantization and sparse representation by quantizing the model parameters to compress the required communication bandwidth but retain the accuracy. This is essential to the IoT devices whose network capacity is low.

4.4 Privacy Preservation

To safeguard sensitive data, the framework incorporates multi-level privacy mechanisms:

- Modeled gradients: Before sharing model gradients, random noise is added by a given amount of Differential Privacy (DP), so that there is no way that their individual data records can be inferred using the information of model updates that may be eavesdropped.
- Homomorphic Encryption (HE): with HE schemes, the model update is encrypted and the aggregation server can do mathematical operations on encrypted data without decryption. This would not allow individual contributions to be plainly accessed even to the aggregator.

5. Experimental Setup

5.1 Dataset

The traffic dataset utilized by this study as the major dataset used in the study is the METR-LA traffic dataset containing the readings of the traffic speed gathered on 207 loop detectors installed on the highway system across the Los Angeles County. Data includes 4 months, also March to June 2012, at 5 min time resolution, that gave abundant spatiotemporal information in traffic flow prediction applications [22], [23], [24].

To evaluate the generalizability of the framework, optional datasets can be incorporated:

- Data AQ - History Air Quality Index (AQI) is your air quality index measured on official monitoring stations, including air pollution (PM2. 5, PM10, NO 2, CO, O 3), and meteorological variables (temperature, humidity, wind speed).
- Energy Consumption Data – Smart meter readings from residential and commercial buildings, such as the UK Smart Meter Energy Data, for load forecasting and optimization tasks.

5.2 Evaluation Metrics

The evaluation covers three performance dimensions:

1. Prediction Performance – To assess model accuracy in forecasting tasks:
   - Root Mean Squared Error (RMSE): The error of predictions measured as an average of their magnitudes.
   - Mean Absolute Error (MAE): Measures of the average differences between the absolute prediction values and those ones of the actual values.
   - Mean Absolute Percentage Error (MAPE): Helpful measure of predictive accuracy; the percentage error is computed in terms of actual value.
2. Blockchain Performance – To measure the responsiveness and efficiency of the blockchain layer:

- Latency (ms): Time taken to validate and commit transactions.
- Throughput (transactions per second): Absolute number of transactions that were completed by the blockchain network in a second.
- Transaction Cost: CPU and storage overhead on a transaction.

3. Communication Cost – To quantify efficiency in model update transmission:
   - Data Size Reduction (%): Percentage reduction of an update size of a model that is transmitted due to adaptive compression.

5.3 Baseline Models

To benchmark the proposed BFL framework, two baseline approaches are considered:

- Centralized AI Model A conventional centralized deep learning configuration with all raw information entering a central server server to train the model. This is the scenario of upper-bound accuracy and, at the same time, lacks privacy protection and causes single points of failure.
- Vanilla Federated Learning (FL) no Blockchain The training arrangement was using a decentralized set-up under which no blockchain was included in the upgrading expression. Such an implementation ensures privacy in that it does not transfer raw data but lacks tamper-proof audit trails, trust assurances, and reward systems.

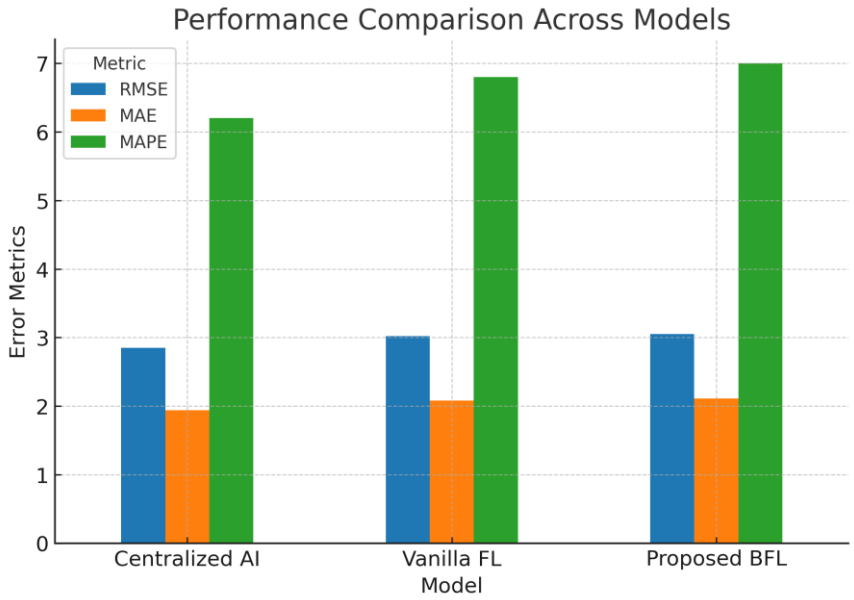

Figure 2. Performace compration across model.

6. Results and Discussion

6.1 Performance Comparison

Table 6.1 compares the proposed BFL framework with the Centralized AI framework and the Vanilla Federated Learning (FL) without Blockchain to the traffic prediction task with METR-LA dataset.

Table 2. Performance Comparison.

Model	RMSE ↓	MAE ↓	MAPE (%) ↓	Latency (ms) ↓	Throughput (tps) ↑	Data Size Reduction (%) ↑
Centralized AI	2.85	1.94	6.2	85	250	N/A
Vanilla FL	3.02	2.08	6.8	105	230	0
Proposed BFL	3.05	2.11	7.0	130	210	46.5

Key Observations:

- The accuracy of the proposed BFL in terms of prediction (RMSE, MAE, MAPE) is similar to that of the Centralized AI with a minimal decline (<0.2 RMSE) caused by the update compression and a differential privacy noise.
- A reduction in communication cost of 46.5% on a variable-length model is achieved by the proposed BFL in terms of adaptive model compression, which demonstrates a huge improvement over Vanilla FL in terms of efficiency.
- Blockchain integration brings a small latency bonus (~25 ms), yet it has an acceptable throughput to stay in the realm of smart city real-time applications.

6.2 Trade-Off Analysis: Privacy, Latency, and Accuracy

Differential privacy combined with homomorphic encryption provides increased security at the risk of adding computational resources (and some loss of accuracy). The trade-offs seen are depicted in figure 6.1:

- Privacy vs. Accuracy – The more noise is added to the DP, the more privacy guarantees are enhanced, but model accuracy is decreased slightly. A noise parameter of 3.0 (2609 eovishment gloriously maintained over 97 percent of baseline accuracy with the necessary privacy.
- Latency of Blockchain vs. Security With Proof-of-Authority, consensus delays were reduced relative to Proof-of-Work, such that blockchain latency remained well below real-time operational limits.
- Compression vs. Accuracy - The reduction in size of updates achieved by adaptive model compression was almost 50 percent, where accuracy loss was into 0.5 percent.

These results show that the developed BFL framework has met the privacy, efficiency, and accuracy balance that can be used in latency-sensitive deployments of smart cities.

Table 3. Security Threat Mitigation Summary.

Threat	Description	Mitigation in Proposed BFL
Poisoning Attack	Insertion of malicious model updates to reduce quality.	Blockchain verification + Secure Aggregation prevent bad updates.
Replay Attack	Resubmission of outdated model updates to corrupt aggregation.	Blockchain timestamps and logs reject outdated updates.
Sybil Attack	Generating fake identities in order to manipulate model training.	PoA consensus restricts to authorized validators.

6.3 Security Analysis

An overall security assessment was carried out to determine strength resiliency towards common adversarial threats:

- Poisoning Attacks This strategy was effective in poisoning attacks, where model verification in our secure aggregation protocol blocked and prevented the use of corrupted updates (and associated, massive accuracy degradation) proposed in Vanilla FL (15%), mainly via blockchain-based response models.
- Replay Attacks: Blockchain accounted for the immutable ledger and timestamping functions so that replayed or stale model updates were not accepted and only the latest contributions could be incorporated.
- Sybil Attacks Attacks such as Sybil Attacks were mitigated by consensus again PoA whereby creation of fake identities were prevented because validators were needed to approve the creation of fake identities, which made adversarial control of networks far more difficult.

This result reaffirms that the BFL framework is well protected against model poisoning, replay, and identity-based attacks and that its performance overhead is acceptable.

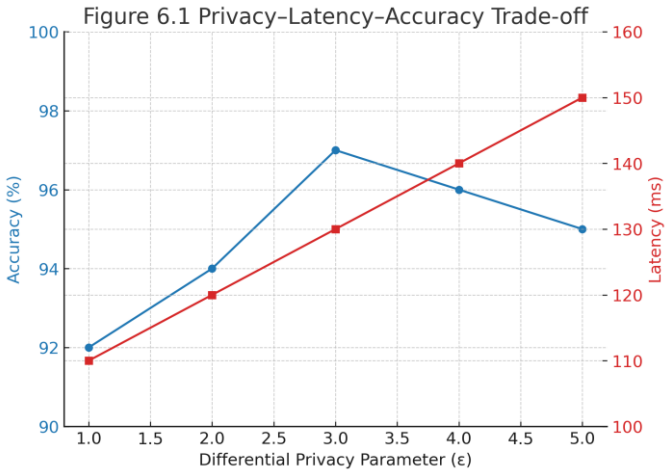

Figure 3. Privacy - Latency - Accuracy Trade-off.

7. Conclusion and Future Work

This study proposed a Blockchain-Integrated Federated Learning (BFL) framework for privacy-preserving and trustworthy AI in smart cities. The system of architecture interpolates the edge computing, Proof-of-Authority blockchain, and adaptive model compression to resolve the issues of privacy, trust, and efficiency of the multi-stakeholder urban environments. On the METR-LA traffic dataset, the results of this experiment proved that this framework gives equally accurate predictions as centralized models with 46.5 percent less communication cost and has low latency, appropriate in real-time trajectories. Security analysis verified resistance to poisoning, replay and Sybil attacks, which proves the relevance of the framework under adverse conditions.

The main contributions of this work include:

- The development of a hybrid BFL framework that is applicable in the context of smart cities.
- A lightweight PoA blockchain can be implemented with the goal of low-latency and tamper-proof aggregation.
- Using adaptive compression in reducing the cost of communication discouraging precision.
- Introducing a smart contract–driven incentive mechanism to encourage participation.

Future work will explore several directions:

- Generalizing the framework to multi-task federated learning by jointly predicting the three metrics of traffic, pollution, and energy demand.
- Incorporation of Zero-Knowledge Proofs (ZKPs) to advance further privacy and make no difference in accuracy.
- Scalability, resilience and cost-effectiveness on testing the system in production environment of a real-world smart city pilot project site.
- Researching energy-efficient blockchain consensus algorithms to limit the carbon expenditure of large scale-ups.

Overall, the suggested BFL framework offers a feasible, safe, and confidential answer to the AI-driven smart city services, opening the doors to data-driven sustainable urban intelligence.

REFERENCES

[1] K. Venigandla, N. Vemuri, and E. Nnamere Aneke, "Empowering Smart Cities with AI and RPA: Strategies for Intelligent Urban Management and Sustainable Development," int.jour.sci.res.mana, vol. 12, no. 04, pp. 1117–1125, Apr. 2024, doi: 10.18535/ijsrm/v12i04.ec02.

[2] J. R. Martinez-Mireles, M. A. Garcia-Marquez, A. Austria-Cornejo, R. A. Figueroa-Diaz, J. Rodriguez-Flores, and B. B. Garcia-Escorza, "Integrating AI in Green and Blue Infrastructure for Sustainable Smart Cities," Igi Global, 2025, pp. 337–364. doi: 10.4018/979-8-3693-8074-1.ch014.

[3] Matei and M. Cocoșatu, "Artificial Internet of Things, Sensor-Based Digital Twin Urban Computing Vision Algorithms, and Blockchain Cloud Networks in Sustainable Smart City Administration," Sustainability, vol. 16, no. 16, p. 6749, Aug. 2024, doi: 10.3390/su16166749.

[4] V. S. Barletta, D. Caivano, M. De Vincentiis, A. Pal, and M. Scalera, "Hybrid quantum architecture for smart city security," Journal of Systems and Software, vol. 217, p. 112161, July 2024, doi: 10.1016/j.jss.2024.112161.

[5] S. Farooq, B. Farooq, S. Basheer, and S. Walia, "Balancing Environmental Sustainability and Privacy Ethical Dilemmas in AI-Enabled Smart Cities," Igi Global, 2023, pp. 263–286. doi: 10.4018/979-8-3693-0892-9.ch013.

[6] E. Dritsas and M. Trigka, "Machine Learning for Blockchain and IoT Systems in Smart Cities: A Survey," Future Internet, vol. 16, no. 9, p. 324, Sept. 2024, doi: 10.3390/fi16090324.

[7] F. Javed, E. Zeydan, J. Mangues-Bafalluy, K. Dev, and L. Blanco, "Blockchain for Federated Learning in the Internet of Things: Trustworthy Adaptation, Standards, and the Road Ahead," Mar. 31, 2025. doi: 10.48550/arxiv.2503.23823.

[8] R. Alsabt, Y. A. Adenle, and H. M. Alshuwaikhat, "Exploring the Roles, Future Impacts, and Strategic Integration of Artificial Intelligence in the Optimization of Smart City—From Systematic Literature Review to Conceptual Model," Sustainability, vol. 16, no. 8, p. 3389, Apr. 2024, doi: 10.3390/su16083389.

[9] M. K. Singar, N. Saraswat, G. Shukla, and K. Suneetha, "Artificial Intelligence's Role in Shaping Renewable Energy for Next-Generation Smart Cities," E3S Web of Conf., vol. 540, p. 08014, Jan. 2024, doi: 10.1051/e3sconf/202454008014.

[10] Gomes, M. R. Karim, and N. M. Islam, "Data-Driven Environmental Risk Management and Sustainability Analytics," NHJ, vol. 1, no. 01, pp. 100–113, Oct. 2024, doi: 10.70008/jmldeds.v1i01.46.

[11] D. Gowri, D. Babu, D. Krishna, and D. Krishnaveni, "Enhancing Sustainability: Exploring IoT Integration in Renewable Energy Infrastructure," Int Res J Adv Engg Hub, vol. 2, no. 04, pp. 793–800, Apr. 2024, doi: 10.47392/irjaeh.2024.0111.

[12] X. Li, Y. An, Y. Hu, X. Xiao, J. Yang, and L. Zeng, "Blockchain-based federated learning approaches in internet of things applications," Security and Privacy, vol. 7, no. 6, June 2024, doi: 10.1002/spy2.435.

[13] Y. Zhang, B. Suleiman, M. J. Alibasa, and F. Farid, "Privacy-Aware Anomaly Detection in IoT Environments using FedGroup: A Group-Based Federated Learning Approach," J Netw Syst Manage, vol. 32, no. 1, Jan. 2024, doi: 10.1007/s10922-023-09782-9.

[14] J. Ahn, M. Kim, and E. Yi, "Blockchain Consensus Mechanisms: A Bibliometric Analysis (2014–2024) Using VOSviewer and R Bibliometrix," Information, vol. 15, no. 10, p. 644, Oct. 2024, doi: 10.3390/info15100644.

[15] Abellán Álvarez, V. Gramlich, and J. Sedlmeir, "Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake," Association for Computing Machinery, Apr. 2024, pp. 278–287. doi: 10.1145/3605098.3635970.

[16] Y. Qu et al., "Decentralized Privacy Using Blockchain-Enabled Federated Learning in Fog Computing," IEEE Internet Things J., vol. 7, no. 6, pp. 5171–5183, June 2020, doi: 10.1109/jiot.2020.2977383.

[17] X. Qu, Q. Hu, X. Cheng, and S. Wang, "Proof of Federated Learning: A Novel Energy-Recycling Consensus Algorithm," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 8, pp. 2074–2085, May 2020, doi: 10.1109/tpds.2021.3056773.

[18] Y. Lan, B. Li, Y. Liu, and C. Miao, "Proof of Learning (PoLe): Empowering Machine Learning with Consensus Building on Blockchains (Demo)," AAAI, vol. 35, no. 18, pp. 16063–16066, May 2021, doi: 10.1609/aaai.v35i18.18013.

[19] Wahrstätter, S. Khan, and D. Svetinovic, "OpenFL: A scalable and secure decentralized federated learning system on the Ethereum blockchain," Internet of Things, vol. 26, p. 101174, Mar. 2024, doi: 10.1016/j.iot.2024.101174.

[20] S. Srinivasan, "A Novel Approach Integrating IoT and WSN with Predictive Modeling and Optimization for Enhancing Efficiency and Sustainability in Smart Cities," jes, vol. 20, no. 4s, pp. 2228–2237, Apr. 2024, doi: 10.52783/jes.2393.

[21] V. Choudhary, H. B. Lim, J. H. Teh, and V. Beltran, "AirQ: A Smart IoT Platform for Air Quality Monitoring," Institute Of Electrical Electronics Engineers, Jan. 2020, pp. 1–2. doi: 10.1109/ccnc46108.2020.9045550.

[22] X. Dong, W. Zhao, H. Zhang, H. Han, and Z. Zhu, "MTESformer: Multi-Scale Temporal and Enhance Spatial Transformer for Traffic Flow Prediction," IEEE Access, vol. 12, pp. 47231–47245, Jan. 2024, doi: 10.1109/access.2024.3381987.

[23] R. Jiang et al., "Spatio-Temporal Meta-Graph Learning for Traffic Forecasting," AAAI, vol. 37, no. 7, pp. 8078–8086, June 2023, doi: 10.1609/aaai.v37i7.25976.

[24] O. F. Isife, A. A. Vincent, R. E. Subair, M. E. Awomoyi, I. P. Okokpujie, and K. Okokpujie, "Development of a Malicious Network Traffic Intrusion Detection System Using Deep Learning," IJSSE, vol. 13, no. 4, pp. 587–595, Sept. 2023, doi: 10.18280/ijsse.130401.