Synergistic Smart Grid: Instability and Fault Detection using Blockchain and Federated Learning

Kalibbala Jonathan Mukisa [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
(kjonmukisa, loveahakonye, ljmpaul, dskim,)@kumoh.ac.kr

2025 Sixteenth International Conference on Ubiquitous and Future Networks (ICUFN) | 979-8-3315-2487-6/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICUFN65838.2025.11170004

***Abstract*—Smart grids have revolutionized energy management by integrating IoT, allowing real-time monitoring and optimization. However, this connectivity also increases vulnerability to cyber threats. We propose an innovative solution that combines federated learning with a customized *IoT-PureChain* network to enhance fault detection and grid stability. Utilizing a hybrid model with LSTM and dense layers tailored for decentralized IoT data, our approach leverages two key datasets for fault simulation and stability analysis. We address non-IID data challenges by employing a trimmed mean aggregation, enhancing robustness and accuracy. Our blockchain, designed for IoT, uses a Proof-of-Authority with Association consensus and adaptive mining for high-efficiency, gas-free transactions. This research demonstrates a scalable, secure, privacy-focused system and paves the way for further exploration in IoT blockchain synergy and advanced federated learning.**

***Index Terms*—Smart-grid, PureChain, POA^2, Blockchain, Fault detection, Federated Learning, Trimmed Mean Aggregation,**

I. Introduction

Smart grids demand scalable, secure, and efficient fault detection systems as grid complexity and data volume increase [1]. Conventional centralized monitoring systems face challenges with scalability, privacy, and cyber threats, especially when managing sensitive data from interconnected devices. Figure 1 highlights the integrated components of a smart grid that ensure efficient energy distribution, enhanced reliability, support for renewable energy integration, and demand-side management [1].

This study integrates federated learning with a custom blockchain network, *IoT-PureChain*, and an SQL database to enhance fault detection reliability. Federated learning enables collaborative anomaly detection across energy nodes while preserving data privacy [2]. Unlike federated averaging, which struggles with non-IID data [3], this study employs a trimmed mean aggregation method [4] to mitigate outliers and malicious data, improving robustness in heterogeneous smart grid environments.

Blockchain ensures data security through cryptographic immutability, while SQL handles complex real-time queries for fault analysis [5]. Inspired by the study in [6], this system combines blockchain and SQL, leveraging SQLite's deterministic concurrency control [7] to achieve high throughput and minimize conflicts. This synergistic approach addresses the limitations of centralized systems, providing a scalable, decentralized solution for smart grid fault detection.

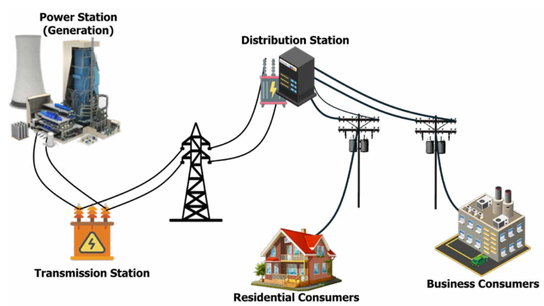

Fig. 1: Components of the smart grid

Concerning the recent research, this paper aims to contribute the following:

- Developing a custom blockchain network known as *IoT-PureChain* exceptionally for Internet of Things networks such as scalable smart grids combined with SQL database for complex queries. The blockchain utilizes automated mining to ensure faster transactions alongside proof of authority and association. (**POA**^{2}) consensus mechanism [8].
- Design a decentralized web platform for managing the nodes on the smart grid for handling the collaborative, decentralized learning of the data centers in the smart grid.
- Implement a hybrid deep learning model for effectively detecting instabilities and faults in decentralized smart grids.

The remainder of this paper is structured as follows: Section II reviews the background and related literature on smart grids, federated learning, and blockchain integration. Section III presents the proposed IoT-PureChain framework, system architecture, and federated learning setup. Section IV discusses the experimental setup, datasets, and evaluates performance through precision, recall, and latency analysis. Section V concludes the paper with key findings and directions for future research.

II. Background of Study and Related Works

Integrating IoT into smart grids has transformed energy management systems by enabling real-time data collection and control via smart meters, sensors, and actuators, enhancing monitoring and operational efficiency. Saleha [9] highlights how IoT supports advanced metering infrastructure, demand response, and distributed energy resource management to improve grid stability and energy distribution. Kirmani [10] further emphasizes IoT's role in fault detection through continuous data streams, enabling faster responses to grid anomalies while identifying challenges in managing the vast data volume and ensuring security and privacy.

Federated learning offers a privacy-preserving solution for training models across distributed data sources. As noted in [11], it enables collaborative fault detection model training without sharing raw data, which is crucial for building robust global anomaly detection systems. However, federated learning in smart grids struggles with non-IID data, which can bias models [12]. Our approach mitigates this by incorporating trimmed mean aggregation, reducing outlier influence for more accurate global models.

Blockchain technology addresses security and transparency in smart grid operations. Liu et al. [13] discussed how blockchain could secure federated learning updates through immutable verification, preventing tampering and unauthorized changes. Zheng, Z. et al. [14] pointed out significant limitations in scalability with existing blockchain networks when applied to IoT in smart grids. However, scalability issues with networks like Ethereum and Hyperledger impede real-time IoT applications. To overcome this, we propose a scalable blockchain network optimized for smart grid demands, incorporating auto-mining technology to adjust transaction processing for reduced latency [15] dynamically.

McMahan et al. [16] pioneered federated learning frameworks but did not fully address data heterogeneity challenges in smart grids. Our methodology improves robustness through trimmed mean aggregation, ensuring that fault detection models perform reliably across diverse grid conditions.

In summary, while IoT, federated learning, and blockchain offer transformative potential for smart grid management, they face scalability, data heterogeneity, and real-time processing challenges. Our research customizes these technologies to address these limitations, providing a synergistic solution that enhances efficiency, security, and reliability in fault detection and energy management systems.

III. Overall Proposed System Architecture

A. Overview of the system

Figure 2 represents a smart grid architecture leveraging a custom private blockchain, IoT-PureChain, a blockchain that is tailored for IoT applications in smart grids. This blockchain is the foundation for decentralized, secure, efficient fault and instability detection across substations. SQLite database was employed in the experimental setup to validate system functionality due to its lightweight and self-contained nature [7]. In this architecture, data centers collect and process transmission data from diverse grid loads, including commercial, industrial, residential, and agricultural sectors. Each data center, connected to the blockchain, operates as an independent node, ensuring secure and decentralized data management. Local fault detection and instability analysis are performed at these centers, with results transmitted as model updates to the *IoT-PureChain* and a central data center.

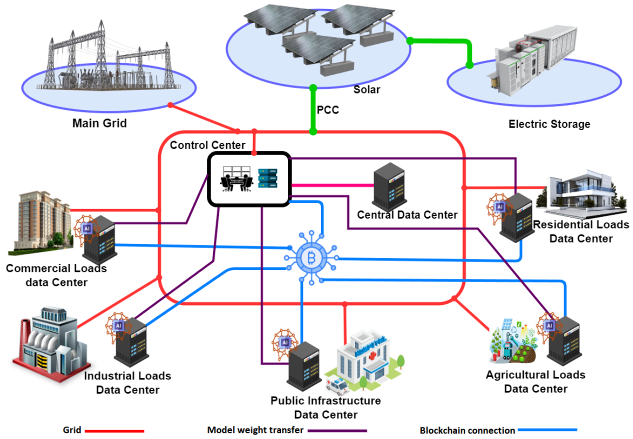

Fig. 2: Proposed System Architecture

The central data center aggregates updates using the trimmed mean method [4], which trims extreme values to enhance the robustness of the global fault detection model against anomalies or malicious inputs. The blockchain secures this process as an immutable ledger, recording transactions and model contributions to ensure transparency and tamper-proof operations. Additionally, it facilitates decentralized authentication by permitting access to only authorized nodes and protects data integrity related to grid stability and health. This design enhances trust, security, and efficiency in smart grid operations.

The architecture ensures seamless communication across data, models, and energy flows. Federated learning pathways enable the exchange of fault detection model updates between data centers and the central node. In contrast, the blockchain pathways securely log these updates, maintaining transparency and process integrity. Energy flow channels demonstrate energy distribution from producers to consumers. The model access channels connect SQLite databases at data centers with the blockchain to retrieve and update the global fault detection model.

B. IoT-PureChain Framework

The IoT-PureChain architecture, shown in Figure 3, is organized into specialized modules for efficient functionality. The foundational Blockchain Module includes a block list for recording transactions, validation logic to ensure integrity, and a Genesis Block for initialization. The transaction module processes energy transactions with structured functions for accuracy and efficiency.

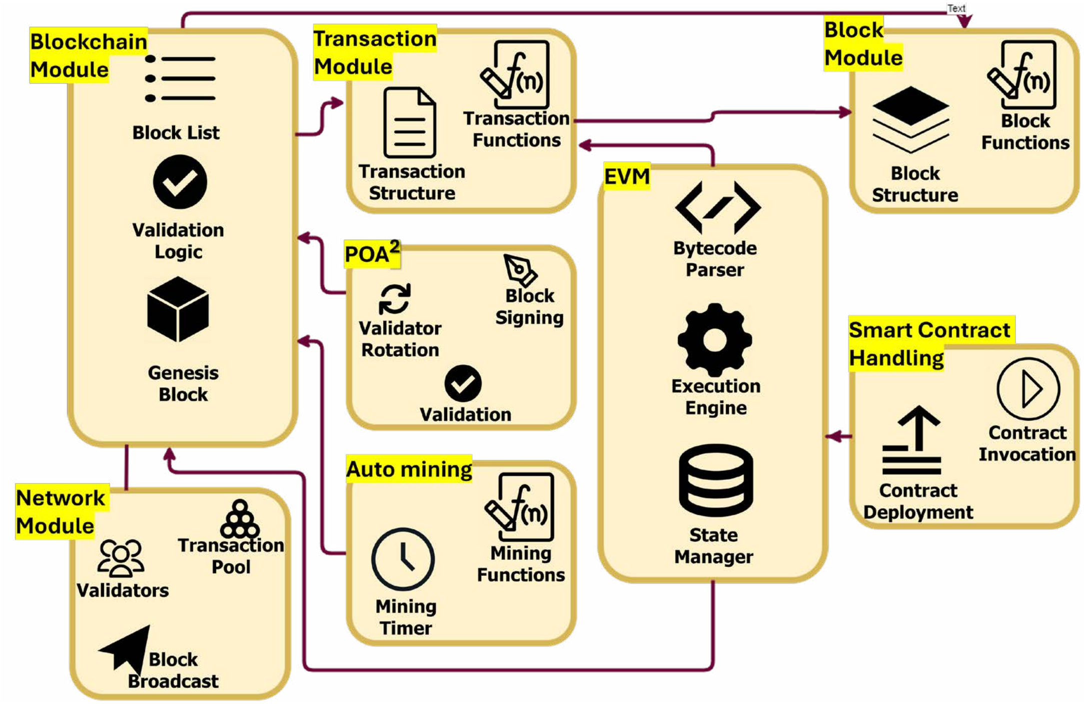

Fig. 3: Proposed IoT-PureChain Network

The **PoA**^{2} consensus employs pre-validated nodes participating in block creation through block validation. It utilizes an intelligent selection process that considers the node's historical performance, the node, the latency of the node concerning the validation process, and the node's availability, whether it is online or offline at the time of validation. This multi-factor tracking of nodes ensures that there are consistently available nodes to validate transactions, which is essential in our *IoT-PureChain* blockchain.

An auto-mining module optimizes the blockchain for IoT by dynamically adjusting mining intervals using a mining timer and tailoring mining functions for scalability. Equations 1 through 3 detail this process. This modular design enhances smart grid applications' scalability, efficiency, and security.

- Let I_b be the base interval in milliseconds, which is set initially as `baseInterval`.
- Let I_c be the current interval in milliseconds, initially set to I_b.

$$I_b = \texttt{baseInterval} \tag{1}$$

$$I_c(0) = I_b \tag{2}$$

- The adjustment of the block interval I_c at time step t can be described as a function of the system metrics at t:

$$I_c(t) = \begin{cases} I_b + 2000, & \text{if } U_{\text{cpu}}(t) > 80 \text{or} U_{\text{mem}}(t) > 80, \\ \max(I_b - 1000, 1000), & \text{if } U_{\text{cpu}}(t) < 20 \text{and} U_{\text{mem}}(t) < 20, \\ I_b, & \text{otherwise.} \end{cases} \tag{3}$$

Here, the function $\max(a, b)$ returns the maximum of a and b, ensuring that the interval does not exceed 1000 milliseconds.

The Network Module ensures efficient communication across nodes through Validators for transaction validation, a Transaction Pool for pending transactions, and Block Broadcast for maintaining a consistent ledger across the network.

C. Dataset Description

Our study utilizes two curated smart grid fault detection and stability analysis datasets. The first dataset, designed for multi-class classification, simulates transmission line faults with 42 features, including phase-wise line voltages and currents. Fault types are categorized into seven classes: No-Fault, Line-to-Line-to-Line (L-L-L), Line-to-Line-to-Line-to-Ground (L-L-L-G), Double Line-to-Ground (DLG), Line-to-Line (L-L), Single Line-to-Ground (SLG), and Line Fault, enabling precise fault scenario prediction. The second dataset, focusing on grid stability, contains 60,000 samples with 13 attributes and supports binary classification of stable versus unstable grid conditions. It provides critical insights for real-time monitoring and predictive maintenance. Both datasets are normalized using min-max scaling to ensure fair feature contribution and enhance the performance of machine learning models within the federated learning framework.

D. Federated Learning Setup

In the federated learning simulation, data is partitioned across smart grid data centers, with each local model using a hybrid deep learning framework combining LSTM networks and dense layers for sequential data analysis. The architecture incorporates Gaussian noise for robust input handling, LSTM layers with dropout to prevent overfitting, batch normalization for training stability, and dense layers with ReLU activation, concluding with a softmax layer for multi-class fault classification. Local models process IoT sensor data independently, preserving raw data privacy.

Model updates are securely transmitted to a coordinating server, where a trimmed mean aggregation technique filters and aggregates them into a global model, mitigating outlier or malicious data impacts. The *IoT-PureChain* network with **POA**^{2} consensus ensures tamper-proof transaction and authentication of nodes. SQL databases efficiently handle complex real-time queries, while a Python-based server-client architecture and SQLite database enable real-time training monitoring. All transactions are immutably logged on the blockchain and database, ensuring secure and transparent records of the training process.

E. Interface design

Figure 4 displays the web interface for managing FL nodes in the training process, offering tools to add or remove clients and secure the system from malicious nodes. Its semi-decentralized structure supports robust model development through dynamic node management. By integrating SQLite with blockchain, we achieve real-time analysis and secure logging, leveraging SQLite's efficient querying to enhance system responsiveness and integrity.

IV. Results and Performance Discussion

Table I summarizes the performance of the model training on two evaluated datasets. For the fault dataset, the model achieves a precision score of 0.8981 and a recall score of 0.9150. The F1 score is 0.8987, reflecting a balanced performance with an effective trade-off between false positives and false negatives. For dataset two, the precision score reaches 0.9776, and 0.9774 recall score. The F1 score of 0.9775 demonstrates notable accuracy and robustness in classifying the grid's stability. These results suggest that the federated learning approach handles the complexity of fault detection and excels in scenarios requiring precise stability assessments. This is potentially due to the effectiveness of the trimmed mean aggregation method in managing data heterogeneity.

TABLE I: Performance of the evaluated datasets

Metric	FaultData	StabilityData
Precision Score	0.8981	0.9776
Recall Score	0.9150	0.9774
F1 Score	0.8987	0.9775

Figure 5 shows the fault detection dataset's receiver operating characteristic curves (ROC), providing a comprehensive visual assessment of the multi-class classification model's performance. The area under the curve for each class ranges from 0.97 to 0.99, demonstrating the model's ability to distinguish various fault classes. In particular, classes 0 (No-Fault), 1 (L-L-L), and 5 (L-L) achieve an AUC of 0.99, indicating near-perfect classification accuracy for these fault types. The rest

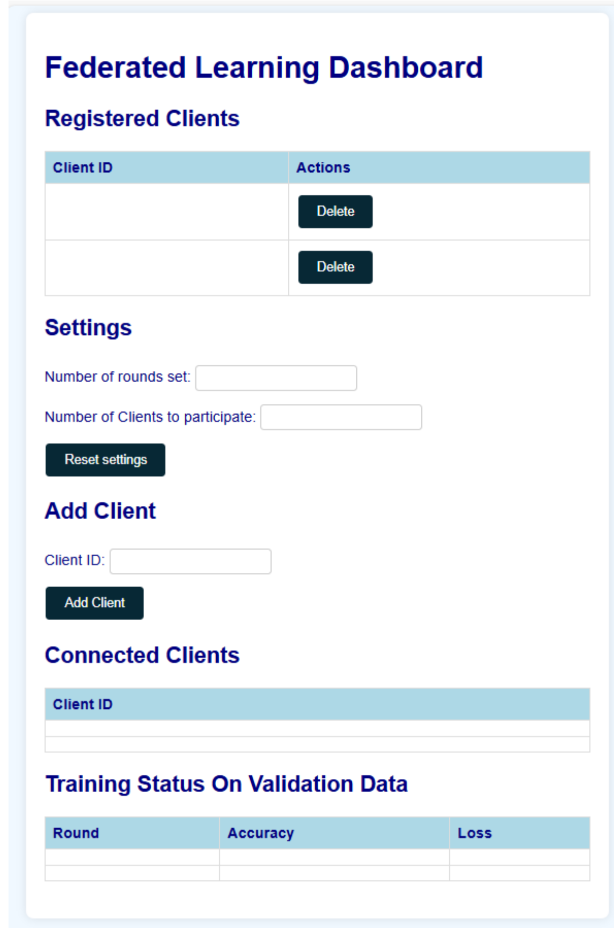

Fig. 4: Interface for managing the FL nodes

of the classes, with an AUC of 0.97, also perform well, albeit slightly less optimally.

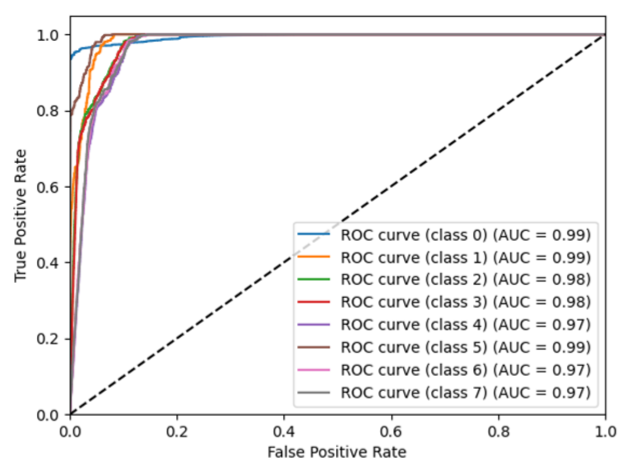

Fig. 5: Graph showing comparison metrics of our custom blockchain with established ones

The steep ascents of the ROC curves near the origin reflect a high true positive rate with minimal false positives. This is crucial in fault detection to minimize false alarms and prevent unnecessary interventions and costs. The significant elevation of these curves above the baseline underscores the model's superior predictive capability compared to random guessing, affirming its effectiveness in accurately differentiating between diverse fault scenarios.

When comparing IoT-PureChain with alternative blockchain solutions, it is apparent that this network offers distinct advantages. In contrast to the fixed-rate transaction processing observed in platforms such as Ethereum and Solana, IoT-PureChain dynamically adjusts its transaction throughput based on the current load, optimizing resource utilization for IoT-specific use cases. This dynamic scaling capability ensures that the system maintains efficiency regardless of transaction volume, which is a significant advantage in the context of the IoT, where transaction frequency can vary considerably. Furthermore, IoT-PureChain emerges as the most cost-effective solution with a transaction cost of zero dollars, particularly when juxtaposed with the relatively high costs associated with Ethereum or the minimal fees of Solana. This cost structure is especially beneficial for IoT applications, where the frequency of transactions can be high, and cost efficiency is paramount.

IoT-PureChain also demonstrates excellence in transaction finality, offering rapid confirmation times comparable to specialized solutions such as Fabric and Solana while maintaining exceptional scalability that rivals industry leaders such as Polygon. The design of IoT-PureChain, focusing on IoT applications, distinguishes it from general-purpose blockchains and provides a more targeted solution. The implementation of the $\mathbf{POA}^2$ consensus mechanism, which combines the Proof of Authority with an associative approach, facilitates a more efficient consensus process than the traditional Proof of Work or Proof of Stake, aligning well with the constraints and requirements of IoT environments where trusted nodes are crucial for security and efficiency.

The results of our IoT-PureChain network in Figures 6, 7 and Table II highlight the efficiency and stability of our system under a significant load. When evaluating the network with a workload of 1000 transactions over approximately $100s$, we observed that memory usage remained remarkably stable at 61% with a sharp increase to 62%. This consistency suggests that our approach to memory management within the $\mathbf{POA}^2$ consensus mechanism is highly effective and capable of handling the demands of IoT transactions without the overhead typically associated with memory-intensive operation. Stable memory utilization points to an optimized system in which resource allocation is finely tuned to prevent unnecessary consumption. This is crucial for IoT deployments, where devices often have limited resources.

Regarding CPU utilization, the system displays a dynamic response to the transaction load. CPU usage oscillated between 15% and 55%, with an average hovering of approximately 30%. This variability reflects the adaptive nature of the smart auto-mining mechanism, which adjusts block creation intervals based on the current system load. A notable peak in CPU usage at $76s$, reaching approximately 55%, illustrates the network's ability to scale its processing power in response to a sudden increase in transaction volume. This adaptability is key for IoT applications, where the load can be unpredictable owing to the nature of the device interactions, ensuring that our network can maintain performance stability under varying conditions.

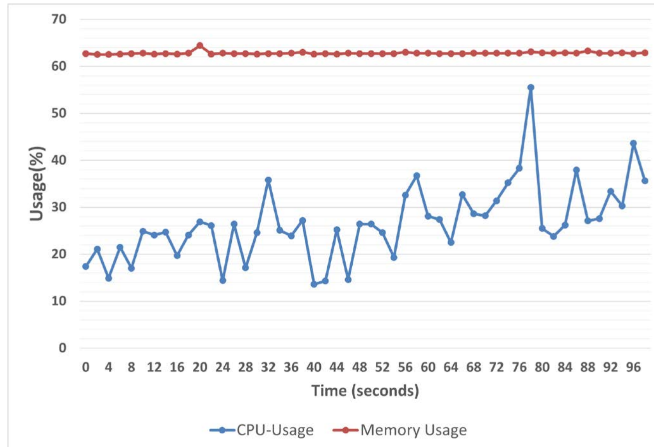

Fig. 6: CPU and Memory Usage Over Time in the IoT-PureChain Network During a 1000 Transaction Load Test

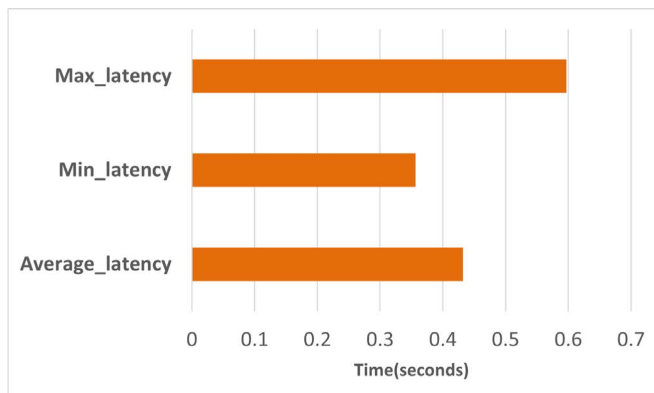

Fig. 7: Latency Analysis of IoT-PureChain Network: Maximum, Minimum, and Average Transaction Latency

The IoT-PureChain network achieved achieved a maximum latency of 0.6s and a minimum of 0.35 seconds, averaging approximately 0.44s per transaction as in Figure 7. This latency includes local model inference, transmission of model updates, aggregation, and blockchain commitment. These values fall well within the acceptable limits for smart grid fault response systems, which typically range between sub-second and 1–2 seconds thresholds for anomaly isolation and mitigation. Thus, the proposed system's with the $\mathbf{POA}^2$ performance aligns with the operational time constraints of latency-sensitive smart grid infrastructures.

V. Conclusion

This study effectively demonstrates the efficacy of integrating Federated learning with a custom blockchain to enhance fault detection and stability in smart grids. The hybrid LSTM model achieves high precision, recall, and F1 scores, showcasing its capacity to address smart grid data's diverse and

TABLE II: Comparative Performance Metrics of IoT-PureChain with Established Blockchain Networks

Metric	IoT-PureChain	Corda R3	Ethereum	Fabric	Solana	Polygon
Type	**Private**	Private	Public	Private	Public	Public
Tx per second	**Dynamic basing on the Load**	500	20	200	10,000	65,000
Cost per transaction	**$0.0**	$0.10	$5.0	$0.0	$0.00025	$0.0002
Transaction Finality	**Fast**	Fast	Slow as it depends on block confirmation	Fast	Fast	Fast
Scalability	**Excellent**	Excellent	Moderate	Good	Excellent	Excellent
Target	**IoT**	Finances	General	Enterprise	General	General
Consensus	**POA[2]**	Notary	Proof of Stake	Customised	Proof of History	Proof of Stake

dynamic nature. The blockchain's architecture, optimized for energy efficiency and devoid of transaction costs, ensures that IoT devices in resource-constrained environments can operate efficiently, enhancing overall system performance without the burden of additional operational expenses.

This configuration fosters a secure environment where data integrity is maintained through immutability and transparency, which are crucial for trust and reliability in critical infrastructure such as smart grids. Furthermore, utilizing SQLite alongside blockchain provides a practical solution for managing the substantial data generated by IoT sensors. It offers expeditious and reliable querying capabilities for real-time decision-making and node coordination. This integration represents a significant advancement towards decentralized control and management of grid operations, minimizing central points of failure and enhancing resilience against cyber threats.

Future investigations aim to develop models that detect and predict faults by adapting to changing grid conditions in real time through reinforcement learning or adaptive neuro-fuzzy systems. Enhanced security protocols, including zero-knowledge proofs or more robust encryption methods, could be investigated to protect against sophisticated cyber attacks, considering the increasing digitization and connectivity of grid assets. Also the work is to be extended to deploy the solution on a real-world smart grid testbed. This research establishes the foundation for more resilient, secure, and efficient smart grid systems, highlighting clear avenues for future development.

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-2025-RS-2020-II201612, 25%) and by Priority Research Centers Program through the NRF funded by the MEST (2018R1A6A1A03024003, 25%) and by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2024-00438430, 25%), by the IITP (Institute of Information & Communications Technology Planning & Evaluation)-ICAN (ICT Challenge and Advanced Network of HRD) grant funded by the Korea government (Ministry of Science and ICT) (IITP-2025-RS-2022-00156394, 25%).

References

[1] L. A. C. Ahakonye, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Low Computational Cost Convolutional Neural Network for Smart Grid Frequency Stability Prediction," *Internet of Things*, vol. 25, p. 101086, 2024.

[2] P. M. Custodio, M. A. P. Putra, J.-M. Lee, and D.-S. Kim, "Tlfed: Federated learning-based 1d-cnn-lstm transmission line fault location and classification in smart grids," in *2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. IEEE, 2024, pp. 026–031.

[3] F. Efthymiadis, A. Karras, C. Karras, and S. Sioutas, "Advanced optimization techniques for federated learning on non-iid data," *Future Internet*, vol. 16, no. 10, p. 370, 2024.

[4] K. J. Mukisa, L. A. C. Ahakonye, D.-S. Kim, and J. M. Lee, "Trimmed Averaging for Efficient Federated Learning in the Internet of Things," in *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*, 2024, pp. 322–326.

[5] 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.

[6] E. L. Ziliang Lai, Chris Liu, "When Private Blockchain Meets Deterministic Database," in *Proceedings of the ACM on Management of Data*, vol. 1, ACM Journals. Association for Computing Machinery, 2023, pp. 1–28.

[7] C. Jin, S. Pang, X. Qi, Z. Zhang, and A. Zhou, "A High Performance Concurrency Protocol for Smart Contracts of Permissioned Blockchain," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 11, pp. 5070–5083, 2022.

[8] D.-S. Kim, I. S. Igboanusi, L. A. C. Ahakonye, and G. O. Anyanwu, "Proof-of-Authority-and-Association Consensus Algorithm for IoT Blockchain Networks," in *The 43rd IEEE International Conference on Consumer Electronics (ICCE 2025)*, 2025.

[9] Tabassum, Saleha, Vijay Babu, Attuluri R., and Dheer, Dharmendra Kumar, "A comprehensive Exploration of IoT-enabled Smart grid systems: power quality issues, Solutions, and Challenges," *Sci. Tech. Energ. Transition*, vol. 79, p. 62, 2024.

[10] S. Kirmani, A. Mazid, I. A. Khan, and M. Abid, "A Survey on IoT-Enabled Smart Grids: Technologies, Architectures, Applications, and Challenges," *Sustainability*, vol. 15, no. 1, 2023.

[11] H. Bousbiat, R. Bousselidj, Y. Himeur, A. Amira, F. Bensaali, F. Fadli, W. Mansoor, and W. Elmenreich, "Crossing roads of Federated Learning and Smart grids: Overview, challenges, and perspectives," *arXiv preprint arXiv:2304.08602*, 2023.

[12] Z. Zhang, S. Rath, J. Xu, and T. Xiao, "Federated learning for smart grid: A survey on applications and potential vulnerabilities," *ArXiv*, vol. abs/2409.10764, 2024.

[13] S. Liu, X. Wang, L. Hui, and W. Wu, "Blockchain-Based Decentralized Federated Learning Method in Edge Computing Environment," *Applied Sciences*, vol. 13, no. 3, 2023.

[14] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[15] A. A. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S. Z. Abdul Rasid, and M. F. Yusof, "Scalability Challenges in Healthcare Blockchain System—A Systematic Review," *IEEE Access*, vol. 8, pp. 23 663–23 673, 2020.

[16] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-efficient learning of deep networks from decentralized data," in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, vol. 54. PMLR, 2017, pp. 1273–1282.