FL Meets LLM: A Hybrid Security Framework for the Internet of Energy

Jiaming Pei, Minghui Dai, R. R. Venkatesha Prasad, Norah Saleh Alghamdi, Yasser D. Al-Otaibi, and Ali Kashif Bashir

Abstract

The accelerating digital transformation of energy sector has led to the emergence of Internet of Energy (IoE) in which a vast array of interconnected devices coordinate the generation, distribution, and consumption of energy. Although this integration boosts the operational efficiency, it broadens the system's attack surface, making infrastructure increasingly vulnerable to cyber threats. Conventional intrusion detection systems often fall short in these distributed and privacy-sensitive settings. In this article, we introduce a hybrid cybersecurity framework that integrates federated learning (FL) with large language models (LLMs) to enable decentralized threat detection and context-aware response in IoE environments. By allowing edge devices to collaboratively train anomaly detection models without exposing raw data, the framework ensures data privacy. Moreover, a centralized LLM-driven reasoning layer interprets alerts and assists operators through natural language interfaces. We evaluate the proposed framework through assessing the quality of LLM responses across different prompt types and examining the temporal evolution of threat patterns. An application scenario for intelligent cyber defense in smart grids is introduced to demonstrate the framework's practical applicability. The results demonstrate that the proposed framework enhances both detection accuracy and interpretability, offering a scalable and transparent defense strategy for next generation energy infrastructure.

Introduction

The ongoing digitalization of the energy sector is ushering the Internet of Energy (IoE) in which the physical energy infrastructure is tightly integrated with advanced cyber technologies [1]. Within this interconnected ecosystem, assets ranging from centralized power plants and rooftop photovoltaic systems to grid-level transformers and smart home applications are connected through intelligent sensing, control, and communication mechanisms [2]. This convergence facilitates real-time situational awareness, decentralized decision-making, and remarkable improvements in operational efficiency across the energy chain.

Although the interconnectedness enables the benefits for IoE, it gives rise to substantial cybersecurity challenges [3], [4]. As illustrated in Fig. 1, the IoE encompasses a broad array of heterogeneous, geographically dispersed edge devices, including wind turbines, smart meters, power station, substation controllers, etc. These devices operate in physically unsecured or sparsely monitored environments, and it forms a highly dynamic and interdependent mesh of cyber-physical interactions. Moreover, since each node can act as a potential attack surface, the adversaries may exploit vulnerabilities such as compromised firmware, data manipulation, protocol-level weaknesses, or denial-of-service (DoS). The cascading impact of such threats can jeopardize system availability, equipment functionality, and even public safety.

Conventional security solutions are ill-equipped to meet the demands of this landscape. Centralized intrusion detection systems often suffer from latency bottlenecks and lack the contextual sensitivity required to detect nuanced, device-specific anomalies [5]. Furthermore, regulatory constraints often restrict the transmission of raw telemetry to cloud-based infrastructures, which impedes the effectiveness of centralized threat analytics [6].

To confront these challenges, in this article, we introduce a hybrid cybersecurity framework that synergistically combines federated learning (FL) with large language models (LLMs). FL enables distributed IoE devices to collaboratively train anomaly detection models without exchanging raw telemetry, thereby preserving data privacy while capturing localized operational nuances. In parallel, LLMs function as the semantic reasoning layer, and it transforms low-level anomaly logs and alert streams into coherent and context-rich narratives that assist in decision-making for human operators. By embedding intelligence at both the edge and central layers, the proposed framework delivers a scalable, interpretable, and privacy-conscious cybersecurity solution to IoE networks.

The main contributions of this article are summarized as follows. We introduce a modular and lightweight anomaly detection mechanism for federated deployment across resource-constrained edge nodes in IoE networks. We propose a secure model aggregation approach to handle

Jiaming Pei is with the School of Computer Science, The University of Sydney, Sydney, NSW 2006, Australia; Minghui Dai (corresponding author) is with the School of Computer Science and Technology, Donghua University, Shanghai 201620, China; R. R. Venkatesha Prasad is with the Delft University of Technology, 2628 CD Delft, The Netherlands; Norah Saleh Alghamdi is with the Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; Yasser D. Al-Otaibi is with the Department of Information Systems, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah 21589, Saudi Arabia; Ali Kashif Bashir is with Department of Computing and Mathematics, Manchester Metropolitan University, M15 6BX Manchester, U.K.

Digital Object Identifier: 10.1109/MNET.2025.3612271
Date of Current Version: 14 January 2026
Date of Publication: 1 October 2025

non-independent and identically distributed (non-IID) and multi-modal data in IoE settings. We present a natural language interface through LLMs to enable intuitive interpretation and explanation of cross-device anomaly patterns.

The remainder of this paper is organized as follows. The section "Background and Challenges" introduces the background and challenges. The section "System Architecture" presents the system architecture design. The key techniques for FL-LLM cybersecurity framework are illustrated in the section "Key Techniques for FL-LLM Cybersecurity Framework." The section "Implementation and Evaluation for FL-LLM Cybersecurity Framework" demonstrates the implementation and evaluation for FL-LLM cybersecurity framework. The application scenario for intelligent cyber defense in smart grids is provided in the section "Application Scenario: Intelligent Cyber Defense in Smart Grids." The section "Conclusion and Future Directions" concludes the paper with conclusion and future directions.

Background and Challenges

Cybersecurity Challenges of IoE

The IoE is rapidly becoming a foundational element of next-generation energy infrastructures, where pervasive digital connectivity, automation, and intelligence span the full energy lifecycle from decentralized generation and storage to distribution and terminal applications. This architecture connects a variety of edge devices, including solar inverters, wind turbines, smart meters, and substation controllers, operating over heterogeneous networks such as 6G, vehicular systems. Although such integration enhances operational visibility and efficiency, it introduces the cybersecurity vulnerabilities [7]. These edge devices deployed in geographically dispersed and physically unsecured environments lack fundamental protections such as hardware root-of-trust or secure runtime environments. It exposes the system to risks including firmware tampering, unauthorized access, and protocol exploitation. Attackers may exploit these weaknesses to orchestrate distributed denial-of-service (DDoS) attacks, manipulate control logic, or intercept command-and-control channels [8]. Moreover, the telemetry generated by these devices (e.g., voltage profiles, load patterns, and control commands) is often both privacy-sensitive and commercially valuable. High-profile cyber incidents such as the 2017 Triton malware campaign and the 2021 Colonial Pipeline breach underscore the urgency of safeguarding cyber-physical energy systems [9]. These events demonstrate the limitations of traditional perimeter-based security mechanisms and static intrusion detection systems, which lack the adaptability to address the dynamic, distributed nature of threats in IoE environments.

FL for Distributed Anomaly Detection

FL has emerged as a privacy-preserving paradigm for collaborative machine learning in scenarios where data is sensitive, siloed, or geographically distributed [10]. By enabling edge devices to locally train models and share aggregated weight updates with a central coordinator, FL aligns with privacy regulations and mitigates the need for transmitting raw telemetry, which conserves both bandwidth and confidentiality. Prior research has applied FL to network intrusion detection, fault diagnosis, and anomaly detection within industrial Internet of Things [11]. However, deploying FL in the context of IoE presents unique challenges. The data distribution across edge nodes is typically non-IID, which leads to model drift or poor generalization performance. Furthermore, the IoE devices are computationally constrained, it is necessary to design lightweight models and efficient communication protocols. Existing FL-based intrusion detection systems mainly focus on coarse-grained, binary classifications (e.g., benign vs. malicious). They offer little insight into the underlying nature, origin, or impact of detected anomalies [12].

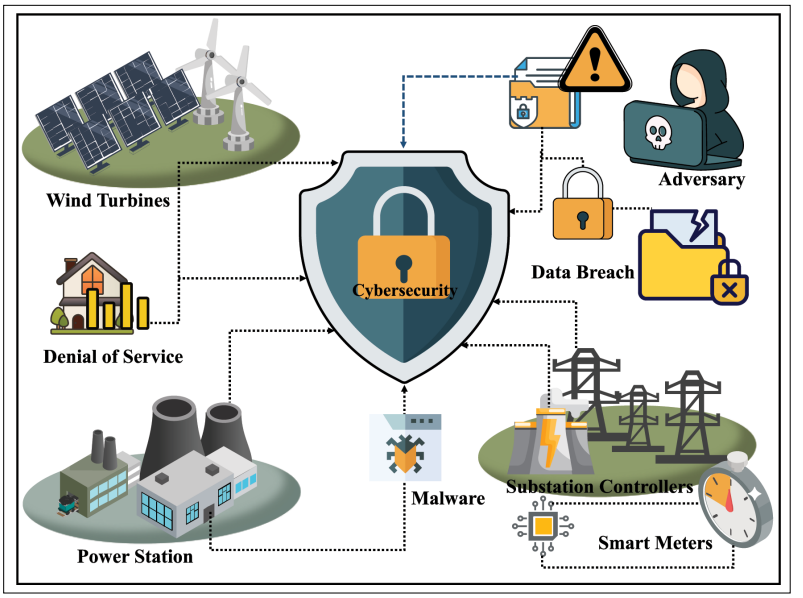

FIGURE 1. Cybersecurity challenges in IoE environment. The devices face exposure to protocol abuse, malware propagation, and privacy violations.

Language Models for Contextual Cyber Reasoning

Recent advances in LLMs (e.g., GPT-3, BERT, and Codex) have demonstrated remarkable capabilities in understanding and generating human-like text [13]. These models have been increasingly applied to a range of cybersecurity tasks, including malware behavior classification, phishing detection, threat intelligence summarization, and vulnerability report generation. Their abilities to bridge the semantic gap between technical data and human understanding make them promising tools for enhancing operator situational awareness. Nonetheless, most current applications of LLMs in cybersecurity remain offline. They rely on curated datasets, predefined prompts, and retrospective analysis. Several works have explored their integration into operational environments such as IoE systems, where alerts are generated in real-time and need to be contextualized across devices. Moreover, LLMs are rarely embedded in closed-loop systems that connect anomaly detection with decision-making, explanation, and policy feedback.

To bridge these gaps, this article introduces a federated anomaly detection mechanism tailored

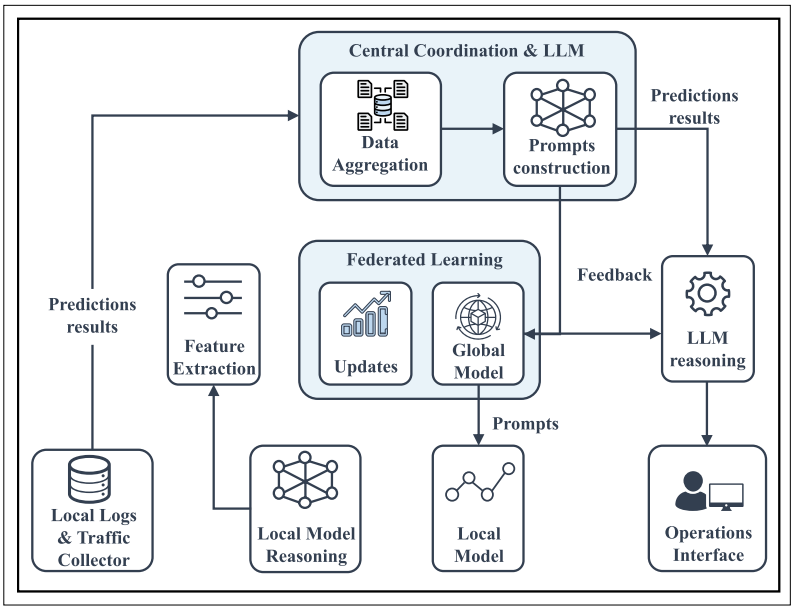

FIGURE 2. Proposed FL-LLM cybersecurity framework for IoE. (1) Local Data Processing and Anomaly Detection: on-device monitoring, feature extraction, and local model reasoning. (2) System Workflow and Module Interaction: FL-based collaborative model training, contextual LLM reasoning, and operator interaction via a natural language interface.

for non-IID energy data, augmented with a semantic reasoning layer that provides human-readable interpretations of model outputs.

System Architecture

In this section, we present a hybrid framework that couples on-device anomaly detection with coordinated, language-driven analysis to address the core challenges of cybersecurity in IoE environments. As illustrated in Fig. 2, the architecture is organized into two functional layers as follows.

- **Local Data Processing and Anomaly Detection**. Each IoE device hosts a lightweight module for real-time monitoring, feature extraction, and local model reasoning, thus enabling rapid, privacy-preserving detection at the edge.
- **System Workflow and Module Interaction**. The FL engine aggregates model updates without transmitting raw data. The central coordination unit synthesizes multi-source alerts into structured prompts. The LLM-based reasoning interface delivers contextual explanations and allows operators to interact with the system in natural language.

This layered design ensures that the system can detect and respond to both localized anomalies (e.g., voltage oscillations in a single inverter) and distributed, multi-device attack patterns (e.g., coordinated protocol scans across substations). Edge-side intelligence guarantees low-latency responses, while the centralized reasoning layer provides a system-wide situational understanding for informed decision-making.

Local Data Processing and Anomaly Detection

Each IoE device (e.g., solar inverters, EV chargers, wind turbine controllers, or distribution transformers) is equipped with a local data processing pipeline to enable on-device anomaly detection. This module consists of four key elements corresponding to the lower-left part of the architecture.

1. **Local Logs and Traffic Collector:** Continuously records operational telemetry (e.g., voltage, frequency, and control commands) as well as communication traffic (e.g., Modbus packet rates, message types, and anomalies).
2. **Feature Extraction:** Transforms raw sensor readings and network traces into compact statistical and temporal features, such as derivatives, entropy values, frequency distributions, and deviations from learned baselines.
3. **Local Model Reasoning:** Applies a lightweight anomaly detection model (such as a small CNN or LSTM) to compute anomaly scores or flag suspicious patterns in real-time.
4. **Local Model:** Stores the current version of the detection model, which is periodically updated through the FL process.

The processing is performed entirely on-device, ensuring that no raw logs or sensor values are transmitted externally. When anomalies are detected, the module either triggers a local mitigation action or sends model updates to the FL engine. Thus, this design minimizes bandwidth usage, preserves privacy, and enables rapid defense against cyber threats.

System Workflow and Module Interaction

As shown in Fig. 2, the proposed framework operates as a closed-loop process involving data collection, local analysis, collaborative model training, centralized reasoning, and operator interaction.

1. **Local Logs and Traffic Collector:** Each IoE device continuously collects operational telemetry and communication traces, forming the raw input for security analysis.
2. **Feature Extraction:** Local preprocessing converts raw data into compact features, which are then passed to the detection model.
3. **Local Model Reasoning:** The on-device anomaly detection model produces predictions in real-time. Prediction results can trigger immediate local responses or be fed into the FL process.
4. **FL Engine:** Devices periodically send encrypted model updates to the central server, where updates are aggregated into a global model and redistributed to devices.
5. **Data Aggregation and Prompt Construction:** When anomalies from multiple devices are reported, they are aggregated at the central coordination module. The system synthesizes these alerts into structured natural-language prompts with spatial, temporal, and contextual metadata.
6. **LLM Reasoning:** The prompt is processed by the LLM, which interprets the events, links them to historical incidents or known vulnerabilities, and generates human-readable explanations and recommendations.
7. **Operations Interface:** Operators receive the LLM output via a natural-language interface, allowing them to act on the insights, request additional analysis, or feed manual observations back into the system.

The workflow ensures that detection is fast and privacy-preserving at the device level, while high-level interpretation and decision support are handled centrally. The continuous feedback loop allows the system to adapt to evolving threats and maintain situational awareness across the entire IoE networks.

Key Techniques for FL-LLM Cybersecurity Framework

The technical foundation of the proposed framework lies in combining lightweight, collaborative learning with semantic-level reasoning. In this section, we detail the core mechanisms that enable scalable, privacy-preserving detection at the edge, as well as intelligent, human-readable interpretation at the center.

FL-Based Collaborative Training

To build global detection intelligence without compromising device-level privacy, we introduce the FL-based collaborative training approach. Each participating edge device maintains a local copy of the global detection model and trains it using their operational logs and communication features [14]. These training sessions are scheduled periodically or triggered upon anomaly detection.

As shown in Fig. 3(a), instead of sending raw data to the cloud, devices transmit only their model updates (e.g., gradients) to a central server, these updates pass through a privacy-preserving pipeline. Secure aggregation protocols cryptographically mask individual updates, ensuring that the central server cannot reconstruct individual contributions. Differential privacy can optionally be applied by injecting noise into updates, further protecting against membership reasoning or model inversion attacks.

The central aggregator combines updates using FedAvg, or FedProx when devices exhibit non-IID data. The updated global model is redistributed to edge devices, where it becomes the baseline for the next training round. This iterative process improves detection accuracy across the system while preserving data sovereignty and reducing communication overhead.

LLM-Powered Contextual Reasoning and Response

Anomaly detection cannot provide sufficient context for decision-making. To address this, we propose the LLM-powered contextual reasoning that serves as a centralized reasoning engine. When correlated anomalies are detected across devices, a prompt generation module constructs natural-language summaries encoding what occurred, where, when, and with what operational context [15]. As shown in Fig. 3(b), the system generates an example query as follows.

"Three smart inverters in a zone have reported repeated unauthorized Modbus commands over the last 30 minutes, with abnormal power oscillations. What is the likely cause, and what mitigation steps should be considered?"

The LLM, fine-tuned on industrial cybersecurity reports and IoE-specific knowledge, generates an interpretable response. This may include the link to known vulnerabilities and mitigation suggestions such as disabling specific ports, updating firmware, or segmenting network access. Unlike static logic trees, the LLM can generalize to novel combinations of events and synthesize information from structured and unstructured inputs. To maintain the reliable operations, the outputs generated by LLM are scored for confidence and routed through a sandboxed filter before being presented to human operators. In high-impact cases, the system recommends manual verification, ensuring that human's oversight remains in the loop.

Natural Language Operator Interface

A key advantage of integrating LLMs is the ability to support natural-language interaction. Instead of deciphering log files or alerts, the operators can ask high-level questions, as shown below.

"Have any similar anomalies occurred in this region over the past week?"

"Is there a known attack pattern related to these control packet spikes?"

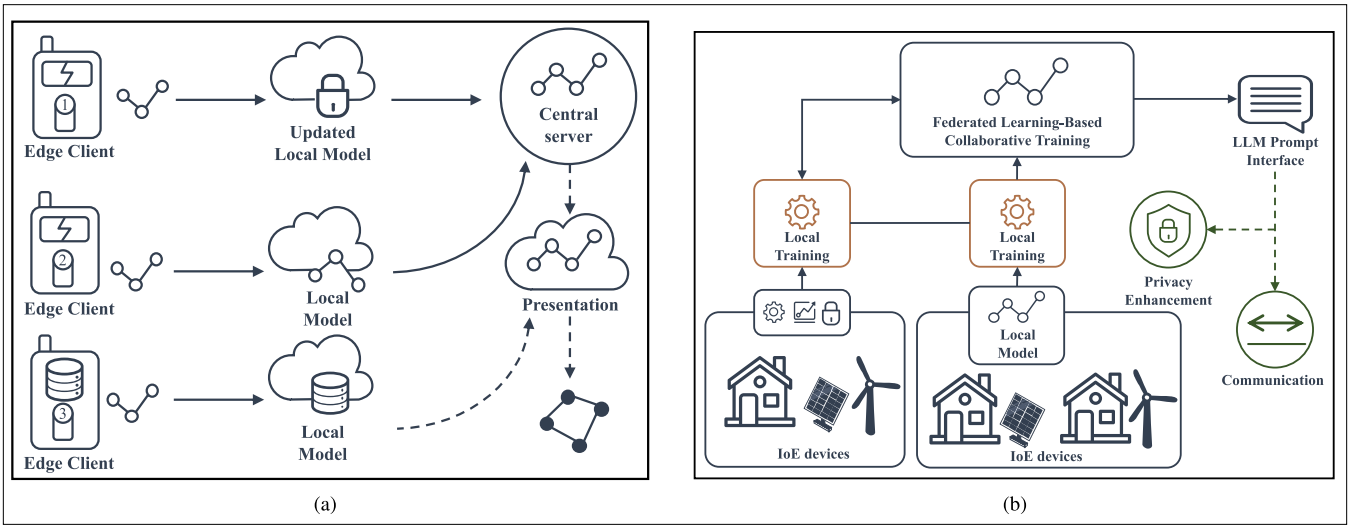

FIGURE 3. System components in the proposed framework. a) FL-based collaborative model training with privacy preservation across edge devices. b) The LLM prompt generation for contextual reasoning and operator interaction.

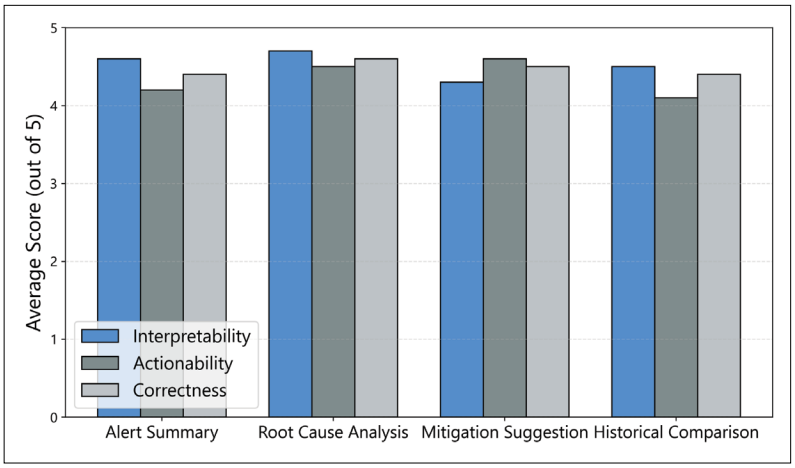

FIGURE 4. LLM evaluation scores across different prompt types, rated on interpretability, actionability, and correctness.

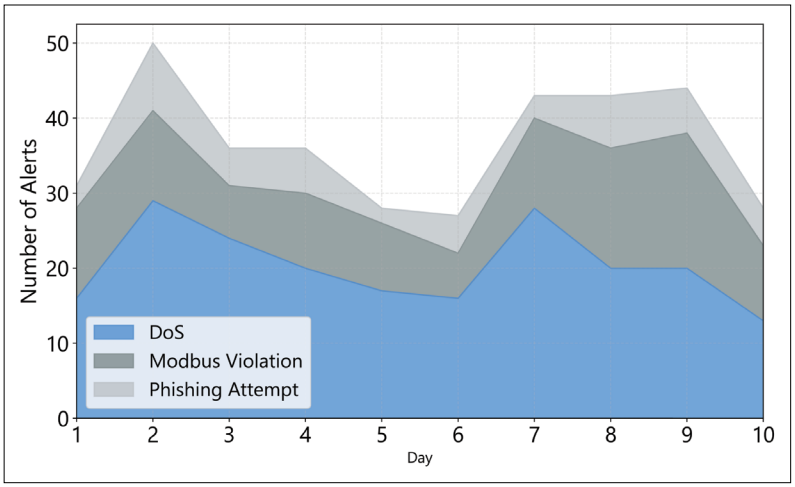

FIGURE 5. Threat type distribution over ten days monitoring window, showing the temporal dynamics of DoS attacks, Modbus violations, and phishing attempts.

The system responds with concise, context-aware summaries based on live and historical data. The operators can not only make incident response but also execute proactive inquiries such as validating a control strategy or anticipating the impact of a configuration change. This bridges the gap between technical output and human interpretation, empowering even non-specialist personnel to make informed decisions. Therefore, the system enhances situational awareness, reduces response latency, and supports continuous learning through dialogue.

Implementation and Evaluation for FL-LLM Cybersecurity Framework

To evaluate the effectiveness and interpretability of the proposed framework for IoE systems, two targeted experiments are conducted. We first explore the impact of using an LLM for post-detection reasoning and operator interaction. The real-time trends in threat activity is then examined to demonstrate the system's adaptability and contextual awareness.

The first experiment investigates how well the LLM can generate useful and actionable responses when given different types of anomaly-related prompts. Here, we define four prompt categories that commonly appear in operational settings including *alert summaries, root cause analysis, mitigation suggestions*, and *historical comparisons*. For each type, we generate realistic prompts based on synthetic but plausible multi-device IoE incidents. These prompts are submitted to an instance of GPT-3.5, and the generated outputs are evaluated by two expert reviewers along three criteria: interpretability, actionability, and correctness.

Fig. 4 shows the LLM evaluation scores across different prompt types, rated on interpretability, actionability, and correctness. It can be seen that the LLM performs well across all prompt types, particularly excelling in root cause and mitigation-oriented prompts. Specifically, interpretability scores remain consistently high, while actionability scores show slight variation depending on the clarity of context encoded in the prompt. Correctness scores are likewise stable across categories, with the highest values for root cause and mitigation prompts where richer context is provided, and slightly lower for alert summary and historical comparison prompts due to fewer explicit ground-truth cues. These results demonstrate that when guided by well-structured inputs, LLMs can assist operators in understanding complex threats and making informed decisions without requiring deep knowledge of underlying protocols or models.

In the second experiment, we simulate a rolling ten days monitoring period across a virtualized IoE networks, and record the number of alerts for three threat categories: DoS attacks, Modbus protocol violations, and phishing attempts. These represent a mix of volumetric, structural, and social-layer threats commonly encountered in smart grid environments. Fig. 5 illustrates the temporal distribution of these alerts using a stacked area chart. The visualization reveals distinct behavioral patterns. DoS alerts occur in sporadic surges, Modbus violations maintain a steady but elevated presence, and phishing attempts remain low-frequency but persistent. This heterogeneous threat landscape highlights the importance of using time-aware anomaly detection models at the edge and context-rich reasoning at the center.

These experiments validate both the low-level detection and high-level interpretation capabilities of the proposed framework. The results show that the proposed framework can effectively surface relevant threat information in real-time and enhance human understanding and operational readiness.

Application Scenario: Intelligent Cyber Defense in Smart Grids

Modern smart grids exemplify the growing intersection between cyber and physical infrastructure, where the integration of renewable energy sources, automated control, and real-time communication brings both operational efficiency and elevated security risks. To demonstrate how the proposed framework can be applied in a real world context, we consider a representative deployment scenario within a renewable-powered grid segment.

Fig. 6 illustrates how our proposed cybersecurity framework can be practically deployed on a smart grid infrastructure. This scene represents a typical renewable powered grid segment, which is composed of solar arrays, wind turbines, distributed controllers, and grid-side converters. Each of the component is both operationally critical and cyber exposed. In specific, edge devices such as power inverters, smart meters, and substation controllers run local anomaly detection models that are trained via FL. This allows models to improve collaboratively without sharing raw sensor or log data preserving. Once local models detect suspicious patterns (e.g., unexpected protocol usage or abnormal power oscillations), these events are flagged by the anomaly detection module. Events from multiple sources are then fed into a central prompt generator that aggregates and summarizes alerts into structured natural-language prompts. These prompts are submitted to a fine-tuned LLM.

The LLM interprets the situation in context through linking the current anomaly to historical threats, known vulnerabilities, or situational trends and returns human readable insights and suggested countermeasures. This output is routed to grid operators or automatic policy engines for response. Through this design, the proposed framework enables a continuous loop of privacy-preserving local learning, centralized semantic interpretation, and operational feedback.

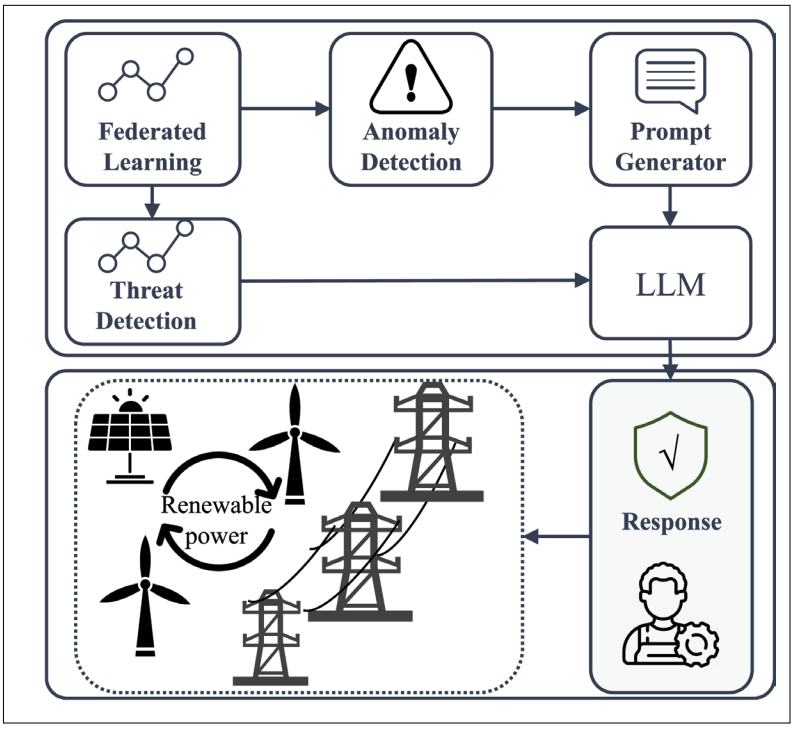

FIGURE 6. Deployment of the proposed cybersecurity framework in smart grid setting. FL enables distributed local detection, while LLM-powered reasoning provides high-level understanding.

Conclusion and Future Directions

In this article, we have presented a hybrid framework that combines FL and LLMs to enable distributed anomaly detection and contextual cyber reasoning across the IoE landscape. We have introduced the edge-side intelligence to detect threats in real-time while preserving data privacy, in which FL enables collaborative training across heterogeneous devices to improve detection accuracy in the presence of non-IID data. The integration of LLMs enhances the framework by translating low-level alerts into actionable, human-readable insights. Moreover, by supporting natural language interaction, the system helps operators understand and respond to emerging threats with low latency and confidence. Finally, we discuss several future research directions as follows.

Adaptive FL Orchestration With LLM-Guided Client Selection: The dynamic FL coordination mechanism is significant where LLMs can be used to analyze network metadata, threat intelligence reports, and device behavioral patterns to intelligently select trustworthy clients for participation, and optimize secure model aggregation strategies. Future research can be focused on enhancing resilience against poisoning attacks and improving model convergence in heterogeneous IoE environments.

LLM-Enhanced Real-Time Threat Interpretation: It is important to develop LLM modules that process diverse, encrypted FL local updates alongside network-level IoE data streams to generate human-readable, context-rich interpretations of potential security anomalies. Future direction can be focused on correlating subtle patterns across decentralized data sources to identify novel multi-stage attacks (e.g., false data injection combined with device compromise) and provide actionable mitigation recommendations.

Lightweight Privacy-Preserving LLM Reasoning: The resource-efficient techniques (e.g., model distillation, quantization, selective activation) is critical to deploy specialized, compact LLMs directly on IoE edge devices. Future research can be focused on validating model updates of LLMs using differential privacy, detecting local data drift indicative of attacks, and generating concise security summaries for the central FL coordinator.

Acknowledgment

This work was supported in part by the National Natural Science Foundation of China under Grant 62501137; and in part by the Deanship of Scientific Research and Libraries at Princess Nourah bint Abdulrahman University for funding this work through the Visiting Researcher Program VR-2025-010.

References

[1] M. Moness and A. M. Moustafa, "A survey of cyber-physical advances and challenges of wind energy conversion systems: Prospects for Internet of Energy," *IEEE Internet Things J.*, vol. 3, no. 2, pp. 134–145, Apr. 2016.
[2] A. Gozuoglu, O. Ozgonenel, and C. Gezegin, "Design and implementation of controller boards to monitor and control home appliances for future smart homes," *IEEE Trans. Ind. Informat.*, vol. 20, no. 9, pp. 11458–11465, Sep. 2024.
[3] K. Kumar et al., "Cybersecurity challenges in the digitization and integration of renewable energy systems: A review," *IEEE Trans. Eng. Manag.*, vol. 72, pp. 3042–3054, 2025.
[4] M. Dai et al., "An edge-driven security framework for intelligent Internet of Things," *IEEE Netw.*, vol. 34, no. 5, pp. 39–45, Sep. 2020.
[5] S. A. Rahman et al., "Internet of Things intrusion detection: Centralized, on-device, or federated learning?" *IEEE Netw.*, vol. 34, no. 6, pp. 310–317, Nov. 2020.
[6] D. Chen et al., "Bridging data silos in finance via federated learning," *IEEE Netw.*, early access, Jul. 1, 2025, doi: 10.1109/MNET.2025.3584806.

[7] F. Li et al., "Enhanced cyber-physical security in Internet of Things through energy auditing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5224–5231, Jun. 2019.
[8] J. C. Balda et al., "Cybersecurity and power electronics: Addressing the security vulnerabilities of the Internet of Things," *IEEE Power Electron. Mag.*, vol. 4, no. 4, pp. 37–43, Dec. 2017.
[9] M. Pourmadadkar, M. Lezzi, A. Corallo, "Cyber security for cyber-physical systems in critical infrastructures: Bibliometrics analysis and future directions," *IEEE Trans. Eng. Manage.*, 2024.
[10] J. Pei et al., "A review of federated learning methods in heterogeneous scenarios," *IEEE Trans. Consum. Electron.*, vol. 70, no. 3, pp. 5983–5999, Aug. 2024.
[11] D. C. Nguyen et al., "Federated learning for Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1622–1658, 3rd Quart., 2021.
[12] H. Kheddar, "Transformers and large language models for efficient intrusion detection systems: A comprehensive survey," 2024, *arXiv:2408.07583*.
[13] F. N. Motlagh et al., "Large language models in cybersecurity: State-of-the-art," 2024, *arXiv:2402.00891*.
[14] J. Pei, W. Li, and S. Mumtaz, "From routine to reflection: Pruning neural networks in communication-efficient federated learning," *IEEE Trans. Artif. Intell.*, early access, Sep. 17, 2025, doi: 10.1109/TAI.2024.3462300.
[15] Y. Zhang et al., "LogiCode: An LLM-driven framework for logical anomaly detection," *IEEE Trans. Autom. Sci. Eng.*, vol. 22, pp. 7712–7723, 2025.

Biographies

Jiaming Pei (Student Member, IEEE) (jpei0906@uni.sydney.edu.au) is currently pursuing the Ph.D. degree with The University of Sydney, Sydney, NSW, Australia. From 2021 to 2022, he visited the Southwestern University of Finance and Economics, Chengdu, China. He has authored or co-authored and worked on some papers in the refereed journals and conferences, such as ICLR, IEEE Journal on Selected Areas in Communications, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network Science and Engineering, IEEE Transactions on Consumer Electronics, and IEEE Transactions on Vehicular Technology. His research interests include the application of data mining and federated learning.

Minghui Dai (Member, IEEE) (minghuidai@dhu.edu.cn) received the Ph.D. degree from Shanghai University, Shanghai, China, in 2021. He is currently an Assistant Professor with the School of Computer Science and Technology, Donghua University, Shanghai, China. His research interests include the general area of wireless network architecture and vehicular networks.

R. R. Venkatesha Prasad (r.r.venkateshaprasad@tudelft.nl) is currently an Associate Professor at the Networked Systems Group, Delft University of Technology. His research interests include tactile internet, the IoT, and 60 GHz mmWave networks. He has supervised 21 Ph.D. students and 63 M.Sc. students. He has over 300 publications in peer-reviewed international journals and conferences, standards, and book chapters. He was the Vice-Chair of the IEEE Tactile Internet Standardization Workgroup and is now a mentor. He is an Associate Editor on the editorial board of IEEE Transactions on Mobile Computing, IEEE Transactions on Sustainable Computing, and IEEE Transactions on Cognitive Communication and Networking. For more information, please refer to http://homepage.tudelft.nl/w5p50

Norah Saleh Alghamdi (Member, IEEE) (nosalghamdi@pnu.edu.sa) received the B.Sc. degree from Taif University, Taif, Saudi Arabia, and the M.Sc. and Ph.D. degrees from the Department of Computer Science, La Trobe University, Melbourne, VIC, Australia. She has been the Vice-Dean of Quality Assurance since 2019. She is currently an Associate Professor with the Department of Computer Science, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University (PNU), Riyadh, Saudi Arabia. She is also the Director of Business and Project Management at her college. Her research interests include data mining, machine learning, text analytics, image classification, bioengineering, and deep learning. She has authored or co-authored many articles published in well-known journals in the research field. She has participated in organizing the International Conference on Computing (ICC 2019). She is a member of the reviewer committee of several journals, such as MDPI, Emerald, and Elsevier.

Yasser D. Al-Otaibi (yalotaibi@kau.edu.sa) received the Ph.D. degree in information systems from Griffith University, Brisbane, QLD, Australia, in 2018. He is currently an Assistant Professor with the Department of Information Systems, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah, Saudi Arabia. His current research interests include information technology adoption and acceptance, wireless sensor networks, and the Internet of Things.

Ali Kashif Bashir (Senior Member, IEEE) (dr.alikashif.b@ieee.org) received the Ph.D. degree from Korea University, South Korea, in 2012. He is a Reader at the Department of Computing and Mathematics, Manchester Metropolitan University, U.K. He is also affiliated with the University of Electronic Science and Technology of China (UESTC), China; National University of Science and Technology, Islamabad (NUST), Pakistan; and the University of Guelph, Canada, in honorary roles. His previous assignments include the National Fusion Research Institute, South Korea; Osaka University, Japan; and the University of the Faroe Islands, Denmark. He has obtained funding from several international bodies, accumulatively over U.S. $3 million. He has obtained over U.S. $4 million funding from Korean, Japanese, European, Asian, and Middle Eastern bodies to solve interdisciplinary research problems in the field of wireless sensor networks, the Internet of Things/cyber-physical systems, cyber security, and smart infrastructures. Along with his students and colleagues, he has published over 200 high-impact articles in the top venues. He has chaired several international conferences and has delivered over 40 invited and keynote talks. He is an editor of several journals and the Editor-in-Chief of the IEEE Technology, Policy and Ethics Newsletter.