Secure Federated Learning for Real-Time Cyber Threat Detection in EV Charging Infrastructures

Hamza Ibrahim [1], Love Allen Chijioke Ahakonye [2], Jae Min Lee [1], Dong-Seong Kim [1] [*]
[1] IT-Convergence Engineering, *Kumoh National Institute of Technology*, Gumi, South Korea
[*] NSLab Co. Ltd., Gumi, South Korea, *Kumoh National Institute of Technology*, Gumi, South Korea
[2] ICT Convergence Research Center, *Kumoh National of Technology*, Gumi, South Korea
(hamza, loveahakonye, ljmpaul, dskim)@kumoh.ac.kr

***Abstract*—Decentralized electric vehicle (EV) charging stations face critical cybersecurity challenges that demand real-time, privacy-preserving threat detection. Traditional centralized monitoring and standard AI models are unsuitable for constrained EVSE nodes. This work introduces a federated learning framework combined with PureChain, a Proof of Authority and Association (PoA^2) blockchain-based consensus mechanisms enabling secure aggregation of local models, authenticated updates, and minimal computational overhead. Using a 1-dimensional Convolutional neural network for detection, the system achieves 98.97% accuracy with low latency (7.99s/round). PureChain enforces verifiable trust via validators, and the framework delivers scalable, real-time security. Future enhancements include explainable AI and optimization for 6G and Multi-Access Edge Computing deployment.**

***Index Terms*—Electric Vehicle (EV) Charging Security, Real-Time Cyber Threat Detection, PureChain, PoA^2 Consensus Mechanism**

I. Introduction

Electric Vehicle Supply Equipment (EVSE) is central to the adoption of electric vehicles, yet the growing interconnectivity and decentralization of EVSE networks introduce significant cybersecurity risks [1]. Threats such as false data injection, malware, and man-in-the-middle attacks require robust, scalable, and real-time security mechanisms [2], [3]. Traditional centralized intrusion detection systems (IDS) face challenges including latency, scalability limits, and privacy risks [4], highlighting the need for adaptive, decentralized security approaches that leverage emerging artificial intelligence (AI) trends [5].

Federated learning (FL) addresses these issues by allowing distributed EVSE nodes to collaboratively train models without centralizing raw data [6], lowering network overhead and enhancing data privacy [7]. Although FL preserves privacy, it exposes vulnerabilities in trust and model integrity, as the central server remains prone to poisoning and compromise [8]. Blockchain offers a verifiable and tamper-proof alternative [9], [10], yet classical consensus mechanisms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) incur heavy computational costs, and Proof-of-authority (PoA) risks centralization [11], [12]. PureChain, implemented using the Proof of Authority and Association (PoA^2) consensus, ensures authenticated updates, deterministic finality, and efficient validation via trusted nodes, achieving an optimal balance of decentralization, scalability, and trust [13]. Performance evaluation by the Author in [14] demonstrated that PureChain outperforms traditional blockchain frameworks like Ethereum and Hyperledger, achieving a 230% increase in throughput, a 70% reduction in latency, and improved scalability, while PoA^2 concurrently strengthens real-time intrusion detection.

Thus, as the author in [3] demonstrated the effectiveness of FL for EVSE security, the integration of blockchain to secure the full FL workflow and a systematic comparison of neural network performance under constrained conditions remain largely unaddressed [15]. These gaps are particularly pressing in real-time EVSE applications, where efficiency and latency are critical. This study proposes a unified federated AI and PureChain a custom blockcahin framework to achieve decentralized, privacy-preserving, and verifiable threat detection with real-time operation. The main contributions are threefold:

1) We propose a unified framework combining Federated Learning with the PoA^2-based PureChain blockchain is introduced to preserve data privacy and establish decentralized trust through secure, auditable model aggregation.
2) We implement and comparatively evaluate CNN, LSTM, and CNN-LSTM architectures within this framework identifies CNN as the optimal model for EVSE systems, achieving superior accuracy and low latency.
3) We demonstrate how the PoA^2 consensus mechanism is shown to secure and accelerate federated updates, ensuring tamper-resistant validation and scalable decentralized coordination across participating nodes.

The remainder of this article is organized as follows: following Section I, the background and related work are presented in Section II. Section III describes the proposed framework in detail. The experimental results and their analysis are discussed in Section IV. Finally, Section V concludes the paper and outlines the directions for future research.

II. Background and Related Work

Federated Learning (FL) has become a key approach to collaborative intelligence to preserve privacy, enabling model training on distributed nodes without sharing raw data [13]. This not only improves data privacy, but also reduces network bandwidth usage [19], making it ideal for sensitive decentralized environments such as smart infrastructure. In the automo-

TABLE I: Summary of Relevant Studies on Federated Learning and Blockchain for Cybersecurity

Ref.	FL	BC	AI Model	Domain	RT	Key Contribution	Identified Limitation / Gap
[3]	✓	×	Multimodal	EVSE	✓	High-accuracy FL-based IDS using multimodal data	Centralized aggregator; no integrity checks for model updates
[16]	✓	×	FL	EVSE (OCPP)	✓	FL-based detection of protocol-level attacks	No decentralized trust mechanism
[6]	✓	×	KNN, RF, SVM	EVSE	✓	FL-based anomaly detection for EVCS	No blockchain; central aggregator risks remain
[17]	✓	✓	SVM, DT, NN, RF	Vehicular (VANETs)	✓	Hybrid FL-BC for intrusion detection	Aggregation remains centralized; partial decentralization
[18]	✓	✓	✗	Vehicular	✓	Robust FL-BC under adversarial noise	Not optimized for low-latency EVSE environments
Proposed	✓	✓	**CNN, LSTM, CNN-LSTM**	**EVSE**	✓	**Decentralized FL with PureChain; CNN optimized for latency.**	**Full decentralization; real-time validation; low latency & compact model**

FL: Federated Learning, BC: Blockchain, RT: Real-Time Focus/Eval, OCPP: Open Charge Point Protocol, VANETs: Vehicular Ad-hoc Networks

tive sector, FL shows great promise, particularly in improving cybersecurity in connected and autonomous vehicles (CAVs), especially intrusion detection systems [20]. The application of FL in EV charging security is also noteworthy. For instance, in the EVSE domain, FL has demonstrated strong performance, with Rahal et al. [3] achieving over 98% accuracy using multimodal telemetry, and Dalamagkas et al. [16] effectively detecting protocol-level attacks on OCPP 1.6. However, FL's reliance on a central aggregator introduces vulnerabilities, which prompts researchers to explore blockchain integration for decentralized trust [21], [22]. While some works, such as Purohit and Govindarasu [6], focus solely on FL, others such as Malik et al. [17] and Almaghthawi et al. [23] propose hybrid FL-Blockchain frameworks, although often with centralized components or lacking real-time validation. Sultana et al. [18] highlight robustness under adversarial conditions, but do not address EVSE-specific constraints.

A. Research Gap and Motivation

A critical review of the literature reveals a gap between conceptual frameworks and practical deployment in real-time cyber-physical systems, particularly regarding (1) decentralized trust for FL aggregation, (2) lightweight blockchain consensus suitable for low-latency environments such as EVSEs, and (3) systematic evaluation of modern deep learning models within a federated-blockchain context for informed model selection. To address these gaps, this study integrates FL with PureChain, a custom permissioned blockchain using PoA^2 consensus, enabling secure, low-latency aggregation and high throughput, while benchmarking CNN, LSTM, and CNN-LSTM models to assess accuracy, latency, and computational efficiency, establishing the first AI-driven blockchain solution for EV charging infrastructure. To the best of our knowledge, this study is the first to integrate FL with PureChain, offering an AI-driven security solution tailored for EV charging infrastructures. Key related works and their contributions are summarized in Table I.

III. System Methodology

The proposed framework, shown in Figure 1, creates a secure and decentralized cyber-threat detection system for EVSE infrastructures. It combines FL and PureChain blockchain to ensure privacy and trust. FL keeps data local to each EVSE node, while PureChain secures model aggregation. Each node trains its own AI model, and updates are sent to the blockchain network for validation through the PoA^2 consensus. After consensus, a new global model is formed and distributed to the nodes, ensuring tamper-proof evolution and eliminating single points of failure.

A. Federated Learning Phase

Each EVSE node k has a local dataset D_k. In each round t, the node performs local training on D_k to minimize its loss function L_k, updating model weights via stochastic gradient descent$w_{k,t+1} = w_{k,t} - \eta \nabla L_k(w_{k,t})$. The central orchestrator collects these updates, but unlike traditional FL, it does not immediately compute the global model. Instead, it first proposes a set of updates for aggregation, with federated averaging as shown in Equation 1.

$$w_t = \frac{1}{K} \sum_{k=1}^{K} n_k \cdot w_{k,t} \tag{1}$$

where K is the total number of nodes and n_k is the number of samples at node k. This aggregation is conditional upon validation by the PureChain network, as described in Section III-C.

B. AI-Based Detection Engine Phase

The anomaly detection engine operates at the edge using the latest global model w_t. It processes multivariate time-series telemetry data X (e.g., power readings, network traffic statistics). The model computes output probabilities as $\hat{y} = \text{softmax}\big(f(X; w_t)\big)$, where f is the forward pass of the chosen neural architecture. A classification of "anomaly" triggers an immediate local alert and may invoke a smart contract on PureChain to log the event immutably and notify the network. The 1D Convolutional Neural Network (1D-CNN) employs a hierarchical feature extraction process through sequential convolutional operations. The architecture begins with a first convolutional layer applying 32 filters with a kernel size of 3, performing the operation in $Y_1 = \sigma(X * W_1 + b_1)$, where $X \in \mathbb{R}^{L \times D}$ is the input multivariate time-series of length L with D features, $W_1 \in \mathbb{R}^{3 \times D \times 32}$ represents the learnable kernel weights, $*$ denotes the 1D cross-correlation (convolution) operation, b_1 is the bias vector, σ is the ReLU activation

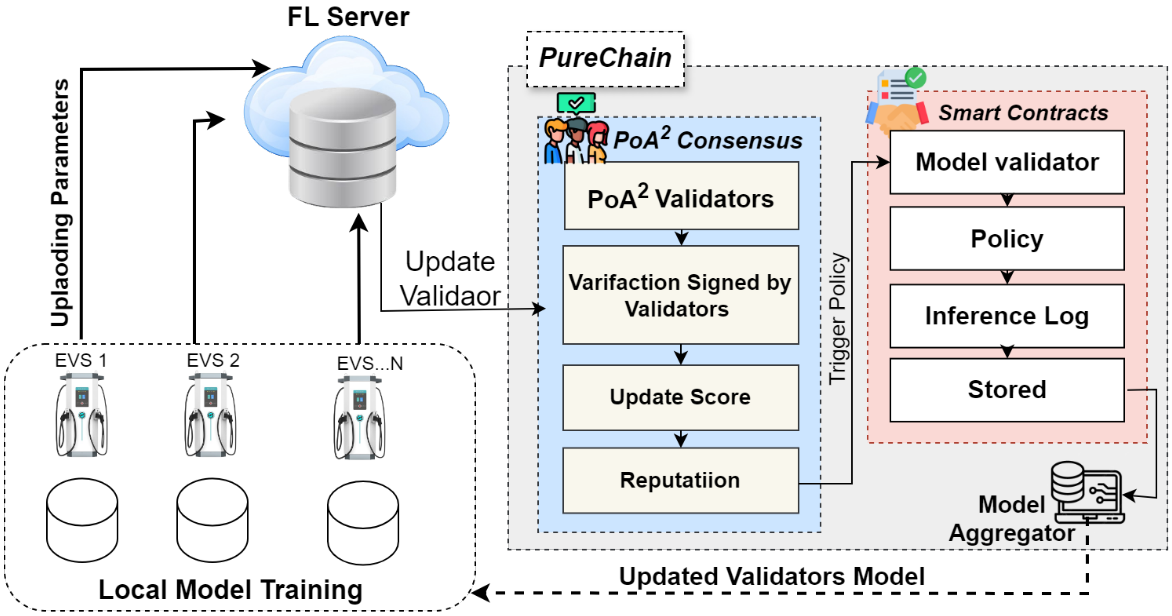

Fig. 1: Illustration of the proposed framework for secure and decentralized cyber threat detection in EVSE infrastructures.

Algorithm 1: Federated Learning with AI Model Training

```
Require: Local datasets $D_i$ for each node $i \in [1, N]$,
         initial model $w_0$
Ensure : Final global model $w_T$
for $t = 1$ to $T$ do
    Server broadcasts current global model $w_t$ to all
     EVSE nodes;
    for $i \in [1, N]$ do
        Compute gradient $\nabla L_i(w_t)$ on local data $D_i$;
        Update local model: $w_i^{(t+1)} = w_t - \eta \nabla L_i(w_t)$;
        Submit local model $w_i^{(t+1)}$ to PureChain for
         validation ;          // Key Integration
         Point
    Aggregator proposes model aggregation to
     PureChain validators;
    Await consensus approval from PureChain;
    Upon approval, compute and distribute new
     global model: $w_{t+1} = \frac{1}{N} \sum_{i=1}^{N} w_i^{(t+1)}$;
```

function, defined as $\sigma(x) = \max(0, x)$, introducing non-linearity. The output Y_1 passes through a second convolutional layer with 64 filters ($W_2 \in \mathbb{R}^{3\times32\times64}$), producing feature maps Y_2. A subsequent 1D max-pooling layer with pool size 2 performs down-sampling via $\text{MaxPool}(Y_2)[i] = \max(Y_2[2i : 2i + 2])$ reducing spatial dimensionality while retaining the most salient features. This architecture is particularly effective for capturing local, translation-invariant temporal motifs in EVSE telemetry data, such as short-duration power surges or specific network traffic bursts indicative of cyber threats. The final stages consist of two fully connected layers that perform non-linear transformations on the flattened feature vectors for final classification.

C. Blockchain Integration via PureChain Phase

This phase is the core of our trust decentralization mechanism. PureChain, a custom permissioned blockchain using the PoA^2 consensus mechanism, actively secures the FL workflow. A validator v is selected to participate in a consensus round based on a composite score as $\text{Select}(v) \Leftrightarrow (R_v \cdot Q_v) > \theta$, where R_v is the historical reputation, Q_v is the reliability of its past model validations, and θ is a threshold. The aggregator's request to compute a new global model is treated as a transaction. A smart contract governs this process, verifying as $\text{Valid}(u) \Leftrightarrow \text{CheckIntegrity}(u) \wedge \text{CheckAuth}(v)$. This ensures model updates are unaltered and originate from authorized nodes. The selected validators run the consensus protocol (Algorithm 2). Upon successful consensus, the new global model's hash and metadata are immutably recorded in a block B_t, with state transition as $S_{t+1} = H(S_t \parallel B_t)$, where H is a cryptographic hash function. This provides a tamper-proof audit trail for the model's entire evolution.

IV. Experimentation and Result Discussion

A. Dataset Description

In this study, we uses the EVSE-CIC-2024 dataset [24] to evaluate the proposed framework. The dataset is a comprehensive 36 GB collection that combines power consumption data, network traffic (OCPP and ISO15118 protocols), and approximately 900 hardware performance counters, captured under both normal and attack conditions. The attack scenarios include reconnaissance, flooding, port scans, cryptojacking,

Algorithm 2: PureChain Consensus for Secure Model Aggregation

```
textbf() 1em
Input: Validator nodes $V$, proposed model updates $U_t$,
       reputation scores $R$
Output: $w_{t+1}$ is approved or rejected
Aggregator computes $w_{t+1}$ from $U_t$;
for each $v_k \in V$ do
    Score$(v_k) = R_k \cdot Q_k$;
Select committee: Score$(v_k) \geq \tau$;
Broadcast $w_{t+1}, H(U_t)$;
Verify: Integrity, Authorization, Soundness;
if $\geq 2/3$ votes accept then
    Form $B_t$, append to PureChain;
    Update $R_k, Q_k$;
else
    Reject $w_{t+1}$, dispute, penalize;
```

and backdoor intrusions, making it highly suitable for developing real-time anomaly detection systems. The data were normalized, and categorical features were encoded. To create a realistic FL environment, the dataset was partitioned across $K = 10$ simulated EVSE nodes. The data was distributed in an Independent and Identically Distributed (IID) manner to establish a baseline performance. A sliding window of 10 timesteps with a stride of 1 were used to create sequential samples, ensuring consistency in AI models. The experiments were conducted in Python on a Google Colab environment with a 6th Gen Intel(R) Core(TM) i5-6300U processor and 4 GB of RAM. The FL process was simulated over $T = 5$ communication rounds. The PureChain consensus and ledger, were simulated using a custom Python class to model the overhead of cryptographic hashing, validator voting, and block commitment during each aggregation round.

B. Model Performance

TABLE II: Comparison of Model Performance Metrics

Model	Accuracy	Latency (s)	Throughput	Scalability
CNN	98.97%	7.9856	0.4102	0.048897
LSTM	59.18%	60.9486	0.0497	0.000657
CNN+LSTM	74.60%	89.8028	0.0339	0.000126

The performance of the three AI models within the federated-PureChain framework is summarized in Table II. The metrics are defined as follows: **Latency** is the total time per FL communication round (local training, communication, and PureChain consensus); **Throughput** is the number of model updates processed per second at the aggregator-PureChain interface; and **Scalability** is a composite score calculated in Equation 2.

$$\text{Scalability} = \frac{\text{Accuracy}}{\text{Latency} \times \text{Model Size}} \tag{2}$$

providing a measure of efficiency under constrained resources. The CNN model demonstrated superior performance across all key metrics. It achieved the highest accuracy (98.97%) and the lowest latency (7.99 s/round), resulting in a throughput of 0.4102 updates/s, which is an order of magnitude higher than the LSTM and CNN-LSTM models. Consequently, its scalability score (0.048897) was significantly higher, underscoring its suitability for a distributed environment with limited resources. Figure 2 shows the five-round communication process, where the CNN model reached 98.97% final accuracy, outperforming the CNN+LSTM hybrid 74.60% and LSTM 59.18%. With more than 94% accuracy in Round 1 and a 39.79% margin above LSTM and 24.37% above hybrid CNN+LSTM, CNN exhibited faster convergence and stronger FL capability.

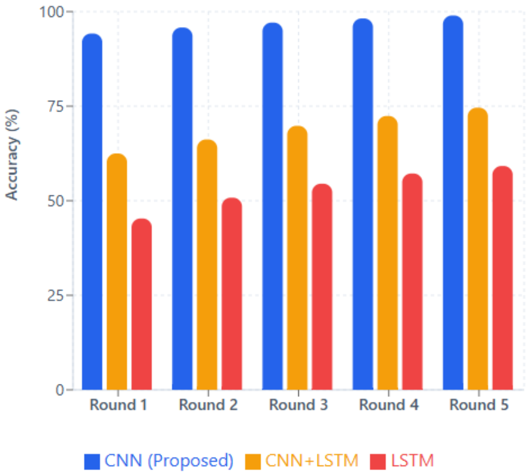

Fig. 2: Progression of accuracy over five FL rounds.

TABLE III: Model Efficiency

Model	Inference Time (s)	Training Time (s)	Model Size (MB)
CNN	0.000102	312.5	2.3
LSTM	0.000283	721.3	6.8
CNN+LSTM	0.000177	869.7	8.5

A deeper analysis of computational efficiency, shown in Table III, reinforces CNN's advantages. The CNN model not only has the fastest inference time (0.000102 seconds) but also the shortest training time and the most compact size (2.3 MB). In contrast, the LSTM and CNN-LSTM models, with their larger parameter counts and complex gating mechanisms, incur significantly higher training costs and memory footprints, rendering them impractical for deployment on typical EVSE edge hardware. Table IV highlights that most prior works lack decentralized trust or real-time validation, relying on centralized aggregators. Our proposed CNN with PureChain stands out with 98.97% accuracy, low latency (7.99s/round), and efficient resource usage (CPU 2.07%, 64MB RAM). It also achieves full decentralization using PoA^2 consensus and supports real-time threat detection. This positions our system as a robust and scalable solution for secure EVSE environments.

TABLE IV: Comparative performance

Ref.	Accuracy (%)	Scalability	Efficiency	Mitigation / Latency	Real-Time
[3]	>98%	Not reported	Not reported	Centralized aggregator; no integrity checks	Partial
[6]	N/S	Not reported	Not reported	Optimized processing speed	Partial
[16]	N/S	Not reported	Not reported	Protocol-level detection only	Yes
[17]	N/S	Partial decentralization	Not reported	Centralized aggregation remains	Yes
[18]	N/S	Not reported	Not reported	Robust under noise; not EVSE-specific	Yes
Proposed	**98.97%**	**0.048897 (Scalability Score)**	**CPU 2.07%; Mem 64 MB; Power 1.85 W**	**Latency: 7.99s/round; Inference: 0.000102s**	**Yes**

V. Conclusion

This paper presented a secure federated AI–blockchain framework that combines FL with the PureChain blockchain with a consensus mechanism based on PoA^2 to secure smart EV charging stations. The system protects data privacy at local EVSE nodes and ensures decentralized trust through verified, immutable aggregation. Experiments on the EVSE-CIC-2024 dataset identified CNN as the best-performing model, achieving 98.97% accuracy with 7.99-second latency per round and 0.000102-second inference time. LSTM variants showed higher delay and computational demand. The framework delivers a scalable and tamper-resistant defense for EVSE infrastructure. Future directions include real testbed deployment, XAI-based model interpretation, and optimization for 6G/Multi-Access Edge Computing environments to improve real-time efficiency and compatibility with legacy systems.

Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the IITP grant funded by the Korea government(MSIT) (IITP-2026-RS-2020-II201612, 33%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 33%) and by the MSIT, Korea, under the ITRC support program(IITP-2026-RS-2024-00438430, 34%).

References

[1] M. Sampson, R. Varriale, M. A. Jaynes, W. Rossow, and D. S. Dobrzynski, "EVs@ Scale-Addressing Cybersecurity Risks Between EVSE and Charge Point Management Systems," Argonne National Laboratory (ANL), Argonne, IL (United States), Tech. Rep., 2024.

[2] S. Hamdare, O. Kaiwartya, M. Aljaidi, M. Jugran, Y. Cao, S. Kumar, M. Mahmud, D. Brown, and J. Lloret, "Cybersecurity Risk Analysis of Electric Vehicles Charging Stations," *Sensors*, vol. 23, no. 15, 2023.

[3] R. Rahal, A. A. Korba, and Y. Ghamri-Doudane, "Fuse and Federate: Enhancing EV Charging Station Security with Multimodal Fusion and Federated Learning," 2025.

[4] Z. U. I. Nasir, A. Iqbal, and H. K. Qureshi, "Securing Cyber-Physical Systems: A Decentralized Framework for Collaborative Intrusion Detection with Privacy Preservation," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 2, pp. 303–311, 2024.

[5] U. A. Bukar, H. Ibrahim, and B. S. Yahaya, "Charting the Future of AI in the Next Decade: Emerging Trends and Conclusions," *The Smart Life Revolution*, pp. 245–263, 2025.

[6] S. Purohit and M. Govindarasu, "FL-EVCS: Federated Learning Based Anomaly Detection For EV Charging Ecosystem," in *2024 33rd International Conference on Computer Communications and Networks (ICCCN)*, 2024, pp. 1–9.

[7] A. Ali, H. Jianjun, and A. Jabbar, "Recent Advances in Federated Learning for Connected Autonomous Vehicles: Addressing Privacy, Performance, and Scalability Challenges," *IEEE Access*, vol. 13, pp. 80 637–80 665, 2025.

[8] A. Sharma and N. Marchang, "A Review on client-Server Attacks and Defenses in Federated Learning," *Computers & Security*, vol. 140, p. 103801, 2024.

[9] H. Ibrahim, J. Kim, and U. A. Bukar, "Leveraging Blockchain Technology for Trustworthy Information Dissemination in Nigerian Networks," *The Journal of Contents Computing*, vol. 5, no. 2, pp. 727–753, 2023.

[10] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of Blockchain in IoT Cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, 2024.

[11] K. Wimal and G. Liyanage, "A Truly Decentralized Blockchain Consensus Protocol that Avoids Concentration of Power," in *2023 IEEE 17th International Conference on Industrial and Information Systems (ICIIS)*, 2023, pp. 1–6.

[12] M. M. Islam, M. M. Merlec, and H. P. IN, "Proof of Random Leader: A Fast and Manipulation-Resistant Proof-of-Authority Consensus Algorithm for Permissioned Blockchains Using Verifiable Random Function," *IEEE Transactions on Services Computing*, vol. 18, no. 3, pp. 1655–1668, 2025.

[13] L. A. C. Ahakonye, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "Purechain-Enhanced Federated Learning for Dynamic Fault Tolerance and Attack Detection in Distributed Systems," *High-Confidence Computing*, p. 100354, 2025.

[14] H. Ibrahim, K. J. Mukisa, L. A. C. Ahakonye, J. M. Lee, and D.-S. Kim, "Impact of PureChain for Secure and Scalable Cybersecurity in Resource-Constrained IIoT," in *Proceedings of the 35th Joint Conference on Communications and Information (JCCI 2025)*, April 2025.

[15] A. A. Ahmed and O. O. Alabi, "Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review," *IEEE Access*, vol. 12, pp. 102 219–102 241, 2024.

[16] C. Dalamagkas, P. Radoglou-Grammatikis, P. Bouzinis, I. Papadopoulos, T. Lagkas, V. Argyriou, S. Goudos, D. Margounakis, E. Fountoukidis, and P. Sarigiannidis, "Federated Detection of Open Charge Point Protocol 1.6 Cyberattacks," *Complex Engineering Systems*, vol. 5, no. 2, 2025.

[17] J. Malik, "Next-Generation Protection: Leveraging Federated Learning and Blockchain for Intrusion Detection in Smart Vehicle Network," *Power System Technology*, vol. 48, pp. 931–952, 05 2024.

[18] S. Sultana, J. Hossain, M. Billah, H. H. Shajeeb, S. Rahman, K. Ansari, and K. F. Hasan, "Blockchain-Enabled Federated Learning Approach for Vehicular Networks," *arXiv preprint arXiv:2311.06372*, 2023.

[19] K. Lazaros, D. E. Koumadorakis, A. G. Vrahatis, and S. Kotsiantis, "Federated Learning: Navigating the Landscape of Collaborative Intelligence," *Electronics*, vol. 13, no. 23, p. 4744, 2024.

[20] J. Ahmad, M. U. Zia, I. H. Naqvi, J. N. Chattha, F. A. Butt, T. Huang, and W. Xiang, "Machine learning and Blockchain Technologies for Cybersecurity in Connected Vehicles," *Wiley interdisciplinary reviews: data mining and knowledge discovery*, vol. 14, no. 1, p. e1515, 2024.

[21] 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," 2025.

[22] I. B. Ababio, J. Bieniek, M. Rahouti, T. Hayajneh, M. Aledhari, D. C. Verma, and A. Chehri, "A Blockchain-Assisted Federated Learning Framework for Secure and Self-Optimizing Digital Twins in Industrial IoT," *Future Internet*, vol. 17, no. 1, p. 13, 2025.

[23] A. Almaghthawi, E. A. A. Ghaleb, N. A. Akbar, L. Asiri, M. Alrehaili, and A. Altalidi, "Federated-Learning Intrusion Detection System Based Blockchain Technology," *International Journal of Online & Biomedical Engineering*, vol. 20, no. 11, p. 16–30, 2024.

[24] E. D. Buedi, A. A. Ghorbani, S. Dadkhah, and R. L. Ferreira, "Enhancing EV Charging Station Security Using a Multi-dimensional Dataset: Cicevse2024," in *Data and Applications Security and Privacy XXXVIII*, A. L. Ferrara and R. Krishnan, Eds. Cham: Springer Nature Switzerland, 2024, pp. 171–190.