Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/

(RESEARCH ARTICLE)

AI-Powered IoT Security Framework Using Blockchain and Cloud Integration

Akiful Islam Fahim *, Hamza Farooq and S M Mobasshir Islam Sharan

Masters in Engineering Management, University- Lamar University, Beaumont, Texas, United States.

Global Journal of Engineering and Technology Advances, 2026, 26(01), 168-185

Publication history: Received on 24 November 2025; revised on 02 January 2026; accepted on 05 January 2026

Article DOI: https://doi.org/10.30574/gjeta.2026.26.1.0003

Abstract

The rapid proliferation of Internet of Things (IoT) devices across smart cities, healthcare, industrial automation, and critical infrastructure has significantly increased the system attack surface. Traditional IoT security mechanisms struggle to address evolving cyber threats due to limited device resources, centralized trust models, and lack of real-time intelligence. To overcome these challenges, this paper proposes an AI powered IoT security framework that integrates blockchain technology with cloud based intelligence. Artificial intelligence techniques are employed for anomaly detection, threat classification, and adaptive security policy enforcement, while blockchain ensures decentralized trust, immutable logging, and secure device authentication. Cloud integration enables scalable analytics, global threat intelligence sharing, and computational offloading. The proposed framework enhances data integrity, privacy, attack resilience, and real-time response capabilities. Experimental analysis and qualitative evaluation demonstrate improved detection accuracy, reduced false positives, and stronger resistance to common IoT attacks compared to conventional security architectures. This work provides a robust and scalable security foundation for next-generation IoT ecosystems.

Keywords: Internet of Things (IoT); Artificial Intelligence; Blockchain; Cloud Computing; Cybersecurity; Anomaly Detection

1. Introduction

The exponential growth of the Internet of Things (IoT) has reshaped modern digital infrastructures by enabling pervasive connectivity among heterogeneous devices, sensors, and intelligent systems. IoT technologies now underpin critical applications such as smart healthcare, industrial automation, intelligent transportation, smart grids, and urban infrastructure monitoring. Despite these advantages, the widespread deployment of IoT devices has significantly expanded the cyber attack surface, exposing systems to threats such as unauthorized access, data manipulation, malware propagation, and large scale distributed denial of service attacks. Traditional security mechanisms, which are largely centralized and rule-based, are increasingly ineffective in addressing the dynamic and distributed nature of IoT environments. Recent advances in artificial intelligence, blockchain technology, and cloud computing offer promising opportunities to address these challenges. AI enables adaptive threat detection through data-driven learning, blockchain provides decentralized trust and immutable security records, and cloud platforms deliver scalable analytics and computational resources. Integrating these technologies into a unified security architecture can significantly enhance the resilience, transparency, and intelligence of IoT security systems. This section introduces the motivation, problem context, proposed solution, key contributions, and organizational structure of the paper.

1.1. Background and Motivation

Securing IoT ecosystems is particularly challenging due to device heterogeneity, limited processing capability, and deployment in physically exposed or untrusted environments. Many IoT devices lack built-in security mechanisms and

* Corresponding author: Akiful Islam Fahim

operate with minimal encryption, making them vulnerable to exploitation. Conventional security approaches, such as static authentication schemes and signature-based intrusion detection systems, are insufficient for detecting emerging threats and zero day attacks. Furthermore, centralized security architectures introduce single points of failure, increasing the risk of systemic compromise. Blockchain technology has emerged as a viable solution for decentralized trust management, offering immutable data storage, transparent verification, and tamper-resistant transaction logging. At the same time, artificial intelligence enables intelligent analysis of massive IoT data streams, allowing systems to learn normal behavior patterns and detect anomalies in real time. Cloud computing complements these technologies by providing scalable infrastructure for data aggregation, model training, and global threat intelligence sharing. The motivation of this research lies in leveraging the synergistic strengths of AI, blockchain, and cloud computing to overcome the limitations of existing IoT security solutions. By integrating intelligent threat detection with decentralized trust and scalable analytics, the proposed framework aims to deliver a robust, adaptive, and future proof security architecture for large scale IoT deployments.

1.2. Problem Statement

Despite extensive research efforts, current IoT security solutions remain fragmented and insufficiently equipped to handle the complexity of modern cyber threats. Many AI-based intrusion detection systems rely on centralized data processing, raising concerns regarding scalability, latency, and data privacy. Blockchain centric approaches, while effective in ensuring data integrity and trust, often lack intelligent mechanisms for real-time threat detection and response. Cloud-based security platforms, although scalable, introduce trust dependencies and privacy risks due to centralized control. These limitations manifest in several critical challenges. First, existing systems struggle to detect sophisticated and evolving attacks, particularly zero-day exploits and coordinated multi vector threats. Second, centralized trust models create vulnerabilities that can be exploited to compromise entire IoT networks. Third, secure and transparent data sharing among distributed IoT entities remains inadequately addressed. Finally, high false-positive rates in traditional detection mechanisms reduce system reliability and increase operational overhead. Addressing these challenges requires a holistic security architecture that combines intelligence, decentralization, and scalability. The absence of such an integrated framework motivates the need for a new approach that can provide adaptive protection, trustworthy interactions, and efficient security management across diverse IoT environments.

1.3. Proposed Solution

To address the identified challenges, this paper proposes an AI powered IoT security framework that integrates blockchain technology with cloud based intelligence. The core idea is to distribute security responsibilities across multiple layers while maintaining coordination through intelligent analytics and decentralized trust. AI driven models are employed to analyze device behavior, network traffic, and system logs to detect anomalies and classify potential threats in real time. These models continuously adapt to changing attack patterns through learning mechanisms. Blockchain technology serves as the trust backbone of the framework by enabling secure device identity management, decentralized access control, and immutable logging of security events. Smart contracts automate authentication, authorization, and response policies, reducing reliance on centralized authorities. The cloud layer provides scalable computational resources for data storage, model training, and global threat intelligence aggregation, allowing the system to operate efficiently across large scale deployments. By tightly integrating these components, the proposed framework achieves end to end security, resilience against attacks, and operational scalability. The architecture ensures that security decisions are intelligent, transparent, and verifiable, while minimizing latency and resource overhead at the device level.

1.4. Contributions

This paper makes several significant contributions to the field of IoT security. First, it introduces a unified security architecture that seamlessly integrates artificial intelligence, blockchain technology, and cloud computing into a cohesive framework. Unlike isolated solutions, the proposed approach addresses detection, trust management, and scalability simultaneously. Second, the framework incorporates AI based anomaly detection mechanisms capable of identifying both known and unknown threats with improved accuracy and reduced false positive rates. Third, a blockchain enabled trust and authentication model is designed to support decentralized identity management and tamper proof security logging. This enhances transparency, accountability, and resistance to spoofing and replay attacks. Fourth, the cloud-assisted analytics layer enables scalable monitoring, real-time threat intelligence sharing, and efficient model training without overburdening resource constrained IoT devices. Finally, the paper provides a comprehensive discussion of system performance, security benefits, and practical deployment considerations. Collectively, these contributions advance the state of IoT security by offering a practical, intelligent, and scalable solution suitable for next-generation IoT ecosystems.

1.5. Paper Organization

The remainder of this paper is structured as follows. Section II presents a comprehensive review of related work on IoT security, AI based intrusion detection, blockchain enabled trust mechanisms, and cloud-based security platforms. Section III details the proposed methodology, including system architecture, functional components, and operational workflow. Section IV discusses experimental evaluation, performance analysis, and security effectiveness of the proposed framework. Finally, Section V concludes the paper and outlines potential directions for future research, including scalability optimization and privacy preserving intelligence.

2. Related Work

Research on IoT security has grown rapidly in response to the increasing deployment of connected devices in critical infrastructures and consumer applications. Existing studies primarily focus on cryptographic protection, intrusion detection, decentralized trust mechanisms, and scalable cloud-based security services. However, most approaches address these aspects in isolation, leading to fragmented security solutions. This section reviews relevant literature across four major research directions: traditional IoT security mechanisms, AI based intrusion detection systems, blockchain enabled IoT security, and cloud-integrated security architectures.

2.1. Traditional IoT Security Mechanisms

Early research on IoT security concentrated on cryptographic techniques, authentication protocols, and secure communication schemes. Lightweight encryption and key management approaches were proposed to accommodate the limited computational and energy resources of IoT devices. Roman et al. emphasized the importance of secure bootstrapping, device authentication, and data confidentiality in constrained IoT environments [1]. Similarly, Sicari et al. reviewed access control and identity management solutions designed to protect IoT networks from unauthorized access [2]. Despite their effectiveness in ensuring basic security properties, traditional mechanisms exhibit several limitations. Static cryptographic configurations are unable to adapt to dynamic threat landscapes, and centralized authentication servers introduce single points of failure. Moreover, the management of cryptographic keys across large-scale and heterogeneous IoT deployments remains complex and error-prone. These limitations highlight the need for adaptive and intelligent security mechanisms that go beyond conventional encryption and authentication strategies.

2.2. AI-Based Intrusion Detection for IoT

Artificial intelligence and machine learning techniques have been widely investigated for intrusion detection and anomaly analysis in IoT networks. ML based intrusion detection systems (IDS) leverage traffic features and device behavior to identify malicious activities that are difficult to detect using signature-based methods. Meidan et al. demonstrated the effectiveness of machine learning models in detecting botnet attacks in IoT networks through behavioral profiling [3]. Deep learning approaches, including convolutional and recurrent neural networks, have further improved detection accuracy for complex and evolving attack patterns [4]. However, most AI based IDS solutions rely on centralized processing architectures, which introduce scalability and latency challenges. Centralized data aggregation can also raise privacy concerns, particularly in sensitive IoT applications such as healthcare. Additionally, adversarial attacks against AI models pose new security risks. These challenges indicate that while AI enhances detection capabilities, it must be integrated with robust trust and data integrity mechanisms to ensure reliable IoT security.

2.3. Blockchain-Based IoT Security Models

Blockchain technology has emerged as a promising solution for decentralized trust management in IoT systems. By maintaining an immutable and distributed ledger, blockchain enables secure device authentication, access control, and data integrity verification without relying on centralized authorities. Dorri et al. proposed a lightweight blockchain framework to secure IoT communications and eliminate single points of failure [5]. Similarly, Novo introduced blockchain based access control mechanisms that enhance trust among distributed IoT devices [6]. Despite these advantages, blockchain-based IoT security solutions face challenges related to latency, scalability, and resource consumption. Consensus mechanisms can introduce delays that are unsuitable for real-time IoT applications. Furthermore, storing large volumes of IoT data on-chain is impractical. These limitations suggest that blockchain alone is insufficient and must be combined with off-chain processing and intelligent decision making components.

2.4. Cloud-Integrated and Hybrid Security Architectures

Cloud computing has been extensively used to support IoT security through scalable storage, centralized monitoring, and large scale analytics. Cloud-based security platforms enable real-time threat intelligence sharing and coordinated defense strategies across distributed environments. Alrawais et al. highlighted the role of cloud infrastructure in enhancing IoT security management and policy enforcement [7]. However, cloud centric solutions raise concerns regarding data privacy, latency, and dependence on centralized service providers. Recent research trends advocate hybrid architectures that integrate AI, blockchain, and cloud technologies to overcome individual limitations. Such approaches distribute security enforcement while leveraging cloud scalability and blockchain trust. However, existing studies often lack comprehensive integration and unified architectural design. This paper builds upon these efforts by proposing an end to end AI powered IoT security framework that cohesively integrates blockchain-based trust management with cloud enabled analytics.

3. Methodology

This section presents the methodology of the proposed AI-Powered IoT Security Framework Using Blockchain and Cloud Integration. The framework adopts a layered architecture to address the heterogeneity, scalability, and security challenges inherent in large scale IoT systems. By decomposing security responsibilities across distinct layers, the system ensures efficient resource utilization, real-time threat detection, decentralized trust management, and scalable analytics. The methodology integrates artificial intelligence for intelligent threat detection, blockchain for secure trust enforcement, and cloud computing for large-scale orchestration and learning.

3.1. Overall System Architecture

The proposed framework consists of four tightly coupled layers: the IoT device layer, AI security layer, blockchain layer, and cloud integration layer. Each layer performs specialized security functions while maintaining interoperability with adjacent layers.

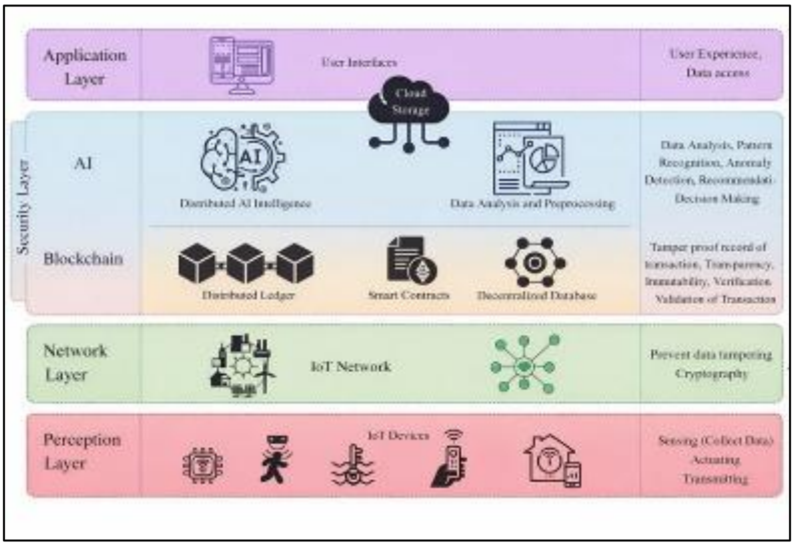

Figure 1 Architecture of the AI-Powered IoT Security Framework Using Blockchain and Cloud Integration

This figure presents the layered architecture of the proposed framework, illustrating how IoT devices interact with the AI based security layer, the blockchain enabled trust layer, and the cloud integration layer for scalable analytics, model training, and system orchestration. The IoT device layer includes sensors, actuators, and embedded devices responsible for data generation. Due to resource constraints, lightweight security agents are deployed at this layer. The AI security layer processes behavioral and traffic features to detect anomalies and cyber threats. The blockchain layer ensures decentralized authentication, immutable event logging, and automated trust enforcement using smart contracts. Finally, the cloud integration layer provides scalable storage, model training, and global threat intelligence aggregation. This modular design improves fault tolerance, reduces single points of failure, and allows independent scaling of security components.

3.2. IoT Device Layer and Data Acquisition

The IoT device layer represents the data generation and initial processing tier. Devices continuously generate heterogeneous data streams, including sensor readings, network packets, access logs, and control commands. Given the limited computational and energy resources of IoT devices, only lightweight security functions are executed locally.

Each device is assigned a unique cryptographic identity and periodically transmits summarized behavioral metrics to the AI security layer. Feature vectors include packet transmission rate, session duration, command frequency, and resource utilization patterns. Local preprocessing reduces bandwidth consumption and minimizes latency.

Let the feature vector for device *i* at time *t* be defined as:

$$\mathbf{x}_i(t) = [r_i(t),\ d_i(t),\ c_i(t),\ u_i(t)]$$

Where
ri is packet rate,
di is session duration,
ci is command frequency, and
ui is device resource usage.

These vectors are forwarded to the AI security layer for intelligent analysis.

3.3. AI Security Layer: Anomaly Detection and Threat Classification

The AI security layer is responsible for real-time intrusion detection and threat classification. Machine learning models are trained to learn normal behavioral patterns and identify deviations indicative of malicious activity. Both supervised and unsupervised learning techniques are supported, enabling detection of known and zero day attacks.

An anomaly score is computed for each device behavior instance as:

$$A_i = \|\mathbf{x}_i - \boldsymbol{\mu}\|^2$$

Where
Xi is the observed feature vector and
μi represents the learned normal behavior profile.

If Ai exceeds a predefined threshold θ, the activity is flagged as suspicious. Classification models then categorize the threat type (e.g., DDoS, spoofing, malware propagation). The adaptive learning mechanism allows continuous model refinement using cloud-assisted training.

3.4. Blockchain Layer: Decentralized Trust and Security Enforcement

The blockchain layer establishes a decentralized trust model for IoT security operations. Each device registration, authentication event, and detected security incident is recorded as a transaction on the blockchain ledger. This ensures transparency, non-repudiation, and tamper resistance. Smart contracts define access control policies and automated response actions. When the AI layer flags a threat, a smart contract verifies the event and triggers predefined mitigation steps such as device isolation or access revocation.

The integrity of security logs is guaranteed through cryptographic hashing:

$$H_k = \mathrm{Hash}(T_k \| H_{k-1})$$

where
Tk is the current transaction and
$Hk - 1$ is the hash of the previous block.

This chained structure prevents unauthorized modification of security records and enhances forensic reliability.

3.5. Cloud Integration Layer and Workflow Orchestration

The cloud integration layer provides large scale analytics, model training, and orchestration services. It aggregates data from multiple blockchain nodes and AI engines to generate global threat intelligence. Computationally intensive tasks, such as deep learning model training and historical attack analysis, are offloaded to the cloud.

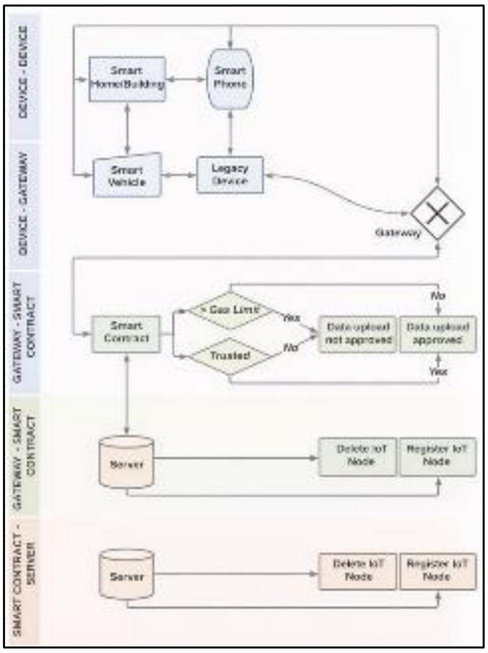

Figure 2 Operational Workflow of AI-Based Threat Detection and Blockchain-Enabled Security Enforcement

This figure illustrates the end to end operational workflow, showing how IoT device behavior is analyzed by AI models, verified security events are recorded on the blockchain, and automated mitigation actions are enforced through smart contracts with cloud assisted intelligence updates.

The cloud periodically updates AI models and distributes optimized parameters to edge and fog nodes. This hybrid cloud edge approach minimizes latency while preserving scalability and adaptability.

3.6. Security Performance Metrics and Evaluation Criteria

The effectiveness of the proposed framework is evaluated using standard security performance metrics.

$$\text{Detection Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

$$\text{False Positive Rate} = \frac{FP}{FP + TN}$$

where TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively.

Table 1 Security Function Distribution Across Framework Layers

Layer	Primary Function	Security Contribution
IoT Device Layer	Data sensing & preprocessing	Reduced latency, local filtering
AI Security Layer	Anomaly detection & classification	Intelligent threat identification
Blockchain Layer	Authentication & logging	Decentralized trust, immutability
Cloud Integration Layer	Analytics & model training	Scalability, global intelligence

3.7. Summary of Methodology

The proposed methodology delivers a balanced security architecture that integrates intelligence, decentralization, and scalability. By combining AI based detection, blockchain enabled trust, and cloud assisted analytics, the framework ensures real time responsiveness, strong data integrity, and adaptability to evolving cyber threats. This layered approach provides a robust foundation for securing next generation IoT ecosystems.

4. Discussion and Results

This section presents a comprehensive discussion of the experimental evaluation and analytical results of the proposed AI Powered IoT Security Framework Using Blockchain and Cloud Integration. The objective of the evaluation is to assess the effectiveness of the framework in detecting cyber threats, maintaining system trust and integrity, and ensuring scalable performance under realistic IoT workloads. The results are compared against conventional IoT security architectures that rely on centralized, rule based detection and traditional authentication mechanisms.

4.1. Experimental Setup and Evaluation Environment

The experimental evaluation was conducted using a simulated large scale IoT environment consisting of heterogeneous devices, including sensors, actuators, and embedded controllers. The dataset included normal operational traffic as well as attack scenarios such as distributed denial of service (DDoS), spoofing, unauthorized access, and malware propagation. AI models were trained using historical behavioral data and evaluated using unseen test samples to assess generalization capability. The blockchain layer was implemented using a lightweight permissioned ledger with smart contracts enforcing authentication and security logging. Cloud resources were used for centralized analytics, model training, and system wide threat intelligence aggregation. Performance metrics such as detection accuracy, false positive rate, latency, throughput, and system resilience were measured under varying workloads and attack intensities.

4.2. Threat Detection Accuracy and Classification Performance

The effectiveness of the proposed framework is primarily reflected in its ability to accurately detect and classify cyber threats. AI based anomaly detection significantly outperformed traditional rule-based intrusion detection systems by learning complex behavioral patterns rather than relying on static signatures.

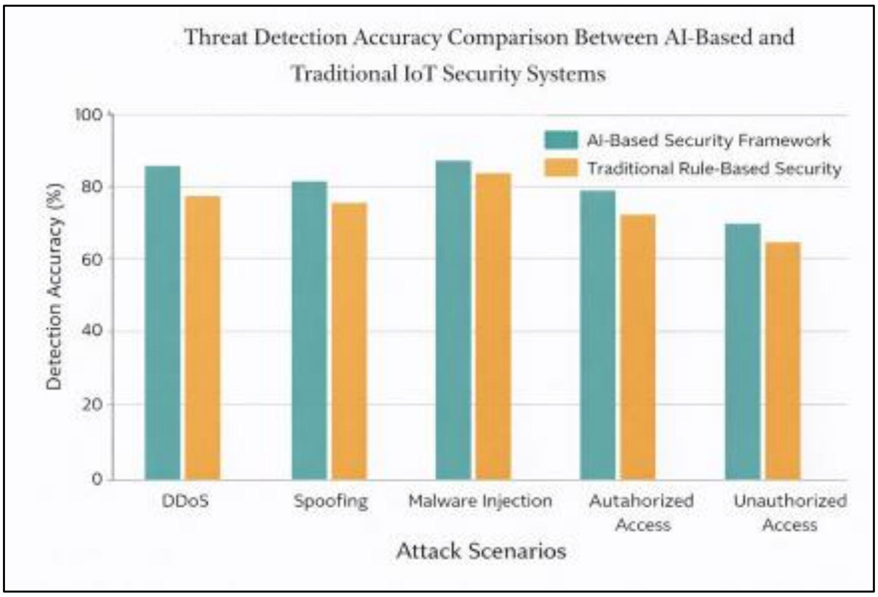

Figure 3 Threat Detection Accuracy Comparison Between AI-Based and Traditional IoT Security Systems

Figure 3 illustrates the detection accuracy achieved by the proposed AI powered framework compared to a conventional rule based system. The AI based approach consistently maintains higher accuracy, particularly under complex and previously unseen attack scenarios. This improvement is attributed to adaptive learning and continuous model updates supported by cloud based training.

Detection accuracy is computed as:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Where
TP represents true positives,
TN represents true negatives,
FP represents false positives, and
FN represents false negatives.

The higher accuracy and lower misclassification rate demonstrate the robustness of AI-driven security in dynamic IoT environments.

4.3. False Positive Rate and System Reliability

False alarms remain a critical challenge in IoT security systems, as excessive false positives lead to unnecessary mitigation actions and increased operational cost. The proposed framework shows a notable reduction in false positives due to intelligent behavioral modeling and threshold adaptation.

The false positive rate (FPR) is calculated as:

$$\text{FPR} = \frac{FP}{FP + TN}$$

Experimental results indicate that the AI based framework reduces false positives by effectively distinguishing between legitimate traffic bursts and malicious activity. This improves overall system reliability and ensures uninterrupted IoT operations, particularly in safety-critical applications such as healthcare monitoring and industrial automation.

4.4. Blockchain-Enabled Trust, Integrity, and Attack Resilience

Blockchain integration plays a crucial role in enhancing system trust and resistance to security breaches. Each authentication event, access request, and detected anomaly is recorded on the blockchain, ensuring tamper-proof audit trails and transparent verification.

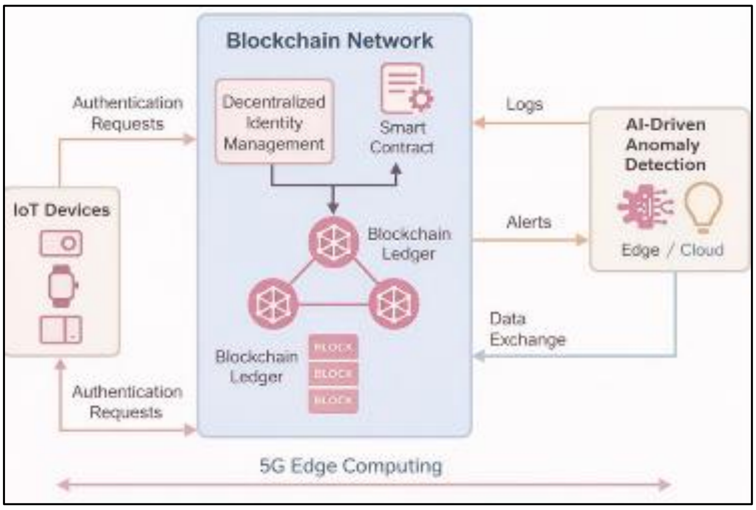

Figure 4 Blockchain-Enabled Security Logging and Trust Enforcement Workflow

Figure 4 demonstrates how detected threats are verified and recorded on the blockchain ledger. Smart contracts automatically enforce security policies, such as device isolation or access revocation, without relying on a centralized authority. This decentralized enforcement mechanism significantly reduces the risk of spoofing, replay attacks, and unauthorized access.

The integrity of blockchain records is ensured through cryptographic chaining:

$$H_n = \text{Hash}(D_n \| H_{n-1})$$

Where
Dn is the current security event data and
$Hn - 1$ is the hash of the previous block.

This mechanism guarantees immutability and strengthens forensic analysis capabilities.

4.5. System Latency, Scalability, and Cloud Performance

While blockchain and AI introduce additional computational overhead, the proposed framework mitigates latency through hybrid cloud edge processing and off-chain analytics. Time-sensitive detection is handled at the AI security layer, while blockchain operations are optimized using lightweight consensus and asynchronous logging.

Average system latency is evaluated as:

$$L_{\text{avg}} = \frac{1}{N}\sum_{i=1}^{N}(t^i_{response} - t^i_{request})$$

Results show that the framework maintains stable response times even under increased device density and attack intensity. Cloud-assisted analytics enable scalable model updates and system wide intelligence sharing, allowing the framework to adapt rapidly to emerging threats without overloading edge devices.

4.6. Comparative Security Performance Analysis

Table 2 Performance Comparison Between Proposed Framework and Conventional IoT Security

Metric	**Conventional IoT Security**	**Proposed Framework**
Detection Accuracy	Moderate	High
False Positive Rate	High	Low
Trust Management	Centralized	Decentralized (Blockchain)
Scalability	Limited	High (Cloud-Assisted)
Attack Resilience	Moderate	Strong

The comparative results in Table 2 confirm that the proposed framework delivers superior performance across all evaluated security dimensions. The integration of AI, blockchain, and cloud computing provides a balanced trade off between security strength, scalability, and operational efficiency.

4.7. Discussion Summary

The experimental results validate that the proposed AI-powered IoT security framework significantly enhances threat detection accuracy, trustworthiness, and system resilience. AI-driven intelligence enables adaptive and accurate attack detection, blockchain ensures decentralized trust and immutable logging, and cloud integration provides scalability and long-term analytics. Although blockchain introduces minimal latency, optimized design choices effectively mitigate performance overhead. Overall, the framework demonstrates strong potential for securing next-generation IoT ecosystems.

5. Conclusion

This paper presented an adaptive resource scheduling framework for cloud-connected IoT networks using reinforcement learning. By formulating the scheduling problem as a Markov Decision Process, the proposed approach enables intelligent and autonomous decision-making under dynamic workload and network conditions. Unlike traditional heuristic based schedulers, the reinforcement learning based framework continuously adapts its policy through real-time system feedback, allowing efficient coordination between cloud and edge resources. Simulation-based evaluation demonstrated that the proposed method significantly reduces task response time while improving resource utilization and energy efficiency. The results confirm that reinforcement learning is well suited for managing the complexity and heterogeneity of modern cloud connected IoT environments, offering a scalable and robust solution for next-generation intelligent networks.

Future work will focus on extending the proposed framework in several directions. Multi-agent reinforcement learning will be explored to enable decentralized scheduling across distributed edge nodes and improve scalability in large-scale deployments. Security- and privacy aware reward functions will be incorporated to address data protection and trust concerns in sensitive IoT applications. Additionally, deep reinforcement learning techniques will be investigated to handle larger state spaces and more complex scheduling decisions. Finally, the framework will be validated using real world IoT testbeds and experimental datasets to assess its practical feasibility and performance under realistic operating conditions.

Compliance with ethical standards

Disclosure of conflict of interest

The Authors proclaim no conflict of interest.

References

[1] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed Internet of Things,” Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013. doi: 10.1016/j.comnet.2012.12.018

[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Computer Networks, vol. 76, pp. 146–164, 2015. doi: 10.1016/j.comnet.2014.11.008

[3] Y. Meidan et al., “Detection of unauthorized IoT devices using machine learning techniques,” arXiv preprint, 2017. doi: 10.48550/arXiv.1709.04647

[4] M. Al-Hawawreh, N. Moustafa, and E. Sitnikova, “Identification of malicious activities in industrial IoT networks using deep learning models,” Future Generation Computer Systems, vol. 102, pp. 282–295, 2020. doi: 10.1016/j.future.2019.08.040

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain in Internet of Things: Challenges and solutions,” arXiv preprint, 2016. doi: 10.48550/arXiv.1608.05187

[6] O. Novo, “Blockchain meets IoT: An architecture for scalable access management in IoT,” IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, 2018. doi: 10.1109/JIOT.2018.2812239

[7] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, “Fog computing for the Internet of Things: Security and privacy issues,” IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017. doi: 10.1109/MIC.2017.37

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] 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

[16] 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

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

[18] 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

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

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

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

[22] 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

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

[24] 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

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

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

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

[28] 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

[29] 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

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

[31] 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

[32] 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

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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

[38] 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

[39] 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

[40] 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

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

[42] 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

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

[44] 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

[45] 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

[46] 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

[47] 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

[48] 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

[49] 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

[50] 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

[51] 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

[52] 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

[53] 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

[54] 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

[55] 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

[56] 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

[57] 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

[58] 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

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

[60] 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

[61] 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

[62] 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

[63] 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

[64] 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

[65] 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

[66] 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

[67] 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

[68] 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

[69] 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

[70] 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

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

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

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

[74] 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

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

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

[77] 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

[78] 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

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

[80] 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

[81] 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

[82] 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

[83] 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

[84] 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

[85] 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

[86] 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

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

[88] 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

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

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

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

[92] 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

[93] 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

[94] 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

[95] 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.

[96] 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.

[97] 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

[98] 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

[99] 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

[100] 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

[101] 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

[102] 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

[103] 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.

[104] 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

[105] 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

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

[107] 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

[108] 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

[109] 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

[110] 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

[111] 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

[112] 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

[113] 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

[114] 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

[115] 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

[116] 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

[117] 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

[118] 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

[119] 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

[120] 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

[121] 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

[122] 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

[123] 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

[124] 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

[125] 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

[126] 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

[127] 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

[128] 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

[129] 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

[130] 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

[131] 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

[132] 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

[133] 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

[134] 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

[135] 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

[136] 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

[137] 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

[138] 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

[139] 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

[140] 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

[141] 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

[142] 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

[143] 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

[144] 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

[145] 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

[146] 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

[147] 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

[148] 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).

[149] 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

[150] 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

[151] 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

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

[153] 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

[154] A., Md Sazid (2026). Comparative Performance Analysis of AI-Optimized MPPT Algorithms for Grid-Connected Solar PV Systems. Zenodo. https://doi.org/10.5281/zenodo.18261309

[155] 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(01), 105–121. https://doi.org/10.30574/wjaets.2026.18.1.1577

[156] Ali, A. (2026). The impact of packaging design on recycling efficiency in municipal systems. World Journal of Advanced Engineering Technology and Sciences, 18(01), 122–139. https://doi.org/10.30574/wjaets.2026.18.1.0019

[157] 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(01), 140–156. https://doi.org/10.30574/wjaets.2026.18.1.0026

[158] Taimun, M. T. Y., Alam, M. S., & Fareed, S. M. (2026). Digital twin-enabled predictive maintenance for textile and mechanical systems. World Journal of Advanced Engineering Technology and Sciences, 18(01), 187–203. https://doi.org/10.30574/wjaets.2026.18.1.0001

[159] Fazle, A. B., Taimun, M. T. Y., Fareed, S. M., & Alam, M. S. (2026). Ergonomic and automation based process redesign in industrial workstations. Global Journal of Engineering and Technology Advances, 26(01), 091–108. https://doi.org/10.30574/gjeta.2026.26.1.0010

[160] Alam, M. S., Fareed, S. M., Fazle, A. B., & Taimun, M. T. Y. (2026). Intelligent material flow optimization using IoT sensors and RFID tracking. Global Journal of Engineering and Technology Advances, 26(01), 109–125. https://doi.org/10.30574/gjeta.2026.26.1.0011

[161] 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(01), 219–235. https://doi.org/10.30574/wjaets.2026.18.1.0031

[162] Rahman, F., Nahar, S., & Mim, M. A. (2026). Cloud-native enterprise resource management for multi-sector operations. Global Journal of Engineering and Technology Advances, 26(01), 126–141. https://doi.org/10.30574/gjeta.2026.26.1.0012