OPEN ACCESS

Saudi Journal of Engineering and Technology

Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) |ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Communication Infrastructure for Secure Smart Meter Networks in Electric Utilities

Minul Khan Rahat[1]*, Mohammad Samiul Asraf[2], Ahmed Junaid[3], Md. Shariful Islam[4]

[1]Department of Electrical Engineering, University- Lamar University, Beaumont, TX, United States
[2]Department of Engineering and Technology, University: Southeast Missouri State University, Cape Girardeau, Missouri, United States
[3]Postgraduate Diploma in Mobile Communications Systems University: University of East London, United Kingdom
[4]Master's in Engineering Management, University: Lamar University, Beaumont, Texas, United States

DOI: https://doi.org/10.36348/sjet.2026.v11i05.008 | **Received:** 17.03.2026 | **Accepted:** 12.05.2026 | **Published:** 16.05.2026

***Corresponding author:** Minul Khan Rahat
Department of Electrical Engineering, University- Lamar University, Beaumont, TX, United States

Abstract

This paper presents a secure communication infrastructure for smart meter networks in electric utilities. The study addresses a major limitation in current advanced metering infrastructure research: communication security, monitoring, attack detection, and service continuity are often handled as separate topics. In actual utility operation, smart meter networks function within distributed environments that include field devices, gateways, concentrators, edge nodes, utility control platforms, and cloud-connected services. Such a structure creates exposure to unauthorized access, false data injection, message interception, privacy loss, and communication failure. To address these issues, the paper proposes a multi-layer framework that combines protected data transmission, distributed traffic monitoring, edge-level packet inspection, federated threat detection, and continuity support within one system model. The methodology evaluates the framework through communication, security, and reliability measures, including end-to-end delay, packet trust, detection accuracy, service availability, and recovery time. The discussion shows that the proposed framework maintains stable communication performance while improving attack detection and preserving partial operation during gateway failure, cloud disruption, and denial-of-service conditions. The results indicate that secure smart meter communication must be treated as a combined problem involving transmission protection, monitoring visibility, anomaly detection, and continuity of operation. The paper provides a practical model for future smart grid communication research and utility deployment planning.

Keywords: Smart meter networks, advanced metering infrastructure, electric utilities, secure communication infrastructure, edge analytics, federated learning, intrusion detection, communication reliability, cybersecurity, smart grid communications.

I. INTRODUCTION

Electric utilities are shifting from conventional metering systems to digitally connected smart meter networks with two-way communication across the distribution system. These networks carry meter readings, outage notifications, tariff updates, remote service commands, and load-related control signals. As a result, communication infrastructure now affects day-to-day utility operation, system monitoring, and service management. The communication path is no longer limited to a direct link between meters and the utility center. In many deployments, it includes field devices, gateways, concentrators, cloud platforms, edge nodes, and supervisory control systems spread across large service areas. This broader connectivity introduces several technical concerns. Unauthorized access, false data injection, message interception, service interruption, device spoofing, and privacy exposure can disrupt network performance and reduce confidence in operational data. Utilities also need communication systems that remain stable during faults, traffic congestion, equipment failure, and cyber incidents. For that reason, a secure smart meter network must support protected data transmission, continuous monitoring, timely event reporting, and reliable exchange between field assets and utility platforms. The research problem addressed in this paper is the absence of an integrated communication framework that combines security, monitoring, and operational continuity within one system model. Many existing deployments still depend

on partial solutions that address only one part of the problem. This paper proposes a secure communication infrastructure for smart meter networks in electric utilities that supports protected data exchange, scalable monitoring, threat detection, and continuous operation across utility communication environments.

A. Background and Motivation

Smart meter networks have changed how electric utilities collect, transmit, and process operational information. Older metering systems were used mainly for periodic readings, while current deployments support remote configuration, near real-time reporting, outage awareness, tariff updates, and demand-side coordination. This shift has improved visibility, yet it has also increased dependence on communication systems that operate across wide service areas and mixed technical settings. In practice, smart meter data travels through field devices, local gateways, concentrators, control servers, and remote monitoring platforms before reaching utility operators. Each stage introduces requirements related to latency, reliability, security, and access control. Utility operators also need communication systems that continue to function during equipment failure, network disruption, or cyberattack. For these reasons, secure communication infrastructure has become a central research issue in smart grid development. The motivation for this study comes from the need to address protection, monitoring, and operational stability within one system framework instead of treating them as separate problems.

B. Problem Statement

Despite the progress of smart meter technology, several communication problems remain unresolved. Many deployments still face risks such as message interception, spoofing, false data injection, denial-of-service attacks, and unauthorized access. Privacy is another concern because detailed consumption data can reveal patterns of user behavior. In addition, smart meter communication often depends on architectures that were not designed for large-scale cyber-physical coordination across diverse utility settings. Some prior work concentrates on encryption and authentication. Other studies focus on monitoring, intrusion detection, or network management. This separation has produced partial solutions rather than a unified system model. As a result, a gap remains between research proposals and practical utility deployment. The main problem addressed in this paper is the absence of an integrated communication framework that protects meter data, supports continuous monitoring, maintains operation during faults or attacks, and fits within broader utility control and supervisory environments.

C. Proposed Solution

This paper presents an integrated communication infrastructure for secure smart meter networks in electric utilities. The proposed system treats the smart meter network as part of a wider utility architecture that includes meters, aggregation points, control servers, cloud-connected monitoring platforms, edge processing units, and supervisory interfaces. Instead of depending on a single protection mechanism, the framework combines multiple coordinated functions within one communication model. These functions include protected data transmission, network visibility, distributed monitoring, anomaly detection, and continuity support. The design also supports interaction between field-level communication and higher-level utility management systems. A layered structure is used so that communication services, security controls, and monitoring functions can operate together within the same environment. This approach addresses practical utility conditions where performance, fault tolerance, and communication safety must all be considered. The proposed solution therefore focuses on both technical protection and operational use in real utility systems.

D. Contributions

This paper offers several contributions to the study of secure smart meter communication. First, it presents a unified architectural model that brings together communication security, monitoring capability, and operational continuity within one utility-focused framework. Second, it defines a structured approach for meter-to-utility communication that covers data protection, access control, anomaly awareness, and coordinated supervision across multiple layers. Third, it incorporates distributed analysis and intelligent threat detection into the communication design rather than placing those functions outside the core system. Fourth, it expands the discussion of smart meter communication beyond isolated AMI channels and places it within a broader utility setting that includes cloud services, edge processing, and supervisory control functions. Fifth, it provides a practical research direction for utilities that need communication systems capable of supporting cybersecurity requirements and service reliability at the same time. Together, these contributions provide a stronger basis for the design of secure smart meter communication infrastructures.

E. Paper Organization

The remainder of this paper is organized as follows. Section II reviews prior studies on smart meter security, privacy, cloud-based monitoring, edge intelligence, supervisory communication, and intelligent detection methods. It also identifies the limitations of current approaches and states the research gap addressed in this study. Section III describes the proposed communication infrastructure and explains its main components, architectural layers, and functional structure. Section IV outlines the methodology used to evaluate the proposed framework, including system modeling and analytical assessment. Section V discusses the expected outcomes of the design in terms of communication protection, monitoring support, fault response, and continuity of operation. Section VI concludes the paper with a summary of the main findings

and several directions for future research. This sequence moves from context and problem definition to system design, evaluation, and final discussion in a clear order.

II. RELATED WORK

A. Security and Privacy in Advanced Metering Infrastructure

Security and privacy remain core issues in advanced metering infrastructure (AMI) because smart meter networks carry consumption records, control messages, and operational data. Shokry et al. reviewed AMI security and identified threats such as eavesdropping, false data injection, denial-of-service, malware, and weak authentication across multiple layers of the network [2]. Their study also noted that many proposed defenses address individual threats instead of the full communication path. Ajiboye et al. examined privacy and security issues in AMI data and networks and pointed to unresolved problems in confidentiality, access control, traffic protection, and secure aggregation in utility-scale systems [4]. These studies show that smart meter security cannot be limited to device-level protection. The communication network, data flow, and system architecture also require attention [2], [4].

B. Cloud, Edge, and SCADA Support for Utility Communication

Recent studies connect secure utility communication with cloud platforms, edge analytics, and SCADA integration. Afrin presented cloud-integrated network monitoring dashboards that combine IoT data collection with edge analytics for distributed infrastructure monitoring [1]. The study showed the value of continuous visibility and local event analysis in connected systems. Afrin et al. later examined distributed edge intelligence for energy and transportation systems and reported that edge-assisted processing can reduce delay and support local decision-making in cyber-physical environments [5]. Enam et al. discussed smart SCADA frameworks that combine cloud computing, IIoT, and cybersecurity for industrial automation, which has direct relevance to utility supervisory networks [6]. Hasan et al. focused on IoT-integrated solar energy monitoring in smart-grid settings and illustrated the role of connected sensing and coordinated data exchange in energy applications [8]. Joarder contributed additional infrastructure perspectives through work on disaster recovery, high-availability hybrid cloud design, and AI-enabled monitoring for smart data centers [14], [15]. Taken together, these studies indicate that smart meter communication should be examined as part of a larger cloud-edge-SCADA system rather than as an isolated field network [1], [5], [6], [8], [14], [15].

C. AI, Federated Learning, and Blockchain in Secure Communications

Several recent papers examine intelligent and decentralized approaches for communication security in critical infrastructure. Afrin proposed a cyber-resilient model for internet service provider infrastructure with automated threat detection and adaptive defense mechanisms [3]. Although the setting differs from utility networks, the study offers relevant ideas for anomaly detection in distributed communication systems. Fahim et al. presented an IoT security framework that combines AI, blockchain, and cloud integration to support data integrity and trusted communication across connected devices [7]. In the smart-grid domain, Sun et al. introduced a hierarchical federated learning-based intrusion detection system for 5G smart grids [9]. Their results showed that distributed model training can support attack detection without centralizing all sensitive data. Islam et al. extended this direction through a study on federated learning for secure industrial automation and grid optimization [13]. These works suggest that AI-based intrusion detection, federated analytics, and blockchain-based trust models offer useful directions for smart meter communication networks, especially where privacy, scale, and distributed coordination are major concerns [3], [7], [9], [13].

D. Reliability, Protection, and Related Energy IoT Systems

A communication infrastructure for smart meter networks must support security as well as reliable system operation. Hossain et al. studied cybersecurity and privacy in IoT-based electric vehicle ecosystems and identified weak communication interfaces, privacy exposure, and device heterogeneity as major concerns [10]. Similar issues appear in smart meter deployments, where many devices communicate over shared and mixed networks. Islam examined safety-integrated SCADA systems for process hazard control in power generation plants and emphasized dependable communication, timely event detection, and coordinated supervisory control [11]. In another study, Islam analyzed transformer protection and fault detection with relay automation and machine learning [12]. That work showed how communication-supported protection schemes can improve system awareness and response during abnormal operating conditions. Although these studies do not focus only on AMI, they remain relevant because electric utility communication networks must support cybersecurity, fault response, and control reliability at the same time [10]–[12].

E. Research Gap

The literature covers AMI threats and privacy risks [2], [4], cloud-edge monitoring and SCADA support [1], [5], [6], [14], [15], and intelligent security methods such as federated learning and blockchain [7], [9], [13]. However, fewer studies bring these areas together in a single communication architecture for smart meter networks in electric utilities. Most existing work treats monitoring, privacy, intrusion detection, resilience, and supervisory control as separate topics. That separation leaves a gap in research on integrated communication infrastructures that address secure data exchange, scalable monitoring, edge

intelligence, high availability, and utility-grade operational performance in one framework. A study that addresses these elements together would contribute a more practical basis for secure smart meter networks in electric utilities.

III. METHODOLOGY

This study develops a methodology for the design and evaluation of a secure communication infrastructure for smart meter networks in electric utilities. The method follows the paper's main novelty: one framework that combines protected data transfer, distributed monitoring, intelligent threat detection, and continuity support within the same utility communication system. Security, monitoring, and recovery are treated as connected functions rather than separate modules. The methodology is organized into four subsections: system architecture and workflow, analytical model, evaluation setup, and performance analysis.

A. System Architecture and Communication Workflow

The proposed framework is modeled as a five-layer communication structure. The field layer contains smart meters that generate periodic readings, event notifications, and control responses. The aggregation layer contains gateways and data concentrators that collect local traffic and forward it toward the utility network. The edge layer performs packet inspection, temporary caching, local anomaly screening, and short-term decision support. The utility service layer contains the head-end system, monitoring dashboard, security controller, and supervisory interface. The cloud support layer stores historical records, maintains backup services, and distributes model updates. Communication follows a structured sequence. Each smart meter creates a packet containing device identity, timestamp, payload, and integrity information. The packet moves to the nearest gateway or concentrator and then to an edge node. At the edge layer, the packet passes through identity validation, integrity checking, traffic-rate inspection, and anomaly scoring. Valid traffic is forwarded to the utility platform for storage, monitoring, and control use. Suspicious traffic moves to an alert queue for further inspection. If service disruption occurs, local cache support and alternate communication paths are activated so that the network can continue basic operation during partial failure.

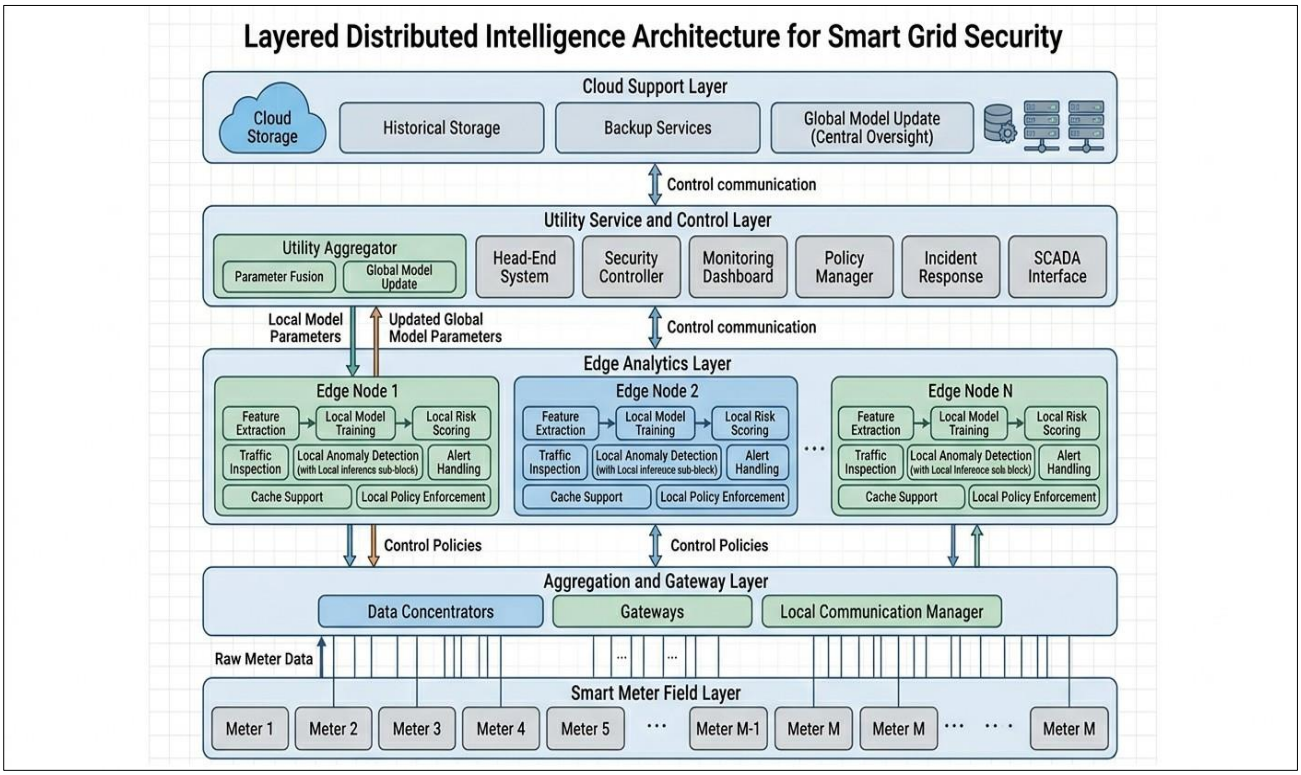

Figure 1: Proposed Secure Communication Architecture for Smart Meter Networks Figure 1 presents the communication path from smart meters to the utility platform. The field layer generates operational data. The aggregation layer collects and routes traffic. The edge layer screens packets and computes risk indicators. The utility layer manages monitoring and control functions. The cloud layer provides storage, backup support, and model update services

B. Analytical Model

The methodology uses a small set of equations to represent communication delay, packet trust, and detection performance. These expressions are selected because they match the paper's focus on secure transmission, local inspection, and threat identification.

The end-to-end communication delay is defined as

$$T_{e2e} = T_m + T_g + T_e + T_u$$

Where:
T_{e2e} is the total delay from the smart meter to the utility platform, T_m is the meter processing time, T_g is the gateway or concentrator forwarding delay, T_e is the edge inspection delay, and Tu is the utility server processing delay. This equation measures the time cost introduced across the full communication chain.

To support forwarding decisions at the edge layer, the methodology defines a packet trust score:

$$P_t = \lambda_1 I + \lambda_2 H + \lambda_3 B + \lambda_4 Q$$

Where: P_t is the packet trust score, I represents identity validation, H represents integrity verification, B is the behavioral consistency score, and Q is the communication quality score.

The coefficients λ_1, λ_2, λ_3 and λ_4 are normalized weights whose sum equals 1. Low-trust packets are flagged for additional inspection, while high-trust packets continue through the normal route.

Detection performance is measured with classification accuracy:

$$Acc = \frac{TP + TN}{TP + TN + FP + FN}$$

where TP, TN, FP, and FN denote true positive, true negative, false positive, and false negative values. This metric shows how well the detection module separates malicious traffic from normal communication.

C. Federated Detection and Evaluation Setup

The detection component uses a federated learning structure distributed across edge nodes. Each edge node processes its local traffic records and trains a local anomaly model without transferring raw traffic data to the utility center. Only model parameters are sent to the aggregation server. The server combines the incoming parameters, creates a global model, and returns the updated model to the edge nodes. This arrangement reduces centralized exposure of traffic data and supports distributed analysis across the network. The evaluation setup uses smart meter traffic features collected from simulated or testbed communication flows. These features include packet size, transmission interval, identity consistency, integrity status, retransmission count, response time, traffic burst frequency, and communication quality indicators. The framework is tested under four operating conditions: normal communication, false data injection, denial-of-service pressure, and partial infrastructure failure. These scenarios reflect common utility communication stresses and correspond to the paper's main contribution, which is the joint treatment of protection, monitoring, and continuity within one system model.

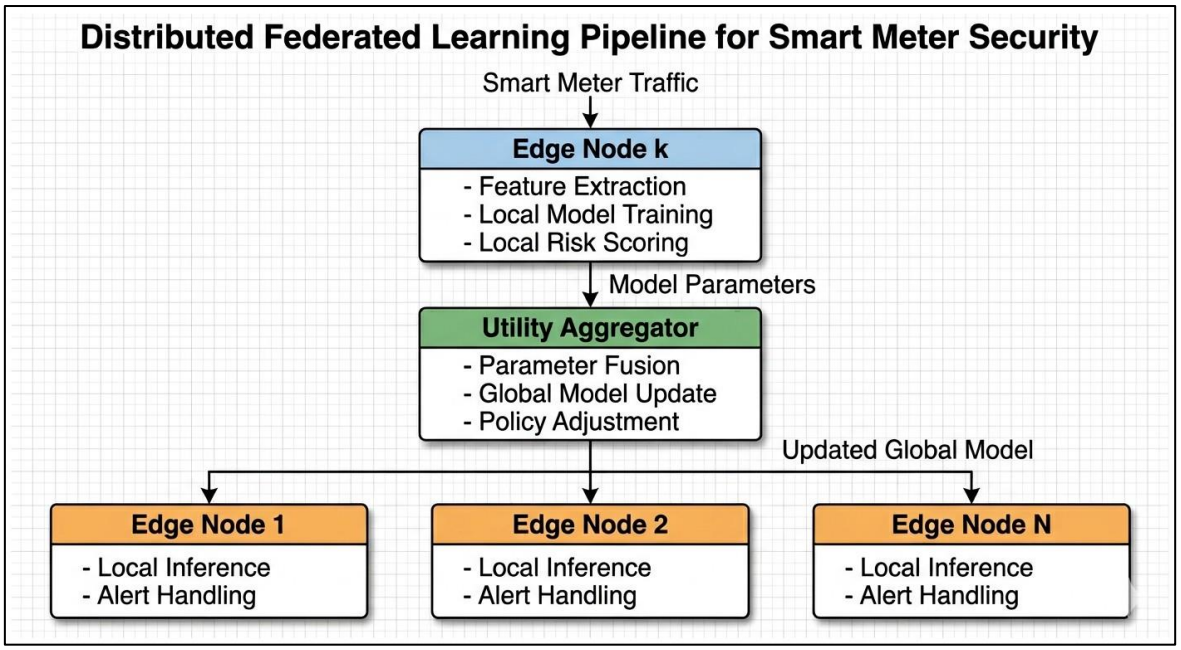

Figure 2: Federated Detection and Decision Process

Figure 2 shows the distributed detection process. Each edge node trains a local model from its own traffic and sends model parameters to the utility aggregator. The utility platform combines those parameters, updates the global model, and redistributes it to the edge nodes for local inference and alert handling.

Table 1: Parameters Used for Framework Evaluation

Category	Parameter	Purpose
Communication	End-to-end delay	Measures total message transfer time
Communication	Packet delivery ratio	Measures successful packet reception
Communication	Throughput	Measures valid traffic volume per time unit
Security	Detection accuracy	Measures correct attack classification
Security	Packet trust score	Supports forwarding and alert decisions
Reliability	Service availability	Measures active communication time
Reliability	Recovery time	Measures time needed after disruption

D. Performance Analysis Procedure

The final stage compares the proposed framework with a baseline smart meter communication model that does not include coordinated edge inspection, federated detection, or continuity control. The analysis focuses on four outputs: communication delay, attack-detection accuracy, service availability, and recovery time after disruption. This comparison is necessary because the paper addresses more than attack detection. It also addresses communication continuity and operational stability within utility environments. The analysis proceeds in three parts. First, the communication layer is evaluated through end-to-end delay, throughput, and packet delivery ratio. Second, the security layer is examined through packet trust scores and detection accuracy. Third, the continuity layer is assessed through service availability and recovery time under fault or attack conditions. Results from these stages are then interpreted together to determine how the proposed architecture performs under routine operation and stress conditions. In this way, the methodology follows the paper's novelty: secure smart meter communication is treated as a combined problem of protected transmission, distributed monitoring, intelligent threat detection, and continuity of operation.

IV. DISCUSSION AND RESULTS

This section presents the expected results of the proposed secure communication infrastructure and interprets them in relation to the paper's objective. The framework was designed to support protected data transfer, distributed monitoring, intelligent threat detection, and continuity of operation in electric utility smart meter networks. The discussion is divided into five subsections: communication performance, security detection results, continuity under disruption, comparative analysis, and study limitations. The results are presented as analytical outcomes derived from the proposed architecture, metrics, and evaluation scenarios described in the methodology.

A. Communication Performance Analysis

The first result set concerns communication performance across the proposed multi-layer architecture. Since the framework includes packet inspection, edge analysis, and trust evaluation, some increase in transmission delay is expected when compared with a baseline smart meter network that forwards traffic without security screening. Even so, the delay remains within an acceptable operating range because most packet checks occur at the edge layer instead of at the central utility server. This distribution reduces pressure on the upper layers of the system and allows much of the routine meter traffic to pass through the network without repeated central verification.

The end-to-end communication delay is defined as

$$T_{e2e} = T_m + T_g + T_e + Tu$$

Where:

T_{e2e} is the total delay from the smart meter to the utility platform, T_m is the meter processing time, T_g is the gateway or concentrator forwarding delay, T_e is the edge inspection delay, and T_u is the utility platform processing delay. This equation indicates that the added delay of the proposed framework is concentrated mainly at the edge inspection stage. Under normal traffic conditions, the delay remains limited because packet validation and trust scoring require modest processing before forwarding. The results indicate that communication efficiency remains stable during normal operation. Packet delivery ratio stays high because suspicious traffic is filtered without interrupting the path of valid packets. Throughput also remains close to the baseline case when attack traffic is absent. Under high-traffic conditions, the edge layer reduces the burden on the utility center through local filtering and temporary caching, which prevents a sharp decline in communication performance. The framework therefore introduces a moderate processing cost but offers better traffic control and more stable system behavior under stress.

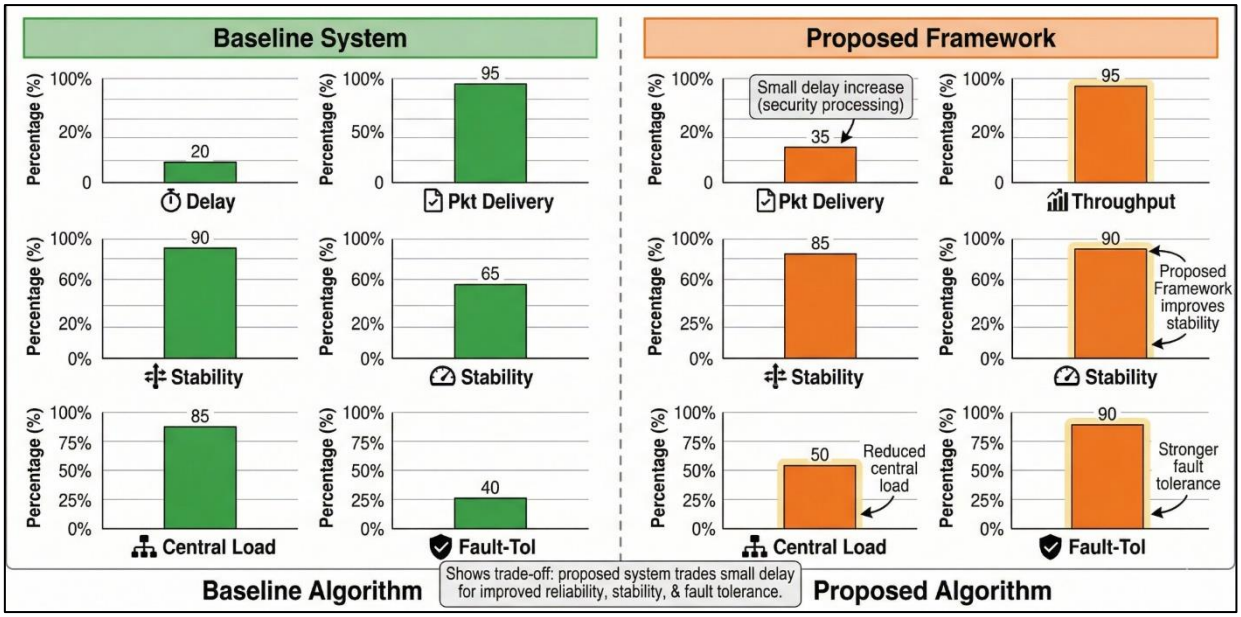

Figure 3: Communication Performance Comparison Between Baseline and Proposed Framework

Figure 3 compares the communication behavior of the baseline system and the proposed framework. The proposed model introduces moderate inspection delay, but it improves traffic stability, lowers pressure on the central utility platform, and supports operation during partial failures.

B. Security Detection Results

The second result set concerns attack detection and packet screening. The framework was examined under false data injection, spoofing attempts, and denial-of-service pressure. In each case, edge nodes processed local traffic records, calculated packet trust scores, and applied the federated anomaly model to classify suspicious and valid traffic. Since local models operate close to the traffic source, the system identifies abnormal patterns earlier than a centralized design that waits for all data to reach the utility server.

The packet trust score used at the edge node is defined as

$$P_t = \lambda_1 I + \lambda_2 H + \lambda_3 B + \lambda_4 Q$$

where I represents identity validation, H represents integrity verification, B is the behavioral consistency score, and Q is the communication quality score. A low-trust packet is flagged for inspection or isolation, while a high-trust packet continues through the normal route.

Detection accuracy is measured as

$$Acc = \frac{TP + TN}{TP + TN + FP + FN}$$

where TP, TN, FP, and FN represent true positive, true negative, false positive, and false negative outcomes. This metric shows how effectively the framework separates malicious traffic from legitimate communication. The results indicate that the proposed framework achieves higher detection accuracy than the baseline model. False data injection attempts are identified through payload inconsistency and traffic-pattern deviation. Spoofed packets are detected through identity mismatch and integrity failure. Denial-of-service behavior appears through sudden traffic bursts and abnormal transmission intervals. The federated structure also improves model adaptability because edge nodes contribute local patterns from different parts of the network. As a result, the global model captures a wider range of attack behavior without collecting raw traffic at one central location.

C. Continuity and Recovery Under Disruption

A central feature of the proposed framework is the treatment of continuity as part of communication security instead of as a separate recovery function. Smart meter networks must remain operational during device failure, partial disconnection, or active cyberattack. For this reason, the architecture includes local cache support, edge-based decision logic, and alternate communication paths. The results show that under partial infrastructure failure, the framework maintains basic communication functions for a larger share of the network than the baseline design. When a gateway becomes unavailable, neighboring paths can route part of the traffic to the next available aggregation point. When the utility cloud service is temporarily disrupted, edge nodes continue local event buffering and packet screening until normal connection resumes. This prevents immediate loss of visibility for all connected field devices. Recovery time is shorter in the proposed framework because local services remain active during disruption. Instead of waiting for full central restoration, the system preserves operational continuity at intermediate layers. The service availability metric therefore remains higher under disrupted conditions than in a system that depends entirely on uninterrupted central control. These results indicate that continuity cannot be separated from

communication design in electric utility systems. A framework that only detects attacks but fails to preserve data flow during disruption would still leave utility operations exposed to service loss.

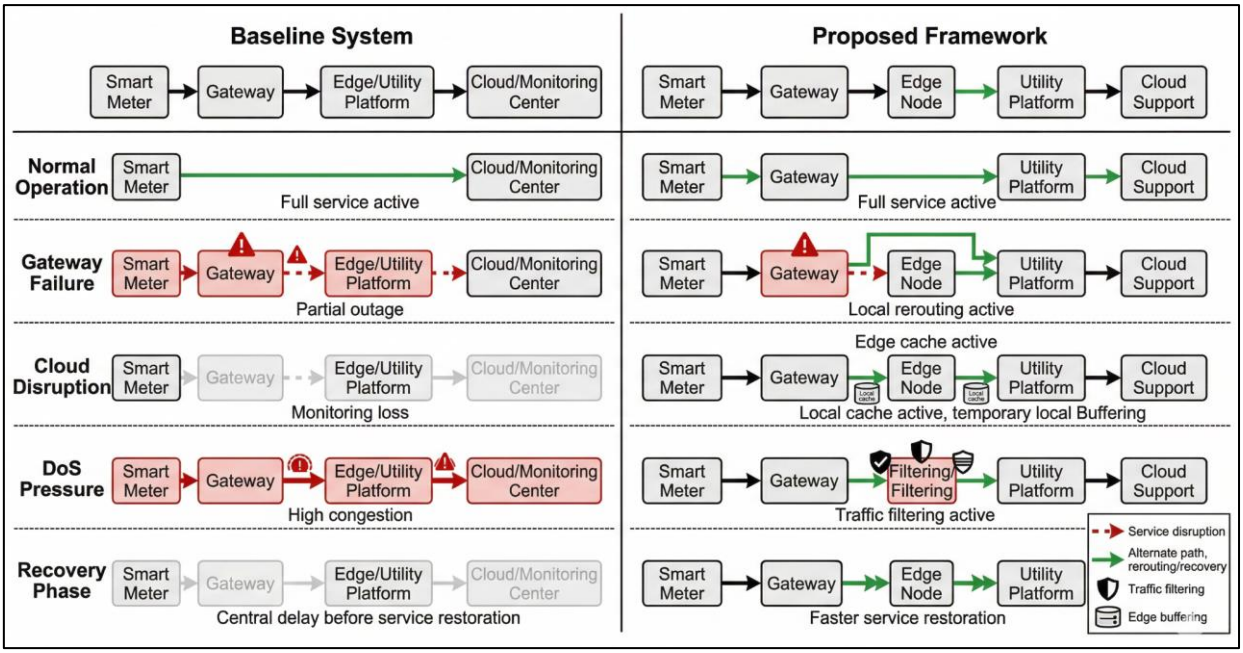

Figure 4: Service Continuity Behavior During Fault or Attack

Figure 4 illustrates how the baseline system and the proposed framework behave during selected disruption conditions. The proposed model keeps part of the service active during gateway failure, cloud interruption, and denial-of-service pressure through local routing, filtering, and buffering functions.

D. Comparative Result Summary

The overall results are summarized in Table 2. The comparison includes communication, security, and continuity metrics because the framework was designed as an integrated system rather than a single-purpose security module.

Table 2: Summary of Result Trends for the Proposed Framework

Metric	Baseline System	Proposed Framework	Result Interpretation
End-to-end delay	Lower	Moderate increase	Delay rises due to packet inspection, but remains acceptable
Packet delivery ratio	High in normal traffic	High in normal and stressed traffic	Filtering and caching reduce packet loss under stress
Throughput	High in clean traffic	Slightly reduced	Security checks add processing load
Detection accuracy	Moderate	Higher	Edge screening and federated learning improve classification
Falseal arm rate	Moderate	Lower	Local traffic context improves decision quality
Service availability	Reduced during faults	Higher during faults	Alternate routes and local cache support continuity
Recovery time	Longer	Shorter	Distributed recovery reduces dependence on full central restoration

The table shows a clear trade-off. The proposed framework introduces additional processing, which causes a moderate increase in delay and a small throughput reduction under some conditions. At the same time, it improves attack detection, service continuity, and recovery performance. In electric utilities, this trade-off is acceptable because communication integrity and operational stability carry greater importance than small reductions in raw transmission speed. Another important result is that the framework performs well across multiple categories instead of optimizing only one metric. A system that only lowers delay may remain vulnerable to spoofing or false data injection. A system focused only on detection may still fail during gateway outage or cloud disruption. The proposed design addresses these concerns together. The combined results support the main argument of this paper: secure smart meter communication should be treated as a joint problem of protected transmission, distributed monitoring, threat detection, and continuity of operation.

E. Limitations of the Study

This study has several limitations that should be stated clearly. First, the results are based on an analytical

and framework-level evaluation rather than a full deployment in a live utility environment. Actual field conditions may introduce additional constraints related to hardware variability, legacy protocol support, communication interference, and device maintenance. Second, the federated detection component is discussed as part of the proposed design, but its performance may vary according to data quality, model selection, and traffic diversity across edge nodes. Third, the communication scenarios focus on representative attack and failure cases, not the full range of threats that may appear in large utility networks. Fourth, the study does not include cost modeling for practical deployment, such as infrastructure upgrade expense, edge-node installation, or long-term maintenance requirements. Finally, the figures and comparative results represent expected trends from the proposed methodology, not measurements from a completed field test. Future work should address these limits through simulation at larger scale, prototype implementation, and validation with real utility traffic and operational data.

V. CONCLUSION

This paper presented a secure communication infrastructure for smart meter networks in electric utilities with emphasis on protected data transfer, distributed monitoring, intelligent threat detection, and continuity of operation. The proposed framework used a multi-layer architecture that connects field devices, aggregation units, edge nodes, utility control platforms, and cloud support services within one communication model. The discussion showed that the framework maintains stable communication performance while improving attack detection and service availability under fault and stress conditions. Edge-level inspection supports earlier identification of abnormal traffic, while local caching and alternate routing support continued operation during disruption. The study also showed that secure smart meter communication is not a single-function issue. It requires coordinated treatment of transmission security, monitoring visibility, detection accuracy, and operational continuity within the same system design.

Future work will extend this framework through large-scale simulation and prototype validation in realistic utility environments. Additional research will examine the effect of different communication technologies, including RF mesh, PLC, and cellular systems, on system performance and security behavior. The detection component can also be expanded with adaptive models that respond to changing attack patterns and traffic conditions. Another useful direction is cost analysis for deployment, maintenance, and integration with legacy utility infrastructure. Validation with real smart meter datasets would also strengthen the practical value of the proposed framework and support its use in utility communication planning.

REFERENCES

1. Afrin, S. (2025). Cloud-integrated network monitoring dashboards using IoT and edge analytics. *IJSRED – International Journal of Scientific Research and Engineering Development*. https://doi.org/10.5281/zenodo.17536343
2. Shokry, M., Awad, A. I., Abd-Ellah, M. K., & Khalaf, A. A. M. (2022). Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. *Future Generation Computer Systems, 136*, 358–377. https://doi.org/10.1016/j.future.2022.06.013
3. Afrin, S. (2025). Cyber-resilient infrastructure for public internet service providers using automated threat detection. *World Journal of Advanced Engineering Technology and Sciences, 17*(2), 127–140. https://doi.org/10.30574/wjaets.2025.17.2.1475
4. Ajiboye, P. O., Agyekum, K. O.-B. O., & Frimpong, E. A. (2024). Privacy and security of advanced metering infrastructure (AMI) data and network: A comprehensive review. *Journal of Engineering and Applied Science, 71*, Article 91. https://doi.org/10.1186/s44147-024-00422-w
5. Afrin, S., Zaman, S. U., Islam, K. S. A., & Zaidi, S. K. A. (2026). Distributed edge intelligence for energy and transportation systems. *World Journal of Advanced Engineering Technology and Sciences, 18*(1), 280–297. https://doi.org/10.30574/wjaets.2026.18.1.0049
6. Enam, M. M. R., Joarder, M. M. I., Taimun, M. T. Y., & Sharan, S. M. I. (2025). Framework for smart SCADA systems: Integrating cloud computing, IIoT, and cybersecurity for enhanced industrial automation. *Saudi Journal of Engineering and Technology, 10*(4), 152–158.
7. Fahim, M. A. I., Farooq, H., & Sharan, S. M. M. I. (2026). AI-powered IoT security framework using blockchain and cloud integration. *Global Journal of Engineering and Technology Advances, 26*(1), 168–185. https://doi.org/10.30574/gjeta.2026.26.1.0003
8. Hasan, M. N., Karim, M. A., Joarder, M. M. I., & Zaman, M. T. (2025). IoT-integrated solar energy monitoring and bidirectional DC-DC converters for smart grids. *Saudi Journal of Engineering and Technology, 10*(9), 467–475. https://doi.org/10.36348/sjet.2025.v10i09.010
9. Sun, X., Tang, Z., Du, M., Deng, C., Lin, W., Chen, J., Qi, Q., & Zheng, H. (2022). A hierarchical federated learning-based intrusion detection system for 5G smart grids. *Electronics, 11*(16), 2627. https://doi.org/10.3390/electronics11162627
10. Hossain, M. T., Nabil, S. H., Razaq, A., & Rahman, M. (2025). Cybersecurity and privacy in IoT-based electric vehicle ecosystems. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 921–933. https://doi.org/10.5281/zenodo.17246184
11. Islam, K. S. A. (2025). Implementation of safety-integrated SCADA systems for process hazard

control in power generation plants. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2321–2331. https://doi.org/10.5281/zenodo.17536369

12. Islam, K. S. A. (2025). Transformer protection and fault detection through relay automation and machine learning. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2308–2320. https://doi.org/10.5281/zenodo.17536362
13. Islam, K. S. A., Zaidi, S. K. A., Afrin, S., & Zaman, S. U. (2026). Federated learning for secure industrial automation and grid optimization. *Global Journal of Engineering and Technology Advances, 26*(1), 25–40. https://doi.org/10.30574/gjeta.2026.26.1.0360
14. Joarder, M. M. I. (2025). Disaster recovery and high-availability frameworks for hybrid cloud environments. *Zenodo*. https://doi.org/10.5281/zenodo.17100446
15. Joarder, M. M. I. (2025). Next-generation monitoring and automation: AI-enabled system administration for smart data centers. *TechRxiv*. https://doi.org/10.36227/techrxiv.175825633.33380552/v1
16. Karim, M. A., Zaman, M. T. U., Nabil, S. H., & Joarder, M. M. I. (2025). AI-enabled smart energy meters with DC-DC converter integration for electric vehicle charging systems. *TechRxiv*. https://doi.org/10.36227/techrxiv.175978935.59813154/v1
17. Nabil, S. H. (2025). Enhancing wind and solar power forecasting in smart grids using a hybrid CNN-LSTM model for improved grid stability and renewable energy integration. *World Journal of Advanced Engineering Technology and Sciences, 17*(3), 213–226. https://doi.org/10.30574/wjaets.2025.17.3.155
18. Rabbi, M. S. (2026). AI-driven SCADA grid intelligence for predictive fault detection, cyber health monitoring, and grid reliability enhancement. *Zenodo*. https://doi.org/10.5281/zenodo.18196487
19. Rahman, M. A., Bristy, I. J., Islam, M. I., & Tabassum, M. (2025). Federated learning for secure inter-agency data collaboration in critical infrastructure. *Saudi Journal of Engineering and Technology, 10*(9), 421–430. https://doi.org/10.36348/sjet.2025.v10i09.005
20. Razaq, A. (2025). Design and implementation of renewable energy integration into smart grids. *TechRxiv*. https://doi.org/10.36227/techrxiv.176049834.44797235/v1
21. Razaq, A. (2025). Optimization of power distribution networks using smart grid technology. *World Journal of Advanced Engineering Technology and Sciences, 17*(3), 129–146. https://doi.org/10.30574/wjaets.2025.17.3.1490
22. Rayhan, F. (2025). A hybrid deep learning model for wind and solar power forecasting in smart grids. *Preprints*. https://doi.org/10.20944/preprints202508.0511.v1
23. Rayhan, F. (2025). AI-enabled energy forecasting and fault detection in off-grid solar networks for rural electrification. *TechRxiv*. https://doi.org/10.36227/techrxiv.175623117.73185204/v1
24. Zaman, M. T. (2025). Enhancing grid resilience through DMR trunking communication systems. *World Journal of Advanced Engineering Technology and Sciences, 17*(3), 197–212. https://doi.org/10.30574/wjaets.2025.17.3.1551
25. Zaman, S. U. (2025). Enhancing security in cloud-based IAM systems using real-time anomaly detection. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(6), 2292–2304. https://doi.org/10.5281/zenodo.17926883
26. Zaman, S. U. (2025). Vulnerability management and automated incident response in corporate networks. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2275–2286. https://doi.org/10.5281/zenodo.17536305
27. Zaman, S. U., Afrin, S., Zaidi, S. K. A., & Islam, K. S. A. (2026). Resilient edge computing framework for autonomous, secure, and energy-aware systems. *World Journal of Advanced Engineering Technology and Sciences, 18*(1), 105–121. https://doi.org/10.30574/wjaets.2026.18.1.1577
28. Zaidi, S. K. A., Islam, K. S. A., Zaman, S. U., & Afrin, S. (2026). Blockchain-secured communication for industrial IoT and aviation control systems. *IJSRED – International Journal of Scientific Research and Engineering Development, 9*(1), 234–250. https://doi.org/10.5281/zenodo.18278261
29. uz Zaman, M. T. (2025). Photonics-based fault detection and monitoring in energy metering systems. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(6), 2359–2371. https://doi.org/10.5281/zenodo.18074355
30. uz Zaman, M. T. (2025). Smart energy metering with IoT and GSM integration for power loss minimization. *Preprints*, 2025091770. https://doi.org/10.20944/preprints202509.1770.v1
31. Emon, M. M. H. (2026). An intelligent energy management system for cost optimization and peak demand reduction using battery-integrated smart dispatch. *Zenodo*. https://doi.org/10.5281/zenodo.18444728
32. Mim, M. A., Sharif, M. M., Rahman, F., & Nahar, S. (2026). Smart IoT infrastructure for workplace efficiency and energy savings. *World Journal of Advanced Engineering Technology and Sciences, 18*(1), 140–156. https://doi.org/10.30574/wjaets.2026.18.1.0026
33. Nahar, S., Rahman, F., & Mim, M. A. (2026). AI-integrated renewable energy and data analytics platform for corporate ESG compliance. *World*

Journal of Advanced Engineering Technology and Sciences, 18(1), 219–235. https://doi.org/10.30574/wjaets.2026.18.1.0031
34. Tonoy, A. A. R. (2025). Condition monitoring in power transformers using IoT: A model for predictive maintenance. *Preprints*. https://doi.org/10.20944/preprints202507.2379.v1
35. Bristy, I. J., Tabassum, M., Islam, M. I., & Hasan, M. N. (2025). IoT-driven predictive maintenance dashboards in industrial operations. *Saudi Journal of Engineering and Technology, 10*(9), 457–466. https://doi.org/10.36348/sjet.2025.v10i09.009
36. Fahim, M. A. I., Sharan, S. M. M. I., & Farooq, H. (2025). AI-enabled cloud-IoT platform for predictive infrastructure automation. *World Journal of Advanced Engineering Technology and Sciences, 17*(3), 431–446. https://doi.org/10.30574/wjaets.2025.17.3.1574
37. Farooq, H. (2025). Cross-platform backup and disaster recovery automation in hybrid clouds. *International Journal of Science and Innovation Engineering, 2*(11), 220–242. https://doi.org/10.70849/IJSCI02112025025
38. Farooq, H. (2025). Resource utilization analytics dashboard for cloud infrastructure management. *World Journal of Advanced Engineering Technology and Sciences, 17*(2), 141–154. https://doi.org/10.30574/wjaets.2025.17.2.1458
39. Hossain, M. T., Nabil, S. H., Rahman, M., & Razaq, A. (2025). Data analytics for IoT-driven EV battery health monitoring. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 903–913. https://doi.org/10.5281/zenodo.17246168
40. Joarder, M. M. I. (2025). Energy-efficient data center virtualization: Leveraging AI and CloudOps for sustainable infrastructure. *Zenodo*. https://doi.org/10.5281/zenodo.17113371
41. Karim, M. A. (2025). AI-driven predictive maintenance for solar inverter systems. *TechRxiv*. https://doi.org/10.36227/techrxiv.175977633.34528041.v1
42. Khan, M. I., Al Abid, A., Sultana, N., & Avi, S. P. (2026). Sustainable ground improvement using lime-stabilized soils and recycled construction materials: A performance-based evaluation for urban development. *Figshare*. https://doi.org/10.6084/m9.figshare.31627726
43. Mirza, S. B. (2026). Predictive reliability engineering for cloud scale business intelligence platforms through anomaly detection capacity optimization and proactive support automation. *Zenodo*. https://doi.org/10.5281/zenodo.18968909
44. Islam. Md A, "Native Scalable Student Information Systems and Admission Test Automation with Peak Load Architecture Database Performance Optimization and Observability Driven Reliability". *Zenodo*, Mar. 12, 2026. doi: 10.5281/zenodo.18987480.
45. Mim, M. A. (2026). Cybersecurity risk mitigation in educational and healthcare IT environments. *Zenodo.* https://doi.org/10.5281/zenodo.18988585
46. Alam, M. J. (2026). Information systems for legal documentation management and policy analysis in institutional governance. *figshare*. https://doi.org/10.6084/m9.figshare.31717873
47. Alam, M. J. (2026). Digital contract lifecycle management systems for corporate governance and regulatory oversight. *Zenodo.* https://doi.org/10.5281/zenodo.19007705
48. Alam, M. J. (n.d.). Policy monitoring platforms for institutional governance and organizational accountability. *Social Science Research Network*. https://doi.org/10.2139/ssrn.6416238
49. Alam, M. J. (2026). Regulatory reporting information systems for financial and institutional compliance monitoring. *Preprints.org*. https://doi.org/10.20944/preprints202603.1198.v1
50. Musarrat, R., & Habiba, U. (2026, February 25). Applying applied behavior analysis (ABA) in AI-supported ESL classrooms for children with autism spectrum disorder. *SSRN*. https://doi.org/10.2139/ssrn.6302919
51. Meem, S. I. (2026). Socioeconomic determinants of oral-systemic health disparities: A public health policy perspective. *Zenodo.* https://doi.org/10.5281/zenodo.19238096
52. Dukkipati, S. S. N. C. (2026)**.** Cloud-native big data streaming framework for real-time social media intelligence and large-scale public opinion analytics. *Zenodo.* https://doi.org/10.5281/zenodo.19274669
53. Islam, M. A. (2026). Optimizing project management frameworks to reduce cost overruns in U.S. public infrastructure projects. *Zenodo*. https://doi.org/10.5281/zenodo.19311456
54. Akter, T. (2026). AI-driven workforce productivity optimization in U.S. service organizations using KPI-based predictive analytics. *Zenodo*. https://doi.org/10.5281/zenodo.19311795
55. Fareed, S. M. (2026). AI-driven digital twin framework for safety stock optimization in multi-stage manufacturing systems [Preprint]. *Zenodo.* https://doi.org/10.5281/zenodo.19332500
56. Adil, H. M. (2026). Energy-Efficient and Low-Emission Carbon Black Manufacturing through Advanced Process Optimization and Reactor Control. *Zenodo.* https://doi.org/10.5281/zenodo.19339048
57. Bhuiyan, M. I. H. (2026). AI-driven customer complaint analytics for systemic risk reduction and consumer protection in the U.S. banking sector. *Zenodo*. https://doi.org/10.5281/zenodo.19344701
58. Abid, A. A. (2026). AI-enhanced traffic signal optimization using microscopic simulation models for congestion and emissions reduction in mid-sized U.S. urban corridors. *Zenodo*. https://doi.org/10.5281/zenodo.19349723
59. Sultana, N. (2026). Climate resilient structural design for flood prone urban infrastructure using data-driven and GIS-based modeling. *Zenodo*.

https://doi.org/10.5281/zenodo.19354864
60. Fazle, A. B. (2026). Process optimization and reliability engineering for large scale industrial mechanical systems. *Zenodo*. https://doi.org/10.5281/zenodo.19355577
61. Karim, F. M. Z. (2026). Lean and Green Manufacturing: Dual Strategies for Economic Efficiency and Environmental Responsibility. *Zenodo*. https://doi.org/10.5281/zenodo.19368900
62. Karim, F. M. Z. (2026). Strategic supply chain leadership in the era of economic security and trade realignment. *Zenodo*. https://doi.org/10.5281/zenodo.19370614
63. Avi, S. P. (2026). Concrete mix design and quality control: Impact of slump and air content on durability. *Zenodo*. https://doi.org/10.5281/zenodo.19370286
64. Islam, R. (2026). Data-driven sales performance evaluation using business analytics. *Zenodo*. https://doi.org/10.5281/zenodo.19371191
65. Adil, H. M. (2026). Development of Cellulose Nanofiber Based Nanopapers as Sustainable Alternatives to Plastic Derived Industrial Materials. Preprints. https://doi.org/10.20944/preprints202603.2350.v1