iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83518

www.ijraset.com

Call: ✆08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Hybrid Edge-IoT Framework for Fault Detection and Reliability Enhancement in Smart Grids

Saba[1], Sharad Kumar[2]
[1]*School of Engineering & Technology, Shri Venkateshwara University, Gajraula , U.P. India*
sabaa0680@gmail.com
Orcid ID: 0009-0003-7578-2422
[2]*School of Engineering & Technology, Shri Venkateshwara University, Gajraula , U.P. India*
sharad.choudhary007@gmail.com
Orcid ID: 0009-0009-5859-9689

Abstract: The increasing deployment of Internet of Things (IoT) devices and intelligent sensing technologies within modern smart grids has significantly improved grid visibility, operational automation, and real-time energy management capabilities. However, the growing complexity of smart grid infrastructures introduces critical challenges related to fault detection, communication latency, system reliability, and rapid decision-making. Traditional cloud-centric architectures often experience delays in processing large volumes of grid data, limiting their ability to respond effectively to time-sensitive operational events and fault conditions. The proposed framework integrates distributed IoT sensing devices, edge computing nodes, intelligent fault detection mechanisms, and centralized cloud services to enable real-time monitoring and localized decision-making. Operational data generated by smart meters, sensors, substations, and distributed energy resources are processed at nearby edge nodes, reducing communication overhead and enabling rapid fault identification. Furthermore, an intelligent reliability assessment module continuously evaluates grid conditions, communication performance, and equipment health to support proactive maintenance and resilient grid operation. The proposed framework enhances fault detection accuracy, minimizes response time, reduces network congestion, and improves overall grid reliability. Experimental evaluation under diverse smart grid operating scenarios demonstrates significant improvements in fault detection performance, communication efficiency, operational resilience, and system scalability compared with conventional monitoring architectures.

Keywords: Smart Grid, Edge Computing, Internet of Things (IoT), Fault Detection, Reliability Enhancement, Edge Intelligence, Real-Time Monitoring

I. INTRODUCTION

The rapid evolution of modern power systems has led to the widespread adoption of smart grid technologies that integrate advanced sensing devices, communication networks, distributed energy resources, and intelligent control systems. Smart grids enable real-time monitoring, automated decision-making, demand-side management, and efficient energy distribution through continuous data exchange among grid components. The integration of Internet of Things (IoT) technologies has further enhanced the capability of smart grids by facilitating large-scale deployment of smart meters, sensors, intelligent electronic devices, and monitoring equipment. These devices continuously generate operational data related to power generation, energy consumption, voltage levels, equipment status, and grid stability, thereby supporting intelligent grid management and enhanced situational awareness. Despite these advancements, the increasing number of interconnected devices and the growing volume of generated data present significant challenges for conventional smart grid monitoring architectures. Singh et al. [1] proposed Intelligent Fault Edge, an AI-driven fault-tolerant edge framework for smart grid monitoring in IoT environments. The framework utilized edge intelligence to process grid data locally and improve fault tolerance while reducing communication delays. The study demonstrated enhanced monitoring efficiency and rapid fault response capabilities; however, comprehensive reliability assessment and adaptive infrastructure management were not fully incorporated into the proposed solution. Traditional cloud-centric approaches require operational data to be transmitted to centralized servers for processing and analysis. As the scale of smart grid deployments increases, such architectures often experience communication bottlenecks, increased latency, network congestion, and delayed responses to critical grid events. These limitations can adversely affect fault detection performance and compromise the reliability of smart grid operations, particularly during emergencies and dynamic operating conditions.

Fault detection is one of the most critical functions in smart grid infrastructures because equipment failures, communication disruptions, sensor malfunctions, and power quality disturbances can significantly impact grid stability and service continuity. Early identification of abnormal conditions enables utility operators to take corrective actions before faults propagate throughout the network. However, conventional fault detection mechanisms often rely on centralized processing models that may not provide the responsiveness required for real-time grid applications. Furthermore, the growing complexity of distributed energy resources, renewable generation systems, and heterogeneous communication networks increases the difficulty of maintaining reliable and resilient grid operations.

Recent advancements in edge computing have introduced new opportunities for addressing these challenges. Edge computing enables data processing and decision-making closer to the source of data generation, thereby reducing communication latency and minimizing dependence on centralized cloud infrastructure. By deploying intelligent processing capabilities at edge nodes located near substations, distributed energy resources, and IoT devices, critical monitoring and fault detection tasks can be executed locally with minimal delay. This distributed processing approach enhances operational responsiveness, improves communication efficiency, and strengthens overall system resilience. Although existing studies have explored IoT-enabled monitoring systems and edge-based computing architectures independently, the integration of edge intelligence, IoT sensing, fault detection, and reliability enhancement within a unified smart grid framework remains an active research area. Senthilkumar and Dass [2] developed a fault detection and isolation framework for smart grids using IoT and edge computing technologies. Their approach enabled localized processing of operational data to identify grid faults with reduced latency. The results showed improvements in fault isolation speed and communication efficiency. Nevertheless, the framework primarily focused on fault detection and lacked an integrated mechanism for continuous reliability evaluation and resilience enhancement. Many current solutions focus either on communication efficiency or fault detection accuracy without simultaneously addressing reliability assessment, adaptive decision-making, and large-scale scalability requirements. Consequently, there is a need for an intelligent framework capable of providing real-time fault identification, localized processing, proactive reliability management, and resilient smart grid operation. The proposed framework integrates distributed IoT sensing devices, edge computing nodes, intelligent fault detection mechanisms, reliability assessment modules, and cloud-based management services shown in fig. 1. Operational data generated by smart grid components are processed at nearby edge nodes, enabling rapid fault identification and localized decision-making while reducing communication overhead. The framework continuously monitors equipment conditions, communication performance, and grid operational parameters to assess system reliability and support proactive maintenance activities.

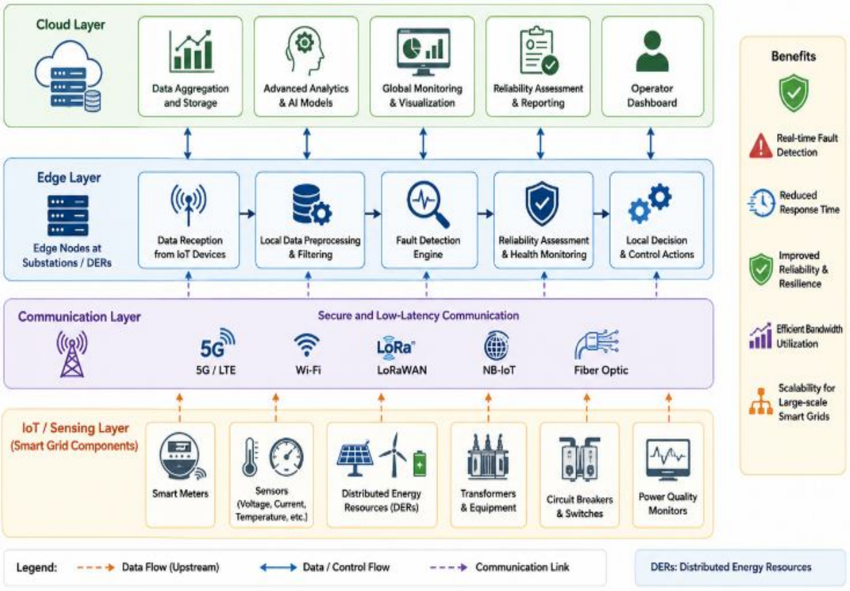

Fig. 1. Conceptual Overview of Hybrid Edge-IoT Framework for Fault Detection and Reliability Enhancement in Smart Grids

By combining edge intelligence with IoT-enabled monitoring and adaptive reliability management, the proposed framework aims to improve fault detection accuracy, reduce response time, enhance communication efficiency, and strengthen grid resilience under dynamic operating conditions. The distributed architecture further supports scalability and enables efficient management of large-scale smart grid infrastructures.

The main contributions of this paper are as follows:

1) A hybrid Edge-IoT architecture that enables real-time monitoring and localized processing of smart grid operational data.
2) An intelligent fault detection mechanism for identifying abnormal grid conditions and equipment failures with minimal delay.
3) A reliability enhancement model that continuously evaluates grid health, communication performance, and operational stability.
4) A comprehensive performance evaluation demonstrating improvements in fault detection accuracy, response time, communication efficiency, scalability, and system reliability.

The remainder of this paper is organized as follows. Section II presents the literature review related to edge computing, IoT-enabled smart grids, and fault detection techniques. Section III describes the proposed Hybrid Edge-IoT Framework and its operational methodology. Section IV discusses the experimental setup and performance evaluation results. Finally, Section V concludes the paper and outlines future research directions.

II. LITERATURE SURVEY

Researchers have proposed various frameworks for fault detection, reliability enhancement, predictive maintenance, cybersecurity, and real-time grid management. This section reviews recent studies related to edge-enabled smart grids, intelligent fault diagnosis, and resilient energy infrastructure. Mukisa et al. [3] investigated smart grid instability and fault detection using a combination of blockchain and federated learning technologies. The proposed architecture enhanced decentralized decision-making and secure data sharing among distributed grid entities. Although the framework improved fault detection performance and cybersecurity, the computational complexity associated with federated learning and blockchain implementation presents challenges for real-time deployment in large-scale smart grid environments. Sarathkumar et al. [4] explored the application of digital twin technology for smart grid monitoring and control. The study demonstrated that virtual replicas of physical grid assets can improve system visibility, operational analysis, and fault diagnosis capabilities. While digital twins provide comprehensive monitoring support, their effectiveness depends on continuous synchronization with physical infrastructure and significant computational resources. Parasdeep et al. [5] proposed an AI-driven smart grid fault diagnosis framework based on federated learning and edge computing in IoT-enabled power systems. The framework enabled distributed learning across multiple edge nodes while preserving data privacy. Experimental results indicated improved fault classification accuracy and reduced dependency on centralized processing. However, the study focused primarily on fault diagnosis and did not address broader reliability optimization requirements. Balla et al. [6] presented scalable IoT frameworks for smart grid management using time-series analysis and predictive maintenance based on ARIMA models. Their work demonstrated the importance of predictive analytics for identifying equipment degradation and preventing system failures. Although the proposed framework improved maintenance planning, adaptive fault response and real-time edge intelligence were not extensively investigated. Kant et al. [7] examined blockchain as a deployment mechanism for enhancing security in IoT-based systems. The study highlighted the benefits of decentralized trust management, data integrity, and secure communication among interconnected devices. The findings provide valuable insights for securing smart grid infrastructures; however, the work focused primarily on security mechanisms rather than operational reliability and fault management. Mjbas et al. [8] conducted a comparative study on lightweight machine learning models for IoT-based smart grid fault detection. The research evaluated multiple algorithms under noisy and real-world deployment scenarios to identify suitable models for resource-constrained environments. The results demonstrated the effectiveness of lightweight machine learning techniques for fault detection; however, the study did not integrate edge orchestration and reliability management functionalities. Masood et al. [9] developed a co-simulation framework for evaluating False Data Injection (FDI) and Denial of Service (DoS) attacks in IoT-enabled next-generation smart grids. The framework assessed the resilience of smart grid communication infrastructures under cyberattack conditions. The study emphasized the importance of resilient monitoring architectures but primarily concentrated on cybersecurity evaluation rather than intelligent fault management and operational optimization. Sharma and Kumar [10] investigated the role of Artificial Intelligence in enhancing data security and privacy within smart city environments. The study highlighted how AI-driven analytics can improve system reliability, anomaly detection, and intelligent decision-making across interconnected infrastructures. The presented concepts demonstrate the potential of AI-based approaches for strengthening the security and resilience of smart grid ecosystems. Zeng et al. [11] explored the application of knowledge management systems and digital services in smart grid environments. Their work emphasized intelligent information management, service automation, and data-driven decision support for improving grid operations. Although the framework enhanced information accessibility and operational efficiency, it did not specifically address edge-enabled fault detection and infrastructure reliability enhancement. Dhinakaran et al. [12] proposed an AIoT-enabled smart flood detection and autonomous power isolation system for real-time safety and predictive risk management.

The framework integrated AI, IoT sensors, and automated control mechanisms to support rapid response during critical events. The study demonstrated the effectiveness of AIoT technologies in enhancing infrastructure resilience and operational safety, highlighting the importance of intelligent edge-based decision-making in mission-critical systems.

III. PROPOSED METHODOLOGY

The objective of this study is to develop a Hybrid Edge-IoT Framework for Fault Detection and Reliability Enhancement in Smart Grids. The proposed methodology integrates IoT-based data acquisition, edge-intelligent processing, fault detection mechanisms, reliability assessment, and adaptive grid management to ensure efficient and resilient smart grid operations. The framework is designed to address challenges associated with communication latency, delayed fault identification, network congestion, equipment failures, and operational instability while maintaining real-time monitoring and reliable power delivery. The proposed architecture combines distributed IoT sensing devices, edge computing nodes, and cloud infrastructure to facilitate localized decision-making and intelligent grid management.

A. IoT-Based Smart Grid Monitoring and Data Acquisition

The first layer of the proposed framework consists of IoT-enabled smart grid devices responsible for collecting and transmitting real-time operational information throughout the power network. These devices include smart meters, phasor measurement units (PMUs), intelligent electronic devices (IEDs), renewable energy sources, transformers, substations, distributed sensors, and energy storage systems. The deployed IoT devices continuously generate data related to voltage levels, current measurements, frequency variations, power consumption, equipment status, environmental conditions, and communication performance. The collected information is transmitted to nearby edge nodes through secure communication channels. Instead of forwarding all raw data directly to centralized cloud servers, the framework performs preliminary filtering, aggregation, and prioritization of data at the network edge. Critical operational events and fault-related information receive higher transmission priority, while redundant or low-priority data are locally processed. This approach minimizes communication overhead, reduces network congestion, and improves the responsiveness of smart grid monitoring operations.

B. Edge-Intelligent Data Processing & Fault Identification

The second component of the framework introduces distributed edge computing nodes for localized data processing and intelligent fault detection. Multiple edge gateways are strategically deployed near substations, renewable energy installations, and critical grid infrastructure to enable real-time analysis of operational data. The edge nodes continuously process incoming measurements and evaluate grid conditions using fault detection algorithms. Various operational parameters including voltage deviations, frequency instability, transformer loading conditions, communication interruptions, equipment temperature, and power quality indicators are analysed to identify abnormal behaviours. The localized processing capability enables faults to be detected near their point of occurrence without requiring continuous cloud interaction. Consequently, fault detection latency is significantly reduced, allowing rapid response to operational disturbances and minimizing the impact of failures on grid performance.

C. Intelligent Fault Classification and Reliability Assessment

The third stage of the proposed methodology focuses on intelligent fault classification and system reliability evaluation. Once abnormal operating conditions are detected, the framework classifies the detected events according to fault severity, affected infrastructure components, and potential operational impact. The reliability assessment module continuously evaluates various grid performance indicators including equipment health, communication reliability, fault frequency, power quality stability, network availability, and service continuity. Based on these measurements, a reliability score is generated to represent the overall operational condition of the smart grid. Components exhibiting deteriorating performance or abnormal operational trends receive lower reliability scores, enabling early identification of potential failures. This proactive reliability assessment mechanism supports preventive maintenance planning and improves the resilience of smart grid infrastructure.

D. Adaptive Grid Control and Cloud Integration

After fault detection and reliability evaluation, the framework activates adaptive control mechanisms to maintain stable grid operation. Edge nodes coordinate with local controllers and grid management systems to initiate corrective actions based on real-time operational conditions. These actions may include load redistribution, fault isolation, demand response activation, distributed generation coordination, and equipment protection measures.

While time-critical operations are handled at the edge layer, summarized operational information and historical data are periodically transmitted to the cloud infrastructure for long-term analysis, system optimization, and model updates. The cloud layer performs large-scale data analytics, predictive maintenance evaluation, historical trend analysis, and centralized grid management functions. The collaborative interaction between IoT devices, edge nodes, and cloud services enables efficient resource utilization while maintaining low-latency operational responsiveness.

E. Performance Evaluation and Comparative Analysis

The evaluation considers fault detection accuracy, fault response time, communication latency, network throughput, reliability index, communication overhead, resource utilization efficiency, and system scalability. The performance of the proposed framework is compared with conventional cloud-based monitoring systems and existing smart grid fault management architectures. Fault detection accuracy and response time measurements are used to evaluate monitoring effectiveness, while latency and throughput analyses assess communication efficiency.

Reliability and scalability evaluations determine the framework's ability to maintain stable operation under varying network conditions and increasing numbers of connected devices. Furthermore, communication overhead and resource utilization analyses measure the effectiveness of localized edge processing in reducing network congestion and improving computational efficiency. The comparative analysis demonstrates the capability of edge intelligence and IoT integration to significantly enhance fault detection performance, operational reliability, and overall smart grid resilience.

IV. RESULT AND ANALYSIS

The performance evaluation of the proposed Hybrid Edge-IoT Framework for Fault Detection and Reliability Enhancement in Smart Grids was conducted under multiple smart grid operating scenarios involving varying communication loads, fault occurrences, equipment failures, and dynamic network conditions.

The proposed framework was compared against conventional cloud-based monitoring systems, traditional IoT-enabled smart grid architectures, and existing edge-assisted monitoring frameworks. The evaluation focused on measuring fault detection performance, communication efficiency, reliability enhancement, response time, and scalability. Experimental results demonstrate that the integration of edge intelligence and IoT technologies significantly improves fault identification capabilities while reducing communication delays and enhancing overall smart grid resilience.

A. System Configuration and Experimental Environment

The simulation environment was designed to emulate a large-scale smart grid infrastructure consisting of smart meters, phasor measurement units (PMUs), intelligent electronic devices (IEDs), substations, transformers, renewable energy resources, battery storage systems, distributed sensors, and utility control centers. The implementation was carried out using an Intel Core i7 processor with 16 GB RAM running Ubuntu Linux.

The simulation framework was developed using Python and various networking and data analytics libraries including NumPy, Pandas, Matplotlib, Scikit-Learn, and EdgeSimPy. The smart grid environment consisted of more than 1500 interconnected devices continuously generating operational and monitoring data. Multiple operating scenarios including normal operation, fault conditions, communication disruptions, and varying traffic loads were evaluated. Furthermore, different fault categories such as equipment failures, voltage abnormalities, communication interruptions, and sensor malfunctions were introduced to evaluate the robustness and adaptability of the proposed framework.

B. Comparative Fault Detection and Reliability Analysis

As shown in TABLE I, the proposed Hybrid Edge-IoT Framework achieved the highest fault detection accuracy and reliability performance while maintaining the lowest communication overhead among all evaluated monitoring architectures. The localized processing capability of edge nodes enables rapid identification of abnormal grid conditions, thereby improving monitoring effectiveness and reducing unnecessary data transmissions.

TABLE I. Comparative Fault Detection and Reliability PErformance of Smart Grid Frameworks

Monitoring Framework	Fault Detection Accuracy (%)	Reliability Index (%)	Communication Overhead (%)
Cloud-Based Monitoring System	84.7	82.9	29.4
Traditional IoT Monitoring Framework	89.5	88.1	22.7
Existing Edge-Assisted Framework	94.3	93.6	16.5
Proposed Hybrid Edge-IoT Framework	98.1	97.4	9.8

The results indicate that the proposed framework significantly improves fault identification and reliability assessment through distributed edge processing and intelligent monitoring mechanisms. The reduction in communication overhead further demonstrates the effectiveness of localized data analysis in minimizing network congestion.

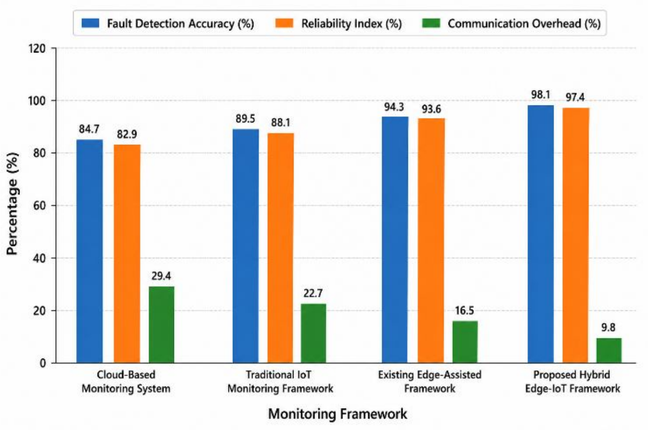

Fig. 2. Comparative Fault Detection Accuracy and Communication Overhead Analysis of Smart Grid Monitoring Frameworks

Fig. 2 demonstrates that the proposed Hybrid Edge-IoT Framework consistently outperforms conventional monitoring architectures in terms of monitoring accuracy, reliability enhancement, and communication efficiency.

C. Latency and Response Performance Analysis

The latency and response performance evaluation examines the capability of the proposed framework to support real-time fault detection and operational decision-making under varying smart grid conditions, as shown in TABLE II.

TABLE II. Comparative Latency, Throughput and Response Analysis

Framework	Average Latency (ms)	Through put (Mbps)	Response Time (ms)
Cloud-Based Monitoring System	176	52.8	194
Traditional IoT Framework	132	68.4	146
Existing Edge-Assisted Framework	87	81.7	96
Proposed Hybrid Edge-IoT Framework	49	97.9	58

The proposed Hybrid Edge-IoT Framework achieved the lowest latency and response time while providing the highest throughput performance among all evaluated architectures. The deployment of edge nodes near smart grid components enables localized processing of critical operational data, thereby minimizing communication delays and accelerating fault response activities. Furthermore, intelligent data prioritization mechanisms improve throughput by reducing redundant transmissions and optimizing network utilization.

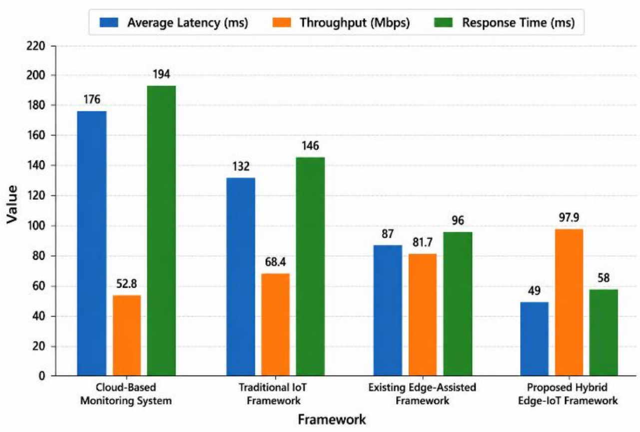

Fig. 3. Comparative Latency and Throughput Analysis of Smart Grid Monitoring Frameworks

Fig. 3 illustrates that the proposed framework provides superior real-time monitoring performance and communication efficiency for modern smart grid environments.

D. Scalability and Edge Processing Efficiency Analysis

The scalability analysis evaluates the effectiveness of the proposed framework under increasing numbers of connected smart grid devices and monitoring components, as presented in TABLE III.

TABLE III. SCALABILITY & RELIABILITY PERFORMANCE UNDER DIFFERENT MICROGRIDS SIZES

Number of Devices	Cloud-Based Reliability (%)	Existing Edge Framework Reliability (%)	Proposed Hybrid Edge-IoT Reliability (%)
500 Devices	86.4	94.2	98.5
1000 Devices	84.9	93.7	98.1
2000 Devices	82.6	92.9	97.8
4000 Devices	80.8	91.6	97.3
6000 Devices	78.5	90.1	96.9

The proposed Hybrid Edge-IoT Framework maintains consistently high reliability performance even as the number of connected devices increases significantly. The distributed edge computing architecture effectively balances computational workloads across multiple edge nodes, preventing centralized processing bottlenecks and supporting scalable smart grid operations. The intelligent reliability assessment mechanism continuously adapts to changing network conditions and operational requirements, thereby ensuring stable system performance under large-scale deployments.

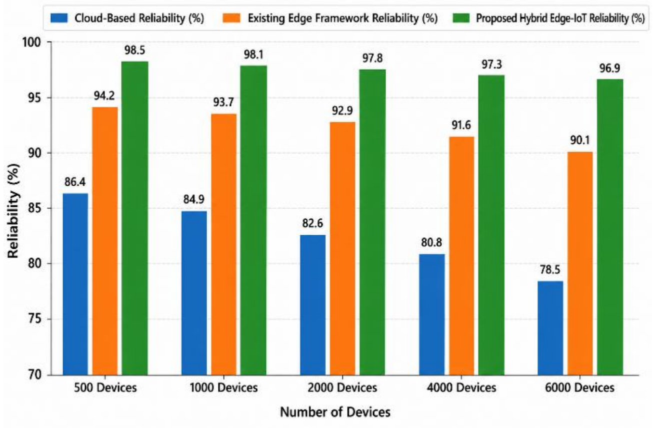

Fig. 4. Scalability Analysis of Hybrid Edge-IoT Framework Under Increasing Smart Grid Device Density

The results presented in Fig. 4 confirm that the proposed framework provides superior scalability, fault detection capability, communication efficiency, and operational reliability for next-generation smart grid infrastructures. The integration of IoT-enabled monitoring, edge-intelligent processing, and adaptive reliability management enables resilient and efficient smart grid operation capable of supporting large-scale distributed energy ecosystems.

V. CONCLUSION AND FUTURE SCOPE

This paper presented a Hybrid Edge-IoT Framework for Fault Detection and Reliability Enhancement in Smart Grids that integrates IoT-enabled monitoring, edge-intelligent data processing, fault identification mechanisms, reliability assessment, and adaptive grid management to improve the performance and resilience of modern smart grid infrastructures. The proposed framework enables localized processing of operational data at distributed edge nodes, thereby reducing communication delays and supporting rapid fault detection and response. Experimental results demonstrated the effectiveness of the proposed approach, achieving a fault detection accuracy of 98.1%, reliability index of 97.4%, and communication overhead of only 9.8%, outperforming conventional cloud-based and existing edge-assisted monitoring architectures. Furthermore, the framework attained the lowest average latency of 49 ms, highest throughput of 97.9 Mbps, and fastest response time of 58 ms, highlighting its suitability for real-time smart grid applications. The scalability analysis further revealed that the proposed framework maintained a reliability level of 96.9% even with 6000 connected devices, confirming its capability to support large-scale smart grid deployments. These results demonstrate that the integration of edge computing and IoT technologies can significantly enhance fault detection performance, communication efficiency, operational reliability, and overall grid resilience. Future research can focus on incorporating Artificial Intelligence and Deep Learning models for predictive fault forecasting, integrating blockchain-based security mechanisms for secure edge communication, developing federated learning-enabled distributed intelligence across edge nodes, supporting autonomous self-healing grid operations, and extending the framework to manage renewable energy-rich smart grids, electric vehicle charging infrastructures, and next-generation cyber-physical energy systems.

REFERENCES

[1] T. Singh *et al.*, "Intelligent FaultEdge: AI-Driven Fault-Tolerant Edge Framework for Smart Grid Monitoring in IoT," 2024 IEEE 12th International Conference on Intelligent Systems (IS), Varna, Bulgaria, 2024, pp. 1-6, doi: 10.1109/IS61756.2024.10705247.

[2] K. Senthilkumar and P. Dass, "Fault Detection and Isolation in Smart Grids Using IoT and Edge Computing," 2025 2nd International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2025, pp. 1-8, doi: 10.1109/ICECONF65644.2025.11379432.

[3] K. J. Mukisa, L. A. C. Ahakonye, J. M. Lee and D. -S. Kim, "Synergistic Smart Grid: Instability and Fault Detection Using Blockchain and Federated Learning," 2025 Sixteenth International Conference on Ubiquitous and Future Networks (ICUFN), Lisbon, Portugal, 2025, pp. 588-593, doi: 10.1109/ICUFN65838.2025.11170004.

[4] D. Sarathkumar et al., "Digital Twin Technology for Smart Grid Monitoring and Control," 2026 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), Bhopal, India, 2026, pp. 1-6, doi: 10.1109/SCEECS68810.2026.11429733.

[5] Parasdeep, Ayushi, D. Upadhaya, M. Pal, M. Kumar and S. Singh, "AI-Driven Smart Grid Fault Diagnosis Using Federated Learning and Edge Computing in IoT-based Power Systems," 2025 IEEE 7th International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2025, pp. 1-6, doi: 10.1109/ICCCA66364.2025.11325716.

[6] R. T. Balla, S. Padmanabham, R. S. Bhandari, V. Kumar and S. Khattar, "Scalable IoT Frameworks for Smart Grid Management: A Time-Series and Predictive Maintenance Analysis Using ARIMA Models," 2026 5th International Conference on Innovative Practices in Technology and Management (ICIPTM), Noida, India, 2026, pp. 1-6, doi: 10.1109/ICIPTM69057.2026.11465901.

[7] R. Kant, S. Sharma, V. Vikas, S. Chaudhary, A. K. Jain and K. K. Sharma, "Blockchain – A Deployment Mechanism for IoT Based Security," 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), Ghaziabad, India, 2023, pp. 739-745, doi: 10.1109/CICTN57981.2023.10140715.

[8] M. Y. H. Mjbas, S. A. Aliesawi and M. R. H. Al-Dahhan, "Deployment-Aware Benchmarking of Lightweight Machine Learning for IoT-Based Smart Grid Fault Detection: A Comparative Study Across Easy, Noisy, and Public Evaluation Settings," 2026 8th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (ICHORA), Ankara, Turkiye, 2026, pp. 1-9, doi: 10.1109/ICHORA69329.2026.11537190.

[9] M. Y. Masood, H. Rifà-Pous, M. Awais, A. Khawar and M. Muzaffar, "Co-Simulation of FDI and DOS Attacks in IoT-Enabled Next-Generation Smart Grids: A Framework for Resilience," 2026 7th International Conference on Advancements in Computational Sciences (ICACS), Lahore, Pakistan, 2026, pp. 1-7, doi: 10.1109/ICACS69208.2026.11433141.

[10] V. Sharma and S. Kumar, "Role of Artificial Intelligence (AI) to Enhance the Security and Privacy of Data in Smart Cities," 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2023, pp. 596-599, doi: 10.1109/ICACITE57410.2023.10182455.

[11] L. Zeng, Y. Shi, L. Li, J. Zhu and R. Tan, "Research on the Application of Knowledge Management System and Digital Service in Smart Grid," 2024 2nd International Conference on Mechatronics, IoT and Industrial Informatics (ICMIII), Melbourne, Australia, 2024, pp. 527-531, doi: 10.1109/ICMIII62623.2024.00104.

[12] A. S. Dhinakaran, E. Harish, P. Maniraj, R. V. Kamali, R. Vishwangar and G. Devayani, "AIoT-Enabled Smart Flood Detection and Autonomous Power Isolation System for Real-Time Safety and Predictive Risk Management," 2026 4th International Conference on Intelligent Data Communication Technologies and Internet of Things *(IDCIoT)*, Ottapalam, India, 2026, pp. 286-291, doi: 10.1109/IDCIoT67589.2026.11455663.