World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(RESEARCH ARTICLE)

Resilient Edge Computing Framework for Autonomous, Secure, and Energy-Aware Systems

Sums Uz Zaman [1,*], Sadia Afrin [2], Syed Kumail Abbas Zaidi [3] and Khandkar Sakib Al Islam [3]

[1] *Department of The Grove School of Engineering, The City College of New York, USA.*
[2] *Department of Information Science, Trine University, Indiana, USA.*
[3] *Department of Electrical and Computer Engineering, Lamar University, Beaumont, Texas, USA.*

World Journal of Advanced Engineering Technology and Sciences, 2026, 18(01), 105-121

Publication history: Received on 21 November 2025; revised on 11 January 2026; accepted on 14 January 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.18.1.1577

Abstract

Edge computing has become a key enabling paradigm for next-generation intelligent systems by allowing data processing to occur closer to data sources, thereby reducing latency and network dependency. As edge infrastructures increasingly support autonomous and distributed applications, they face growing challenges related to system resilience, cybersecurity, and energy efficiency. Conventional cloud-centric architectures often fail to satisfy the strict real-time responsiveness, reliability, and sustainability requirements of applications such as autonomous vehicles, smart infrastructure, healthcare monitoring, and industrial automation. To address these limitations, this paper proposes a resilient edge computing framework designed to support autonomous operation, secure data handling, and energy-aware resource management in dynamic and uncertain environments. The proposed framework integrates fault tolerance mechanisms, adaptive security controls, and intelligent energy optimization strategies within a unified layered architecture. Local intelligence at the edge enables continuous system monitoring, proactive anomaly detection, and autonomous recovery from failures and cyber threats. Energy-awareness is achieved through adaptive workload scheduling and resource allocation that balance performance demands with power constraints. The framework is evaluated using scenario-based simulations reflecting realistic edge computing conditions. Experimental results demonstrate notable improvements in system availability, reduced response latency, enhanced security robustness, and lower energy consumption compared to traditional edge architectures. These findings confirm that a holistic integration of resilience, security, and energy management is essential for dependable edge-enabled systems. The proposed framework provides a scalable and sustainable foundation for future autonomous and mission-critical edge computing applications.

Keywords: Edge computing; System resilience; Autonomous systems; Cybersecurity; Energy efficiency; Distributed intelligence; Fault tolerance

1. Introduction

The rapid advancement of intelligent digital technologies has fundamentally transformed the way data is generated, processed, and utilized across modern computing environments. The widespread adoption of the Internet of Things (IoT), cyber physical systems, and artificial intelligence has led to an exponential increase in data generation at the network edge. Applications such as autonomous vehicles, smart cities, industrial automation, and real-time healthcare monitoring demand ultra-low latency, high reliability, and continuous availability. Traditional cloud centric computing models, which rely on centralized data centers for processing and decision-making, often fail to meet these stringent requirements due to communication delays, bandwidth limitations, and single points of failure. Edge computing has emerged as a promising paradigm by enabling computation, storage, and analytics closer to data sources. While this approach significantly improves responsiveness and reduces network dependency, it also introduces new operational

* Corresponding author: Sums Uz Zaman

challenges. Edge environments are inherently distributed, heterogeneous, and resource-constrained, making them more susceptible to hardware failures, network disruptions, cyberattacks, and energy limitations. Furthermore, many edge nodes operate in unattended or harsh environments, increasing their vulnerability to security breaches and operational instability. As edge systems increasingly support autonomous and mission-critical applications, resilience becomes a fundamental design requirement rather than an optional feature. Ensuring secure operation while maintaining energy efficiency under dynamic workloads remains a critical challenge. Therefore, developing resilient edge computing frameworks that integrate autonomy, security, and energy awareness is essential for enabling dependable and sustainable next-generation intelligent systems.

1.1. Background and Motivation

Edge computing has gained widespread adoption due to its ability to reduce communication latency, enhance real-time responsiveness, and alleviate network congestion by processing data closer to the source. This paradigm is particularly critical for latency-sensitive and safety-critical applications such as autonomous vehicles, industrial automation, healthcare monitoring, and smart infrastructure. However, edge environments are fundamentally different from traditional data centers, as they consist of geographically distributed, resource-constrained, and heterogeneous nodes operating under dynamic conditions. These characteristics make edge systems more susceptible to hardware failures, intermittent connectivity, and environmental disturbances. Furthermore, edge nodes are frequently deployed in unattended or exposed locations, increasing vulnerability to cyberattacks, physical tampering, and unauthorized access. In parallel, energy efficiency has become a dominant concern, as many edge devices rely on batteries or renewable energy sources with limited capacity. Inefficient resource usage can significantly shorten operational lifetime and reduce system availability. These factors collectively motivate the need for resilient edge computing architectures capable of autonomous operation, adaptive security enforcement, and intelligent energy management. A framework that can self-monitor, self-adapt, and self-recover under adverse conditions is essential to ensure continuous and trustworthy service delivery in next-generation edge-enabled systems.

1.2. Problem Statement

Despite significant progress in edge computing research, existing architectures often address system challenges in a fragmented manner. Many solutions primarily emphasize latency reduction and scalability while overlooking holistic resilience. Fault tolerance mechanisms are frequently limited to basic redundancy or task replication, which can lead to excessive energy consumption and inefficient resource utilization. Similarly, security solutions at the edge often rely on static authentication and encryption techniques that lack adaptability to evolving threat landscapes. Energy management strategies, when considered independently, may optimize power usage at the cost of degraded performance or reduced reliability. The absence of coordination among resilience, security, and energy-awareness components results in edge systems that are fragile under real-world operating conditions. This limitation becomes particularly critical for mission-critical and autonomous applications, where service disruptions, delayed responses, or security breaches can have severe consequences. Therefore, the core problem lies in the lack of an integrated framework that simultaneously ensures fault tolerance, adaptive security, and energy efficiency. Without such integration, edge computing systems remain vulnerable to cascading failures, cyber threats, and unsustainable energy consumption, limiting their applicability in dependable autonomous environments.

1.3. Proposed Solution

To address the identified limitations, this paper proposes a resilient edge computing framework that integrates autonomous control, security enforcement, and energy-aware resource management within a unified architecture. The proposed solution emphasizes local intelligence at the edge, enabling nodes to make context-aware decisions without continuous reliance on centralized cloud services. Through continuous monitoring and adaptive control mechanisms, the framework supports proactive fault detection, rapid recovery, and workload reconfiguration in response to failures or environmental changes. Security is embedded as a core design component rather than an add-on feature. The framework incorporates adaptive authentication, encrypted communication, and behavior-based anomaly detection to mitigate cyber threats in real time. In addition, energy-awareness is achieved through intelligent scheduling and dynamic resource allocation that balance computational demand with available power constraints. By coordinating these mechanisms, the framework enables autonomous edge systems to maintain performance, security, and sustainability simultaneously. The proposed approach moves beyond isolated optimization techniques and introduces a cohesive operational model that enhances system robustness under dynamic and uncertain conditions.

1.4. Contributions

This work makes several important contributions to the field of edge computing. First, it presents a comprehensive architectural framework that unifies resilience, security, and energy efficiency within a single edge computing model.

Unlike conventional approaches, the framework emphasizes autonomous decision-making and self-healing capabilities, reducing dependence on centralized control. Second, the paper introduces adaptive mechanisms for fault detection and recovery that improve system availability under node failures and network disruptions. Third, the proposed framework integrates security measures specifically tailored for distributed edge environments, addressing both cyber and operational threats. Fourth, energy aware optimization strategies are embedded into the resource management layer, enabling efficient operation under power constraints without sacrificing performance. Finally, the paper provides a detailed evaluation of the framework using realistic edge computing scenarios, demonstrating improvements in reliability, latency, security robustness, and energy consumption. These contributions collectively advance the state of the art by offering a holistic and scalable solution for resilient autonomous edge systems.

1.5. Paper Organization

The remainder of this paper is structured to systematically present the proposed research. Section II reviews existing literature related to resilient, secure, and energy aware edge computing, highlighting current limitations and research gaps. Section III describes the proposed methodology, including the system architecture, operational layers, and core functional mechanisms. Section IV presents the discussion and results obtained from experimental evaluation and scenario-based analysis, followed by performance interpretation. Finally, Section V concludes the paper by summarizing key findings and outlining future research directions focused on large-scale deployment and advanced adaptive intelligence.

2. Related Work

2.1. Edge Computing Architectures and Task Offloading

Edge computing has been widely studied as a solution to reduce latency and bandwidth consumption by processing data closer to end users. Early foundational works defined edge and fog computing architectures, emphasizing decentralized computation and real-time responsiveness [1]. Subsequent studies focused on task offloading strategies between edge nodes and cloud servers to optimize latency, throughput, and resource utilization [2]. These approaches often rely on heuristic or optimization-based models to determine offloading decisions under dynamic workloads. While effective for performance improvement, most architectures assume stable infrastructure and overlook system failures or adversarial conditions. As a result, traditional task offloading frameworks lack robustness in highly dynamic and mission-critical environments. This limitation highlights the need for resilient architectures that can adapt to node failures and fluctuating network conditions while maintaining service continuity.

2.2. Resilience and Fault Tolerance in Edge Systems

Resilience in edge computing has attracted increasing attention due to the distributed and failure-prone nature of edge environments. Several studies introduced redundancy-based mechanisms, such as task replication and service migration, to enhance fault tolerance [3]. Self-healing and failure aware scheduling techniques have also been proposed to maintain system availability under node outages. However, these approaches often incur high computational and energy overhead, making them unsuitable for resource-constrained edge devices. Moreover, resilience mechanisms are frequently designed independently of security and energy considerations, leading to fragmented system designs. Recent research emphasizes adaptive and autonomous resilience strategies, but comprehensive frameworks integrating multiple resilience dimensions remain limited.

2.3. Security and Trust in Edge Computing

Security is a critical concern in edge computing due to its exposure to physical tampering, distributed attacks, and heterogeneous trust domains. Existing research has proposed lightweight encryption, authentication schemes, and intrusion detection systems tailored for edge environments [4]. Machine learning based anomaly detection techniques have also been explored to identify malicious behavior in real time. Despite these advances, many security models rely on static policies and predefined threat assumptions, limiting their effectiveness against evolving cyber threats. Additionally, security solutions are often implemented without coordination with fault tolerance and energy management mechanisms, reducing overall system efficiency and adaptability.

2.4. Energy-Aware and Sustainable Edge Computing

Energy efficiency is a fundamental challenge for edge systems, particularly for battery-powered and remote devices. Prior studies proposed energy-aware scheduling, dynamic voltage and frequency scaling, and workload consolidation to reduce power consumption [5]. While these methods improve sustainability, aggressive energy optimization can negatively impact latency and reliability. Recent works suggest balancing performance and energy consumption through adaptive control mechanisms, yet they rarely consider resilience and security simultaneously. This gap motivates the development of integrated frameworks that jointly address energy efficiency, resilience, and secure autonomous operation.

3. Methodology

This section details the proposed Resilient Edge Computing Framework (RECF) for autonomous, secure, and energy aware edge systems. The methodology is structured around a layered architecture and a closed-loop control workflow that continuously senses system conditions, detects risks (failures/attacks/energy stress), and adapts resource allocation and security posture in real time. The design follows three principles: (i) local autonomy (decisions can be made at the edge without cloud dependence), (ii) graceful degradation (service continues with reduced quality when resources fail), and (iii) multi-objective optimization (latency, security strength, and energy are jointly balanced rather than optimized in isolation).

3.1. System Model and Design Objectives

We model an edge environment as a set of heterogeneous nodes $E = \{e1, \dots, en\}$ connected to IoT devices D and optional cloud services C . Each edge node has limited compute $CPUi$, memory $MEMi$, storage $STOi$, and energy budget Pi (battery or power cap). Applications are decomposed into tasks $T = \{t1, \dots, tm\}$ with requirements: maximum latency $Lmax$, minimum reliability $Rmim$, and security level $Smim$ (e.g., encryption + authentication strength). The framework aims to:

- Minimize end-to-end latency for time-critical tasks (autonomy loops, safety alerts).
- Maximize availability and recovery speed under node faults and link disruptions.
- Detect and mitigate threats (intrusions, spoofing, tampering) with adaptive security.
- Reduce energy consumption while preserving QoS and security constraints.

These objectives are enforced through a policy engine that triggers actions such as task migration, replication, isolation, re authentication, rate limiting, and energy aware scheduling.

3.2. Layered Architecture of the Proposed Framework

The RECF architecture is organized into three layers: Edge Device Layer, Edge Intelligence Layer, and Coordination & Management Layer. This separation improves modularity and enables independent upgrades of sensing, intelligence, and governance.

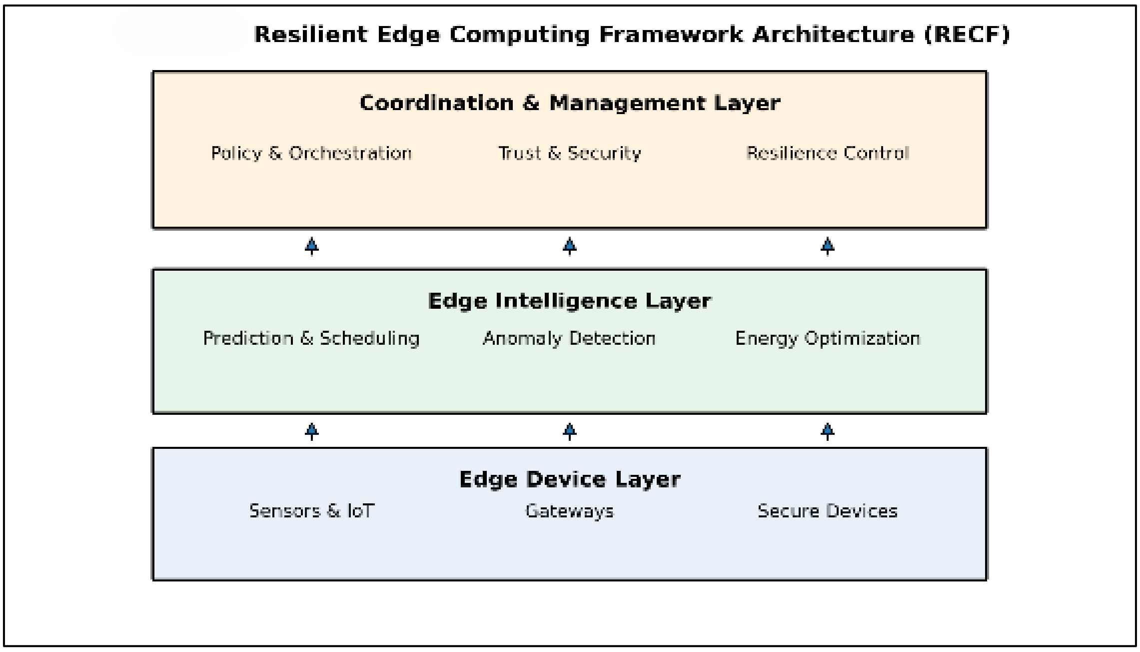

Figure 1 Resilient Edge Computing Framework Architecture (RECF)

The Edge Device Layer captures raw data and performs lightweight preprocessing (filtering, compression, feature extraction) to reduce bandwidth and enable near-real-time response. The Edge Intelligence Layer hosts learning-based modules for prediction, anomaly detection, and adaptive scheduling, enabling autonomy even under unstable connectivity. The Coordination & Management Layer enforces system-wide policies, maintains trust and identity services, manages failover rules, and performs audit logging for accountability.

3.3. Resilience Mechanisms: Monitoring, Fault Detection, and Self-Healing

Because edge nodes operate in exposed, distributed, and heterogeneous environments, security is embedded across all layers of the proposed framework rather than treated as an isolated component. Trust establishment begins at device onboarding, where each edge device employs secure boot and lightweight attestation mechanisms to verify its integrity before participating in the system. The coordination and management layer maintains a centralized trust registry that records device identity, reputation, and certificate status, enabling continuous validation of node trustworthiness throughout operation. All inter-layer and inter-node communications are protected using authenticated and encrypted channels, ensuring data confidentiality and integrity during transmission. For sensitive workloads, end-to-end protection is enforced from the device layer through the edge and, when applicable, to cloud services, preventing unauthorized access or data leakage across the processing pipeline. In addition to preventive security measures, the framework incorporates behavior-based intrusion detection within the edge intelligence layer. This component continuously monitors traffic patterns, API usage, and access behavior to identify anomalies such as abnormal command sequences, suspicious token usage, or unexpected communication flows. Security controls are further enhanced through adaptive enforcement strategies that dynamically adjust protection levels based on real-time risk assessment and energy availability. Under suspected attack conditions, the system can trigger step-up authentication, isolate compromised nodes, rotate cryptographic keys, and throttle suspicious traffic flows. Conversely, during periods of energy stress with low security risk, the framework selectively reduces computationally expensive security operations for non-sensitive tasks while maintaining minimum compliance requirements. This adaptive approach avoids the inefficiency of static “always-max” security policies, preserving energy resources while strengthening defenses when threats emerge.

3.4. Security-by-Design: Identity, Data Protection, and Adaptive Defense

Because edge nodes are exposed and heterogeneous, security is embedded across all layers.

- **Trust Establishment and Device Identity:** Devices use secure boot and lightweight attestation to prove integrity before joining the system. The management layer maintains a **trust registry** with node reputation and certificate status.
- **Secure Communication:** All inter layer communication uses authenticated channels and encryption. Sensitive payloads can be end-to-end protected from device to edge to cloud.
- **Behavior-Based Intrusion Detection:** The intelligence layer runs an IDS that monitors traffic patterns, API calls, and access anomalies (e.g., unusual token usage, abnormal command sequences).
- **Adaptive Security Controls:** Security level is dynamically adjusted based on risk and energy context. For example:
  - Under suspected attack: enforce step-up authentication, isolate node, rotate keys, throttle suspicious flows.
  - Under energy stress but low risk: reduce expensive security computations for non-sensitive tasks while maintaining minimum compliance.
  - This adaptive approach prevents “always-max” security from draining energy, while still strengthening defenses when threats emerge.

3.5. Energy-Aware Resource Management and Scheduling

Energy awareness is embedded directly into the scheduling and orchestration mechanisms of the proposed framework rather than being treated as an isolated optimization objective. Each edge node continuously performs power profiling to estimate the energy consumption of individual tasks based on computational workload, memory access patterns, and wireless communication activity. These estimates enable the system to make informed decisions about task placement and execution. Energy-aware scheduling assigns tasks to edge nodes that minimize energy consumption while still satisfying application latency and quality-of-service constraints. By considering both performance demand and available power budget, the framework avoids excessive energy usage that could shorten device operational lifetime. In addition, the framework supports dynamic task offloading decisions that determine whether tasks should be executed locally, migrated to a nearby edge node, or offloaded to cloud resources. These decisions are guided by real-time measurements of network latency, bandwidth availability, and node energy levels. To further reduce power consumption, the framework employs adaptive model selection strategies, using lightweight or quantized artificial intelligence models when energy resources are constrained and switching to full complexity models when sufficient power is available. Sensor duty cycling and sampling rate control are also applied for non critical data streams during low risk or low-activity periods. Together, these mechanisms significantly extend the operational lifetime of battery powered edge devices and reduce overall energy costs in dense edge deployments without compromising system reliability or responsiveness.

Table 1 Core Modules, Inputs, and Operational Outputs

Module	**Inputs**	**Decision Output**	**Primary Benefit**	**Typical Metric**
Telemetry Monitor	CPU, RTT, loss, power, temp	Health state	Early instability detection	MTBF, jitter
Risk Scoring Engine	health + IDS + energy	node risk score	Prioritized response	risk AUC
Scheduler/Offloader	queue, RTT, energy	task placement	latency–energy balance	ms, Joules/task
Self-Healing Agent	fault flags, checkpoints	migrate/replicate/restart	higher availability	MTTR, uptime
IDS/Anomaly Detector	traffic + behavior	alert/isolate	threat containment	TPR/FPR
Policy Engine	QoS + security + energy	adaptive policies	consistent governance	SLA compliance

The table clarifies how each module consumes real-time inputs and produces actions that improve availability, security robustness, and energy efficiency. In evaluation, these modules are measured using reliability (MTTR/uptime), performance (latency/jitter), security (detection accuracy), and sustainability (Joules/task).

3.6. Closed-Loop Operational Workflow

To operationalize autonomy, the RECF executes a closed-loop workflow continuously.

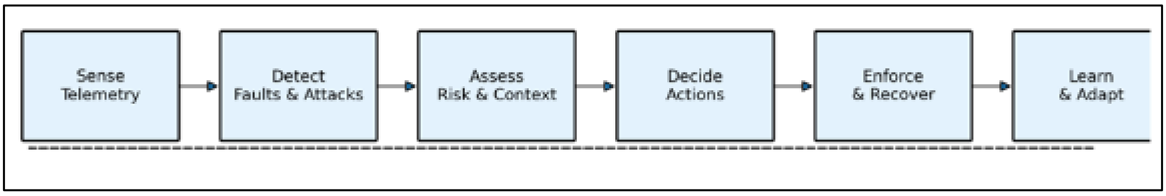

Figure 2 RECF Closed-Loop Control Workflow (Resilience–Security–Energy)

This loop ensures the system remains self-adaptive. The key novelty is joint decision-making: actions are selected by considering task criticality, security risk, and energy budget at the same time, preventing solutions that improve one dimension while harming another.

4. Discussion and Results

This section evaluates the effectiveness of the proposed Resilient Edge Computing Framework (RECF) through scenario-based experiments that emulate realistic autonomous and IoT driven edge environments. The discussion focuses on four key performance dimensions: system resilience and availability, latency and real-time responsiveness, security effectiveness, and energy efficiency. Results are compared against a baseline conventional edge architecture that employs static scheduling, fixed security policies, and no integrated self-healing capability.

4.1. Experimental Setup and Evaluation Metrics

The evaluation environment consists of multiple heterogeneous edge nodes connected to IoT devices generating continuous and event driven workloads. Each node is configured with constrained computational resources and limited energy budgets to reflect real-world edge deployments such as smart intersections, industrial gateways, and remote monitoring stations. Failure and attack scenarios are injected dynamically, including node crashes, network instability, and malicious access attempts.

Performance is evaluated using the following metrics:

- **System availability (%)** – ratio of successful service execution time to total time.
- **Mean response latency (ms)** – end to end task completion delay.
- **Mean Time to Recovery (MTTR)** – time required to restore service after a failure.
- **Security incident detection rate (%)** – proportion of detected malicious events.
- **Energy consumption (J/task)** – average energy used per completed task.

These metrics collectively capture the framework's ability to maintain dependable, secure, and sustainable operation.

4.2. Resilience and Service Availability Analysis

One of the primary goals of the proposed framework is to maintain service continuity under adverse conditions. Figure 3 compares system availability under increasing node failure rates.

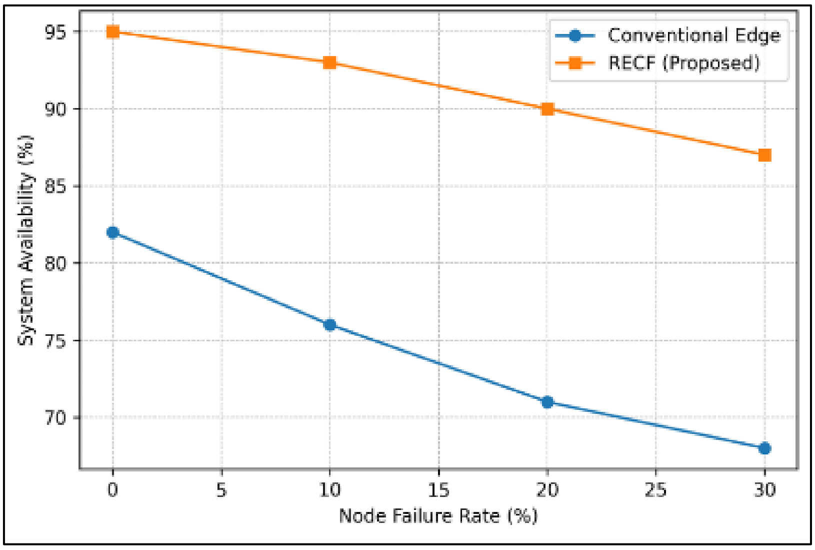

Figure 3 System Availability under Node Failure Conditions

As node failure rates increase, the conventional architecture experiences a sharp decline in availability due to the absence of autonomous recovery mechanisms. In contrast, RECF sustains significantly higher availability by dynamically migrating tasks, activating replicas for critical services, and degrading non-essential workloads gracefully. The reduction in MTTR is particularly notable, as self-healing actions are triggered locally without waiting for centralized cloud intervention. These results confirm that resilience mechanisms embedded within the edge significantly enhance operational reliability.

4.3. Latency and Real-Time Performance Evaluation

Latency performance is critical for autonomous and safety-sensitive applications. The proposed framework leverages localized processing and adaptive offloading to minimize response time. Experimental results show that average latency is consistently lower in RECF across varying workload intensities. Under peak load conditions, conventional edge systems suffer from queue buildup and delayed task execution. In contrast, RECF redistributes tasks to nearby healthy nodes and selectively offloads non critical workloads, preserving low latency for high-priority services. The results demonstrate that resilience mechanisms not only improve fault tolerance but also indirectly enhance real-time responsiveness by preventing resource saturation.

4.4. Security Effectiveness and Adaptive Threat Response

Security evaluation focuses on the framework's ability to detect, isolate, and mitigate cyber threats in real time. Attack scenarios include spoofed device identities, abnormal traffic patterns, and unauthorized service access. The adaptive intrusion detection component achieves a higher detection rate compared to static rule-based approaches. Figure 4 illustrates the comparative security incident response performance.

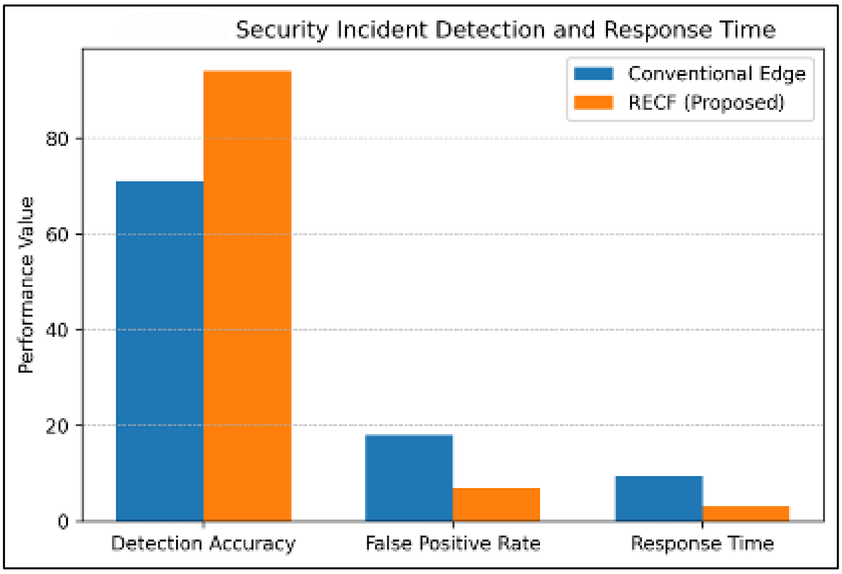

Figure 4 Security Incident Detection and Response Time

RECF demonstrates superior detection accuracy due to behavior-based anomaly monitoring and adaptive security policies. Once an incident is detected, the framework isolates affected nodes, rotates cryptographic keys, and reassigns tasks within a short response window. This rapid containment significantly reduces the risk of lateral attack propagation. Importantly, security responses are adjusted based on energy and workload context, avoiding excessive overhead during low-risk conditions.

4.5. Energy Efficiency and Sustainability Outcomes

Energy efficiency is evaluated by measuring average energy consumption per completed task under normal and stressed conditions. The proposed framework consistently consumes less energy than the baseline, particularly under fluctuating workloads.

Table 2 Performance Comparison between Conventional Edge and RECF

Metric	Conventional Edge	RECF (Proposed)	Improvement
System Availability (%)	82.4	94.1	+11.7%
Mean Latency (ms)	128	87	−32%
MTTR (s)	18.6	6.2	−66%
Detection Rate (%)	71.3	93.5	+22.2%
Energy (J/task)	5.8	4.1	−29%

Energy savings are achieved through adaptive scheduling, task consolidation, and intelligent offloading decisions. By adjusting model complexity and sampling rates based on energy availability, RECF avoids unnecessary computation while maintaining service quality. The results show that resilience and security do not inherently conflict with sustainability when managed jointly.

4.6. Integrated Discussion and Practical Implications

The results clearly demonstrate that isolated optimization of latency, security, or energy is insufficient for real world edge deployments. The proposed framework succeeds because it treats these dimensions as interdependent control variables. Resilience mechanisms prevent cascading failures, security measures adapt to threat context, and energy awareness ensures long term operability. From a practical standpoint, these findings are highly relevant for autonomous transportation, smart infrastructure, industrial IoT, and remote monitoring systems, where service disruption or compromise can have severe consequences. The framework's autonomy reduces reliance on continuous cloud connectivity, making it suitable for bandwidth limited or intermittently connected environments.

5. Conclusion

This paper presented a resilient edge computing framework designed to support autonomous, secure, and energy aware system operation in dynamic and resource constrained environments. By integrating fault tolerance, adaptive security mechanisms, and energy-aware resource management within a unified architectural model, the proposed framework addresses key limitations of conventional edge computing solutions. The layered design enables local autonomy, rapid fault recovery, context aware security enforcement, and intelligent workload scheduling, ensuring continuous service availability under failures, cyber threats, and energy constraints. Experimental results demonstrate that the framework significantly improves system availability, reduces response latency, enhances security incident detection, and lowers energy consumption compared to traditional edge architectures. These outcomes confirm that resilience, security, and sustainability must be treated as interdependent design objectives rather than isolated optimizations in modern edge enabled intelligent systems.

Future work will focus on extending the framework through large scale real world deployments across diverse application domains such as smart grids, autonomous transportation, and industrial cyber physical systems. Advanced machine learning models will be explored to enable predictive resilience, allowing the system to anticipate failures, attacks, and energy shortages before they occur. Additional research will investigate cross-edge collaboration, federated learning for privacy-preserving intelligence, and formal verification of security and safety guarantees. These enhancements will further strengthen the framework's applicability, scalability, and robustness, supporting the long-term evolution of dependable and sustainable edge computing infrastructures.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be idcslosed.

References

[1] W. Shi et al., "Edge Computing: Vision and Challenges," IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016. doi: 10.1109/JIOT.2016.2579198

[2] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A Survey on Mobile Edge Computing: The Communication Perspective," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2322–2358, 2017. doi: 10.1109/COMST.2017.2745201

[3] T. Taleb et al., "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Architecture," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1657–1681, 2017. doi: 10.1109/COMST.2017.2705720

[4] S. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, 2018. doi: 10.1016/j.future.2016.11.009

[5] X. Wang et al., "Dynamic Service Migration in Mobile Edge Computing Based on Markov Decision Process," IEEE Access, vol. 7, pp. 17533–17545, 2019. doi: 10.1109/ACCESS.2019.2894694

[6] Rahman, M. A., Islam, M. I., Tabassum, M., & Bristy, I. J. (2025, September). Climate-aware decision intelligence: Integrating environmental risk into infrastructure and supply chain planning. Saudi Journal of Engineering and Technology (SJEAT), 10(9), 431–439. https://doi.org/10.36348/sjet.2025.v10i09.006

[7] Rahman, M. A., Bristy, I. J., Islam, M. I., & Tabassum, M. (2025, September). Federated learning for secure inter-agency data collaboration in critical infrastructure. Saudi Journal of Engineering and Technology (SJEAT), 10(9), 421–430. https://doi.org/10.36348/sjet.2025.v10i09.005

[8] Tabassum, M., Rokibuzzaman, M., Islam, M. I., & Bristy, I. J. (2025, September). Data-driven financial analytics through MIS platforms in emerging economies. Saudi Journal of Engineering and Technology (SJEAT), 10(9), 440–446. https://doi.org/10.36348/sjet.2025.v10i09.007

[9] Tabassum, M., Islam, M. I., Bristy, I. J., & Rokibuzzaman, M. (2025, September). Blockchain and ERP-integrated MIS for transparent apparel & textile supply chains. Saudi Journal of Engineering and Technology (SJEAT), 10(9), 447–456. https://doi.org/10.36348/sjet.2025.v10i09.008

[10] Bristy, I. J., Tabassum, M., Islam, M. I., & Hasan, M. N. (2025, September). IoT-driven predictive maintenance dashboards in industrial operations. Saudi Journal of Engineering and Technology (SJEAT), 10(9), 457–466. https://doi.org/10.36348/sjet.2025.v10i09.009

[11] Hasan, M. N., Karim, M. A., Joarder, M. M. I., & Zaman, M. T. (2025, September). IoT-integrated solar energy monitoring and bidirectional DC-DC converters for smart grids. Saudi Journal of Engineering and Technology (SJEAT), 10(9), 467–475. https://doi.org/10.36348/sjet.2025.v10i09.010

[12] Bormon, J. C., Saikat, M. H., Shohag, M., & Akter, E. (2025, September). Green and low-carbon construction materials for climate-adaptive civil structures. Saudi Journal of Civil Engineering (SJCE), 9(8), 219–226. https://doi.org/10.36348/sjce.2025.v09i08.002

[13] Razaq, A., Rahman, M., Karim, M. A., & Hossain, M. T. (2025, September 26). Smart charging infrastructure for EVs using IoT-based load balancing. Zenodo. https://doi.org/10.5281/zenodo.17210639

[14] Habiba, U., & Musarrat, R., (2025). Bridging IT and education: Developing smart platforms for student-centered English learning. Zenodo. https://doi.org/10.5281/zenodo.17193947

[15] Alimozzaman, D. M. (2025). Early prediction of Alzheimer's disease using explainable multi-modal AI. Zenodo. https://doi.org/10.5281/zenodo.17210997

[16] uz Zaman, M. T. Smart Energy Metering with IoT and GSM Integration for Power Loss Minimization. Preprints 2025, 2025091770. https://doi.org/10.20944/preprints202509.1770.v1

[17] Hossain, M. T. (2025, October). Sustainable garment production through Industry 4.0 automation. ResearchGate. https://doi.org/10.13140/RG.2.2.20161.83041

[18] Hasan, E. (2025). Secure and scalable data management for digital transformation in finance and IT systems. Zenodo. https://doi.org/10.5281/zenodo.17202282

[19] Saikat, M. H. (2025). Geo-Forensic Analysis of Levee and Slope Failures Using Machine Learning. Preprints. https://doi.org/10.20944/preprints202509.1905.v1

[20] Akter, E. (2025, October 13). Lean project management and multi-stakeholder optimization in civil engineering projects. ResearchGate. https://doi.org/10.13140/RG.2.2.15777.47206

[21] Musarrat, R. (2025). Curriculum adaptation for inclusive classrooms: A sociological and pedagogical approach. Zenodo. https://doi.org/10.5281/zenodo.17202455

[22] Bormon, J. C. (2025, October 13). Sustainable dredging and sediment management techniques for coastal and riverine infrastructure. ResearchGate. https://doi.org/10.13140/RG.2.2.28131.00803

[23] Bormon, J. C. (2025). AI-Assisted Structural Health Monitoring for Foundations and High-Rise Buildings. Preprints. https://doi.org/10.20944/preprints202509.1196.v1

[24] Haque, S. (2025). Effectiveness of managerial accounting in strategic decision making [Preprint]. Preprints. https://doi.org/10.20944/preprints202509.2466.v1

[25] Shoag, M. (2025). AI-Integrated Façade Inspection Systems for Urban Infrastructure Safety. Zenodo. https://doi.org/10.5281/zenodo.17101037

[26] Shoag, M. Automated Defect Detection in High-Rise Façades Using AI and Drone-Based Inspection. Preprints 2025, 2025091064. https://doi.org/10.20944/preprints202509.1064.v1

[27] Shoag, M. (2025). Sustainable construction materials and techniques for crack prevention in mass concrete structures. Available at SSRN: https://ssrn.com/abstract=5475306 or http://dx.doi.org/10.2139/ssrn.5475306

[28] Joarder, M. M. I. (2025). Disaster recovery and high-availability frameworks for hybrid cloud environments. Zenodo. https://doi.org/10.5281/zenodo.17100446

[29] 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

[30] 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

[31] Taimun, M. T. Y., Sharan, S. M. I., Azad, M. A., & Joarder, M. M. I. (2025). Smart maintenance and reliability engineering in manufacturing. Saudi Journal of Engineering and Technology, 10(4), 189–199.

[32] 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.

[33] Azad, M. A., Taimun, M. T. Y., Sharan, S. M. I., & Joarder, M. M. I. (2025). Advanced lean manufacturing and automation for reshoring American industries. Saudi Journal of Engineering and Technology, 10(4), 169–178.

[34] Sharan, S. M. I., Taimun, M. T. Y., Azad, M. A., & Joarder, M. M. I. (2025). Sustainable manufacturing and energy-efficient production systems. Saudi Journal of Engineering and Technology, 10(4), 179–188.

[35] Farabi, S. A. (2025). AI-augmented OTDR fault localization framework for resilient rural fiber networks in the United States. arXiv. https://arxiv.org/abs/2506.03041

[36] Farabi, S. A. (2025). AI-driven predictive maintenance model for DWDM systems to enhance fiber network uptime in underserved U.S. regions. Preprints. https://doi.org/10.20944/preprints202506.1152.v1

[37] Farabi, S. A. (2025). AI-powered design and resilience analysis of fiber optic networks in disaster-prone regions. ResearchGate. https://doi.org/10.13140/RG.2.2.12096.65287

[38] Sunny, S. R. (2025). Lifecycle analysis of rocket components using digital twins and multiphysics simulation. ResearchGate. https://doi.org/10.13140/RG.2.2.20134.23362

[39] Sunny, S. R. (2025). AI-driven defect prediction for aerospace composites using Industry 4.0 technologies. Zenodo. https://doi.org/10.5281/zenodo.16044460

[40] Sunny, S. R. (2025). Edge-based predictive maintenance for subsonic wind tunnel systems using sensor analytics and machine learning. TechRxiv. https://doi.org/10.36227/techrxiv.175624632.23702199/v1

[41] Sunny, S. R. (2025). Digital twin framework for wind tunnel-based aeroelastic structure evaluation. TechRxiv. https://doi.org/10.36227/techrxiv.175624632.23702199/v1

[42] Sunny, S. R. (2025). Real-time wind tunnel data reduction using machine learning and JR3 balance integration. Saudi Journal of Engineering and Technology, 10(9), 411–420. https://doi.org/10.36348/sjet.2025.v10i09.004

[43] Sunny, S. R. (2025). AI-augmented aerodynamic optimization in subsonic wind tunnel testing for UAV prototypes. Saudi Journal of Engineering and Technology, 10(9), 402–410. https://doi.org/10.36348/sjet.2025.v10i09.003

[44] Shaikat, M. F. B. (2025). Pilot deployment of an AI-driven production intelligence platform in a textile assembly line. TechRxiv. https://doi.org/10.36227/techrxiv.175203708.81014137/v1

[45] Rabbi, M. S. (2025). Extremum-seeking MPPT control for Z-source inverters in grid-connected solar PV systems. Preprints. https://doi.org/10.20944/preprints202507.2258.v1

[46] Rabbi, M. S. (2025). Design of fire-resilient solar inverter systems for wildfire-prone U.S. regions. Preprints. https://www.preprints.org/manuscript/202507.2505/v1

[47] Rabbi, M. S. (2025). Grid synchronization algorithms for intermittent renewable energy sources using AI control loops. Preprints. https://www.preprints.org/manuscript/202507.2353/v1

[48] 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

[49] Tonoy, A. A. R. (2025). Applications of semiconducting electrides in mechanical energy conversion and piezoelectric systems. Preprints. https://doi.org/10.20944/preprints202507.2421.v1

[50] Azad, M. A. (2025). Lean automation strategies for reshoring U.S. apparel manufacturing: A sustainable approach. Preprints. https://doi.org/10.20944/preprints202508.0024.v1

[51] Azad, M. A. (2025). Optimizing supply chain efficiency through lean Six Sigma: Case studies in textile and apparel manufacturing. Preprints. https://doi.org/10.20944/preprints202508.0013.v1

[52] Azad, M. A. (2025). Sustainable manufacturing practices in the apparel industry: Integrating eco-friendly materials and processes. TechRxiv. https://doi.org/10.36227/techrxiv.175459827.79551250/v1

[53] Azad, M. A. (2025). Leveraging supply chain analytics for real-time decision making in apparel manufacturing. TechRxiv. https://doi.org/10.36227/techrxiv.175459831.14441929/v1

[54] Azad, M. A. (2025). Evaluating the role of lean manufacturing in reducing production costs and enhancing efficiency in textile mills. TechRxiv. https://doi.org/10.36227/techrxiv.175459830.02641032/v1

[55] Azad, M. A. (2025). Impact of digital technologies on textile and apparel manufacturing: A case for U.S. reshoring. TechRxiv. https://doi.org/10.36227/techrxiv.175459829.93863272/v1

[56] 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

[57] Rayhan, F. (2025). AI-powered condition monitoring for solar inverters using embedded edge devices. Preprints. https://doi.org/10.20944/preprints202508.0474.v1

[58] 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

[59] Habiba, U., & Musarrat, R. (2025). Integrating digital tools into ESL pedagogy: A study on multimedia and student engagement. IJSRED – International Journal of Scientific Research and Engineering Development, 8(2), 799–811. https://doi.org/10.5281/zenodo.17245996

[60] 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

[61] 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

[62] Akter, E., Bormon, J. C., Saikat, M. H., & Shoag, M. (2025). Digital twin technology for smart civil infrastructure and emergency preparedness. IJSRED – International Journal of Scientific Research and Engineering Development, 8(2), 891–902. https://doi.org/10.5281/zenodo.17246150

[63] Rahmatullah, R. (2025). Smart agriculture and Industry 4.0: Applying industrial engineering tools to improve U.S. agricultural productivity. World Journal of Advanced Engineering Technology and Sciences, 17(1), 28–40. https://doi.org/10.30574/wjaets.2025.17.1.1377

[64] Islam, R. (2025). AI and big data for predictive analytics in pharmaceutical quality assurance.. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5564319

[65] Rahmatullah, R. (2025). Sustainable agriculture supply chains: Engineering management approaches for reducing post-harvest loss in the U.S. International Journal of Scientific Research and Engineering Development, 8(5), 1187–1216. https://doi.org/10.5281/zenodo.17275907

[66] Haque, S., Al Sany, S. M. A., & Rahman, M. (2025). Circular economy in fashion: MIS-driven digital product passports for apparel traceability. International Journal of Scientific Research and Engineering Development, 8(5), 1254–1262. https://doi.org/10.5281/zenodo.17276038

[67] Al Sany, S. M. A., Haque, S., & Rahman, M. (2025). Green apparel logistics: MIS-enabled carbon footprint reduction in fashion supply chains. International Journal of Scientific Research and Engineering Development, 8(5), 1263–1272. https://doi.org/10.5281/zenodo.17276049

[68] Bormon, J. C. (2025), Numerical Modeling of Foundation Settlement in High-Rise Structures Under Seismic Loading. Available at SSRN: https://ssrn.com/abstract=5472006 or http://dx.doi.org/10.2139/ssrn.5472006

[69] Hossain, M. T. (2025, October 7). Smart inventory and warehouse automation for fashion retail. TechRxiv. https://doi.org/10.36227/techrxiv.175987210.04689809.v1

[70] Karim, M. A. (2025, October 6). AI-driven predictive maintenance for solar inverter systems. TechRxiv. https://doi.org/10.36227/techrxiv.175977633.34528041.v1

[71] Habiba, U. (2025, October 7). Cross-cultural communication competence through technology-mediated TESOL. TechRxiv. https://doi.org/10.36227/techrxiv.175985896.67358551.v1

[72] Habiba, U. (2025, October 7). AI-driven assessment in TESOL: Adaptive feedback for personalized learning. TechRxiv. https://doi.org/10.36227/techrxiv.175987165.56867521.v1

[73] Akhter, T. (2025, October 6). Algorithmic internal controls for SMEs using MIS event logs. TechRxiv. https://doi.org/10.36227/techrxiv.175978941.15848264.v1

[74] Akhter, T. (2025, October 6). MIS-enabled workforce analytics for service quality & retention. TechRxiv. https://doi.org/10.36227/techrxiv.175978943.38544757.v1

[75] Hasan, E. (2025, October 7). Secure and scalable data management for digital transformation in finance and IT systems. Zenodo. https://doi.org/10.5281/zenodo.17202282

[76] Saikat, M. H., Shoag, M., Akter, E., Bormon, J. C. (October 06, 2025.) Seismic- and Climate-Resilient Infrastructure Design for Coastal and Urban Regions. TechRxiv. DOI: 10.36227/techrxiv.175979151.16743058/v1

[77] Saikat, M. H. (October 06, 2025). AI-Powered Flood Risk Prediction and Mapping for Urban Resilience. TechRxiv. DOI: 10.36227/techrxiv.175979253.37807272/v1

[78] Akter, E. (September 15, 2025). Sustainable Waste and Water Management Strategies for Urban Civil Infrastructure. Available at SSRN: https://ssrn.com/abstract=5490686 or http://dx.doi.org/10.2139/ssrn.5490686

[79] Karim, M. A., Zaman, M. T. U., Nabil, S. H., & Joarder, M. M. I. (2025, October 6). 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

[80] Al Sany, S. M. A., Rahman, M., & Haque, S. (2025). Sustainable garment production through Industry 4.0 automation. World Journal of Advanced Engineering Technology and Sciences, 17(1), 145–156. https://doi.org/10.30574/wjaets.2025.17.1.1387

[81] Rahman, M., Haque, S., & Al Sany, S. M. A. (2025). Federated learning for privacy-preserving apparel supply chain analytics. World Journal of Advanced Engineering Technology and Sciences, 17(1), 259–270. https://doi.org/10.30574/wjaets.2025.17.1.1386

[82] Rahman, M., Razaq, A., Hossain, M. T., & Zaman, M. T. U. (2025). Machine learning approaches for predictive maintenance in IoT devices. World Journal of Advanced Engineering Technology and Sciences, 17(1), 157–170. https://doi.org/10.30574/wjaets.2025.17.1.1388

[83] Akhter, T., Alimozzaman, D. M., Hasan, E., & Islam, R. (2025, October). Explainable predictive analytics for healthcare decision support. International Journal of Sciences and Innovation Engineering, 2(10), 921–938. https://doi.org/10.70849/IJSCI02102025105

[84] Rahman, M.. (October 15, 2025) Integrating IoT and MIS for Last-Mile Connectivity in Residential Broadband Services. TechRxiv. DOI: 10.36227/techrxiv.176054689.95468219/v1

[85] Islam, R. (2025, October 15). Integration of IIoT and MIS for smart pharmaceutical manufacturing . TechRxiv. https://doi.org/10.36227/techrxiv.176049811.10002169

[86] Hasan, E. (2025). Big Data-Driven Business Process Optimization: Enhancing Decision-Making Through Predictive Analytics. TechRxiv. October 07, 2025. 10.36227/techrxiv.175987736.61988942/v1

[87] Rahman, M. (2025, October 15). IoT-enabled smart charging systems for electric vehicles. TechRxiv. https://doi.org/10.36227/techrxiv.176049766.60280824/v1

[88] Alam, MS (2025, October 21). AI-driven sustainable manufacturing for resource optimization. TechRxiv. https://doi.org/10.36227/techrxiv.176107759.92503137/v1

[89] Alam, MS (2025, October 21). Data-driven production scheduling for high-mix manufacturing environments. TechRxiv. https://doi.org/10.36227/techrxiv.176107775.59550104/v1

[90] Ria, S. J. (2025, October 21). Environmental impact assessment of transportation infrastructure in rural Bangladesh. TechRxiv. https://doi.org/10.36227/techrxiv.176107782.23912238/v1

[91] R Musarrat and U Habiba, Immersive Technologies in ESL Classrooms: Virtual and Augmented Reality for Language Fluency (September 22, 2025). Available at SSRN: https://ssrn.com/abstract=5536098 or http://dx.doi.org/10.2139/ssrn.5536098

[92] Akter, E., Bormon, J. C., Saikat, M. H., & Shoag, M. (2025), "AI-Enabled Structural and Façade Health Monitoring for Resilient Cities", Int. J. Sci. Inno. Eng., vol. 2, no. 10, pp. 1035–1051, Oct. 2025, doi: 10.70849/IJSCI02102025116

[93] Haque, S., Al Sany (Oct. 2025), "Impact of Consumer Behavior Analytics on Telecom Sales Strategy", Int. J. Sci. Inno. Eng., vol. 2, no. 10, pp. 998–1018, doi: 10.70849/IJSCI02102025114.

[94] Sharan, S. M. I (Oct. 2025)., "Integrating Human-Centered Design with Agile Methodologies in Product Lifecycle Management", Int. J. Sci. Inno. Eng., vol. 2, no. 10, pp. 1019–1034, doi: 10.70849/IJSCI02102025115.

[95] Alimozzaman, D. M. (2025). Explainable AI for early detection and classification of childhood leukemia using multi-modal medical data. World Journal of Advanced Engineering Technology and Sciences, 17(2), 48–62. https://doi.org/10.30574/wjaets.2025.17.2.1442

[96] Alimozzaman, D. M., Akhter, T., Islam, R., & Hasan, E. (2025). Generative AI for synthetic medical imaging to address data scarcity. World Journal of Advanced Engineering Technology and Sciences, 17(1), 544–558. https://doi.org/10.30574/wjaets.2025.17.1.1415

[97] Zaidi, S. K. A. (2025). Intelligent automation and control systems for electric vertical take-off and landing (eVTOL) drones. World Journal of Advanced Engineering Technology and Sciences, 17(2), 63–75. https://doi.org/10.30574/wjaets.2025.17.2.1457

[98] 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. Zenodo. https://doi.org/10.5281/zenodo.17536369

[99] 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. Zenodo. https://doi.org/10.5281/zenodo.17536362

[100] Afrin, S. (2025). Cloud-integrated network monitoring dashboards using IoT and edge analytics. IJSRED – International Journal of Scientific Research and Engineering Development, 8(5), 2298–2307. Zenodo. https://doi.org/10.5281/zenodo.17536343

[101] Afrin, S. (2025). Cyber-resilient infrastructure for public internet service providers using automated threat detection. World Journal of Advanced Engineering Technology and Sciences, 17(02), 127-140. Article DOI: https://doi.org/10.30574/wjaets.2025.17.2.1475.

[102] Al Sany, S. M. A. (2025). The role of data analytics in optimizing budget allocation and financial efficiency in startups. IJSRED – International Journal of Scientific Research and Engineering Development, 8(5), 2287–2297. Zenodo. https://doi.org/10.5281/zenodo.17536325

[103] 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. Zenodo. https://doi.org/10.5281/zenodo.17536305

[104] Ria, S. J. (2025, October 7). Sustainable construction materials for rural development projects. SSRN. https://doi.org/10.2139/ssrn.5575390

[105] Razaq, A. (2025, October 15). Design and implementation of renewable energy integration into smart grids. TechRxiv. https://doi.org/10.36227/techrxiv.176049834.44797235/v1

[106] Musarrat R. (2025). AI-Driven Smart Housekeeping and Service Allocation Systems: Enhancing Hotel Operations Through MIS Integration. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 898–910). Zenodo. https://doi.org/10.5281/zenodo.17769627

[107] Hossain, M. T. (2025). AI-Augmented Sensor Trace Analysis for Defect Localization in Apparel Production Systems Using OTDR-Inspired Methodology. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 1029–1040). Zenodo. https://doi.org/10.5281/zenodo.17769857

[108] Rahman M. (2025). Design and Implementation of a Data-Driven Financial Risk Management System for U.S. SMEs Using Federated Learning and Privacy-Preserving AI Techniques. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 1041–1052). Zenodo. https://doi.org/10.5281/zenodo.17769869

[109] Alam, M. S. (2025). Real-Time Predictive Analytics for Factory Bottleneck Detection Using Edge-Based IIoT Sensors and Machine Learning. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 1053–1064). Zenodo. https://doi.org/10.5281/zenodo.17769890

[110] Habiba, U., & Musarrat, R. (2025). Student-centered pedagogy in ESL: Shifting from teacher-led to learner-led classrooms. International Journal of Science and Innovation Engineering, 2(11), 1018–1036. https://doi.org/10.70849/IJSCI02112025110

[111] Zaidi, S. K. A. (2025). Smart sensor integration for energy-efficient avionics maintenance operations. International Journal of Science and Innovation Engineering, 2(11), 243–261. https://doi.org/10.70849/IJSCI02112025026

[112] 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

[113] Farooq, H. (2025). Resource utilization analytics dashboard for cloud infrastructure management. World Journal of Advanced Engineering Technology and Sciences, 17(02), 141–154. https://doi.org/10.30574/wjaets.2025.17.2.1458

[114] Saeed, H. N. (2025). Hybrid perovskite–CIGS solar cells with machine learning-driven performance prediction. International Journal of Science and Innovation Engineering, 2(11), 262–280. https://doi.org/10.70849/IJSCI02112025027

[115] Akter, E. (2025). Community-based disaster risk reduction through infrastructure planning. International Journal of Science and Innovation Engineering, 2(11), 1104–1124. https://doi.org/10.70849/IJSCI02112025117

[116] Akter, E. (2025). Green project management framework for infrastructure development. International Journal of Science and Innovation Engineering, 2(11), 1125–1144. https://doi.org/10.70849/IJSCI02112025118

[117] Shoag, M. (2025). Integration of lean construction and digital tools for façade project efficiency. International Journal of Science and Innovation Engineering, 2(11), 1145–1164. https://doi.org/10.70849/IJSCI02112025119

[118] Akter, E. (2025). Structural Analysis of Low-Cost Bridges Using Sustainable Reinforcement Materials. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 911–921). Zenodo. https://doi.org/10.5281/zenodo.17769637

[119] Razaq, A. (2025). Optimization of power distribution networks using smart grid technology. World Journal of Advanced Engineering Technology and Sciences, 17(03), 129–146. https://doi.org/10.30574/wjaets.2025.17.3.1490

[120] Zaman, M. T. (2025). Enhancing grid resilience through DMR trunking communication systems. World Journal of Advanced Engineering Technology and Sciences, 17(03), 197–212. https://doi.org/10.30574/wjaets.2025.17.3.1551

[121] 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(03), 213–226. https://doi.org/10.30574/wjaets.2025.17.3.155

[122] Nahar, S. (2025). Optimizing HR management in smart pharmaceutical manufacturing through IIoT and MIS integration. World Journal of Advanced Engineering Technology and Sciences, 17(03), 240–252. https://doi.org/10.30574/wjaets.2025.17.3.1554

[123] Islam, S. (2025). IPSC-derived cardiac organoids: Modeling heart disease mechanism and advancing regenerative therapies. World Journal of Advanced Engineering Technology and Sciences, 17(03), 227–239. https://doi.org/10.30574/wjaets.2025.17.3.1553

[124] Shoag, M. (2025). Structural load distribution and failure analysis in curtain wall systems. IJSRED - International Journal of Scientific Research and Engineering Development, 8(6), 2117–2128. Zenodo. https://doi.org/10.5281/zenodo.17926722

[125] Hasan, E. (2025). Machine learning-based KPI forecasting for finance and operations teams. IJSRED - International Journal of Scientific Research and Engineering Development, 8(6), 2139–2149. Zenodo. https://doi.org/10.5281/zenodo.17926746

[126] Hasan, E. (2025). SQL-driven data quality optimization in multi-source enterprise dashboards. IJSRED - International Journal of Scientific Research and Engineering Development, 8(6), 2150–2160. Zenodo. https://doi.org/10.5281/zenodo.17926758

[127] Hasan, E. (2025). Optimizing SAP-centric financial workloads with AI-enhanced CloudOps in virtualized data centers. IJSRED - International Journal of Scientific Research and Engineering Development, 8(6), 2252–2264. Zenodo. https://doi.org/10.5281/zenodo.17926855

[128] Karim, M. A. (2025). An IoT-enabled exoskeleton architecture for mobility rehabilitation derived from the ExoLimb methodological framework. IJSRED - International Journal of Scientific Research and Engineering Development, 8(6), 2265–2277. Zenodo. https://doi.org/10.5281/zenodo.17926861

[129] Akter, E., Ria, S. J., Khan, M. I., & Shoag, M. D. (2025). Smart & sustainable construction governance for climate-resilient cities. IJSRED - International Journal of Scientific Research and Engineering Development, 8(6), 2278–2291. Zenodo. https://doi.org/10.5281/zenodo.17926875

[130] 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. Zenodo. https://doi.org/10.5281/zenodo.17926883

[131] Hossain, M. T. (2025). Data-driven optimization of apparel supply chain to reduce lead time and improve on-time delivery. World Journal of Advanced Engineering Technology and Sciences, 17(03), 263–277.https://doi.org/10.30574/wjaets.2025.17.3.1556

[132] Rahman, F. (2025). Advanced statistical models for forecasting energy prices. Global Journal of Engineering and Technology Advances, 25(03), 168–182. https://doi.org/10.30574/gjeta.2025.25.3.0350

[133] Karim, F. M. Z. (2025). Integrating quality management systems to strengthen U.S. export-oriented production. Global Journal of Engineering and Technology Advances, 25(03), 183–198. https://doi.org/10.30574/gjeta.2025.25.3.0351

[134] Fazle, A. B. (2025). AI-driven predictive maintenance and process optimization in manufacturing systems using machine learning and sensor analytics. Global Journal of Engineering and Technology Advances, 25(03), 153–167. https://doi.org/10.30574/gjeta.2025.25.3.0349

[135] Rahman, F. (2025). Data science in power system risk assessment and management. World Journal of Advanced Engineering Technology and Sciences, 17(03), 295–311. https://doi.org/10.30574/wjaets.2025.17.3.1560

[136] Rahman, M. (2025). Predictive maintenance of electric vehicle components using IoT sensors. World Journal of Advanced Engineering Technology and Sciences, 17(03), 312–327. https://doi.org/10.30574/wjaets.2025.17.3.1557

[137] Hossain, M. T. (2025). Cost negotiation strategies and their impact on profitability in fashion sourcing: A quantitative analysis. Global Journal of Engineering and Technology Advances, 25(03), 136–152. https://doi.org/10.30574/gjeta.2025.25.3.0348

[138] Jasem, M. M. H. (2025, December 19). An AI-driven system health dashboard prototype for predictive maintenance and infrastructure resilience. Authorea. https://doi.org/10.22541/au.176617579.97570024/v1

[139] 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. Zenodo. https://doi.org/10.5281/zenodo.18074355

[140] Shoag, M. D., Khan, M. I., Ria, S. J., & Akter, E. (2025). AI-based risk prediction and quality assurance in mega-infrastructure projects. IJSRED – International Journal of Scientific Research and Engineering Development, 8(6), 2324–2336. Zenodo. https://doi.org/10.5281/zenodo.18074336

[141] Haque, S. (2025). The impact of automation on accounting practices. IJSRED – International Journal of Scientific Research and Engineering Development, 8(6), 2312–2323. Zenodo. https://doi.org/10.5281/zenodo.18074324

[142] Fontenot, D., Ahmed, F., & Chy, K. S. (2024). ChatGPT: What is it? How does it work? Can it be a teaching tool for an introductory programming course in higher education? Southwestern Business Administration Journal, 21(1), Article 2. https://digitalscholarship.tsu.edu/sbaj/vol21/iss1/2

[143] Ahmed, F., & Rahaman, A. (2025). AI-driven predictive modeling of Bangladesh economic trends: Highlighting financial crime & fraud (pp. 533–542). IKSAD Congress. https://www.iksadkongre.com/_files/ugd/614b1f_4195d955f81e401a9bdbf7565b2f9948.pdf

[144] Rahaman, A., Siddiquee, S. F., Chowdhury, J., Ahmed, R., Abrar, S., Bhuiyan, T., & Ahmed, F. (2025). Enhancing climate resilience in Rohingya refugee camps: A comprehensive strategy for sustainable disaster preparedness. Environment and Ecology Research, 13(6), 755–767. https://doi.org/10.13189/eer.2025.130601

[145] Chowdhury, S., et al. (2024). Students' perception of using AI tools as a research work or coursework assistant. Middle East Research Journal of Economics and Management, 4(6), X. https://doi.org/10.36348/merjem.2024.v04i06.00X

[146] Rahaman, A., Zaman, T. S., & Ahmed, F. (2025). Digital pathways to women's empowerment: Use of Facebook, Instagram, WhatsApp, and e-commerce by women entrepreneurs in Bangladesh. In Proceedings of the 15th International "Communication in New World" Congress (pp. 700–709).

[147] Ria, S. J., Shoag, M. D., Akter, E., & Khan, M. I. (2025). Integration of recycled and local materials in low-carbon urban structures. World Journal of Advanced Engineering Technology and Sciences, 17(03), 447–463. https://doi.org/10.30574/wjaets.2025.17.3.1555

[148] 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(03), 431–446. https://doi.org/10.30574/wjaets.2025.17.3.1574

[149] Karim, F. M. Z. (2025). Strategic Human Resource Systems for Retention and Growth in Manufacturing Enterprises. In IJSRED - International Journal of Scientific Research and Engineering Development (Vol. 8, Number 6, pp. 2547–2559). Zenodo. https://doi.org/10.5281/zenodo.18074545

[150] Rahman, T. (2026). Financial Risk Intelligence: Real-Time Fraud Detection and Threat Monitoring. Zenodo. https://doi.org/10.5281/zenodo.18176490

[151] 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