Open Access Research Journal of
Engineering and Technology
Journals home page: https://oarjpublication/journals/oarjet/
ISSN: 2783-0128 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(RESEARCH ARTICLE)

A CYBER-RESILIENT EDGE INTELLIGENCE FRAMEWORK FOR SECURE AUTONOMOUS ROBOTIC SYSTEMS IN CRITICAL INFRASTRUCTURE

Mission Franklin [1,*] and Kufre Christopher Ukpe [2]

[1] Department of Computer Engineering, Rivers State University, Port Harcourt, Rivers State, Nigeria
[2] Department of computer Science, Obong university, Obong Ntak, Akwa Ibom State, Nigeria.
* Corresponding Author

ORCID Details
Mission Franklin: https://orcid.org/0009-0003-1382-3460
Kufre Christopher Ukpe: https://orcid.org/0009-0005-2734-9821

Open Access Research Journal of Engineering and Technology, 2026, 11(02), 024–034

Publication history: Received on 27 September 2026; revised on 05 November 2026; accepted on 07 November 2026

Article DOI: https://doi.org/10.53022/oarjet.2026.11.2.0073

Copyright © 2026 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution License 4.0

ABSTRACT

The increasing deployment of autonomous robotic systems in critical infrastructure has heightened cybersecurity concerns, particularly regarding operational safety, reliability, and continuity. This study proposes a Cyber-Resilient Edge Intelligence Framework (CREIF) for secure autonomous robotic systems in critical infrastructure. The framework was developed using the Design Science Research (DSR) methodology, involving requirements analysis, architectural design, expert validation, and refinement. It integrates six layers: perception, edge intelligence, cyber resilience, secure communication, trust management, and adaptive robotic control. The framework was evaluated by ten experts using five criteria: functionality, security, resilience, scalability, and applicability. Descriptive statistical analysis produced an overall mean score of 4.64 and a standard deviation of 0.49 on a five-point Likert scale, exceeding the acceptance threshold of 3.50. Security recorded the highest mean score (4.80), followed by functionality (4.70), resilience and applicability (4.60 each), and scalability (4.50). These findings indicate strong expert agreement on the framework's design quality and suitability for critical infrastructure applications. The study concludes that CREIF provides an integrated architectural foundation for strengthening cybersecurity, edge intelligence, trust management, and operational resilience in autonomous robotic systems. The framework offers a basis for subsequent simulation-based and real-world implementation and evaluation.

Keywords: Autonomous robotic systems; Cyber resilience; Edge intelligence; Edge computing; Artificial intelligence; Critical infrastructure; Secure communication; Trust management; Design Science Research.

1 INTRODUCTION

The increasing adoption of autonomous robotic systems has transformed the operation of critical infrastructure, including power grids, oil and gas facilities, transportation networks, healthcare institutions, water treatment plants, and smart manufacturing industries. Equipped with artificial intelligence (AI), Internet of Things (IoT) technologies, edge computing, and cyber-physical systems (CPS), these robots perform critical tasks such as infrastructure inspection, predictive maintenance, surveillance, and emergency response with minimal human intervention. Their ability to operate efficiently in hazardous and complex environments has improved productivity, enhanced operational safety,

and reduced human risk. However, the growing connectivity and autonomy of these systems have also expanded their exposure to cyber threats, making the security of autonomous robotic systems an increasingly important concern (Santoso & Finn, 2024; Singh & Gill, 2023).

As critical infrastructure continues to embrace Industry 4.0 and Industry 5.0 technologies, autonomous robotic systems have become indispensable for ensuring reliable and uninterrupted service delivery. Despite these benefits, integrating robotics with cloud platforms, industrial IoT devices, and wireless communication networks has introduced new cybersecurity challenges. Cyberattacks such as denial-of-service (DoS), distributed denial-of-service (DDoS), false data injection, sensor spoofing, replay attacks, malware, GPS spoofing, and command hijacking can disrupt robot perception, manipulate control decisions, and compromise mission-critical operations. In environments where timely and accurate decisions are essential, even minor disruptions can lead to equipment damage, service outages, environmental incidents, or threats to human safety (Ansari et al., 2024; Segovia-Ferreira et al., 2024).

Most existing autonomous robotic systems rely on cloud-centric architectures to support data processing, storage, and AI model execution. Although cloud computing provides substantial computational resources, it also introduces communication delays, bandwidth limitations, privacy concerns, and dependence on stable network connectivity. These limitations become particularly critical during cyberattacks or network failures, where delayed responses or interrupted communication can significantly degrade robotic performance. As a result, edge computing has emerged as an attractive alternative by enabling data processing and intelligent decision-making closer to robotic devices, thereby reducing latency, improving responsiveness, and enhancing system reliability (Singh & Gill, 2023; Gill et al., 2025).

The integration of edge computing with AI, commonly referred to as Edge Intelligence (Edge AI), enables autonomous robots to analyse data, detect anomalies, and make decisions locally without relying heavily on centralized cloud infrastructure (Zhou et al., 2024). This capability supports real-time applications such as object recognition, navigation, path planning, predictive maintenance, and adaptive control while reducing communication overhead and improving operational efficiency. Nevertheless, current research has largely focused on individual aspects of robotic security, such as intrusion detection, anomaly detection, or secure communication, with limited attention given to developing an integrated framework that combines edge intelligence, cyber resilience, and autonomous robotic control (Gill et al., 2025).

Cyber resilience extends beyond conventional cybersecurity by focusing not only on preventing cyberattacks but also on ensuring that systems can anticipate, withstand, recover from, and adapt to evolving threats while maintaining essential operations. For autonomous robotic systems deployed in critical infrastructure, achieving cyber resilience requires the seamless integration of intelligent threat detection, resilient control mechanisms, secure communication, trust management, and adaptive recovery capabilities. Recent studies have highlighted the need for comprehensive architectures capable of delivering these capabilities while satisfying the stringent requirements for low latency, high availability, and operational continuity in mission-critical environments (Ansari et al., 2024; Segovia-Ferreira et al., 2024).

Despite significant advances in AI-based cybersecurity and edge computing, there remains a lack of unified frameworks that simultaneously address intelligent cyberattack detection, resilient autonomous control, secure communication, and edge-enabled decision-making for robotic systems operating in critical infrastructure. Existing approaches often address these challenges independently, resulting in solutions that are difficult to deploy in complex, real-world environments. This gap underscores the need for an integrated framework capable of providing both robust cybersecurity and uninterrupted autonomous operation.

1.1 Statement of the Problem

The increasing deployment of autonomous robotic systems in critical infrastructure has improved the efficiency, safety, and reliability of operations such as inspection, surveillance, predictive maintenance, and emergency response. However, the integration of artificial intelligence (AI), Internet of Things (IoT), edge computing, and cyber-physical systems (CPS) has also expanded the cyberattack surface of these systems, exposing them to increasingly sophisticated threats. Cyberattacks, including denial-of-service (DoS), false data injection, sensor spoofing, malware, replay attacks, and command hijacking, can disrupt robotic perception, manipulate control decisions, interrupt communication, and compromise mission-critical operations. In sectors such as power, oil and gas, healthcare, transportation, and water treatment, these attacks may result in operational downtime, equipment damage, financial losses, environmental hazards, and risks to human safety (Santoso & Finn, 2024; Ansari et al., 2024).

Although cloud computing provides the computational resources required for AI-driven robotic applications, cloud-centric architectures are often unsuitable for safety-critical environments because they depend on continuous network connectivity and centralized processing. Communication delays, bandwidth limitations, and network failures can significantly reduce the responsiveness and reliability of autonomous robotic systems during cyber incidents. While

edge computing addresses many of these limitations by enabling localized processing and real-time decision-making, existing studies have largely focused on isolated solutions, such as intrusion detection, anomaly detection, secure communication, or robotic control, rather than providing an integrated approach that combines these capabilities within a cyber-resilient architecture (Singh & Gill, 2023; Gill et al., 2025).

Furthermore, current approaches often prioritize attack detection without adequately addressing cyber resilience, which is the ability of autonomous robotic systems to anticipate, withstand, recover from, and adapt to cyberattacks while maintaining essential operations. As a result, there remains a lack of comprehensive frameworks that integrate edge intelligence, AI-driven threat detection, resilient autonomous control, secure communication, and trust management to ensure continuous and secure robotic operation in critical infrastructure (Segovia-Ferreira et al., 2024). To address this gap, this study proposes a Cyber-Resilient Edge Intelligence Framework for Secure Autonomous Robotic Systems in Critical Infrastructure.

1.2 Aim and Objectives of the Study

This study aims to design and evaluate a Cyber-Resilient Edge Intelligence Framework for enhancing the security and resilience of autonomous robotic systems in critical infrastructure.

The study objectives are to:

- Design a cyber-resilient edge intelligence framework for secure autonomous robotic systems.
- Develop an AI-driven mechanism for real-time cyberattack detection and resilient control.
- Evaluate the framework under representative cyberattack scenarios.
- Assess the framework's performance in terms of security, latency, resilience, and operational efficiency.

1.3 Significance and Scope of the Study

This study proposes a Cyber-Resilient Edge Intelligence Framework designed to enhance the security, resilience, and real-time operation of autonomous robotic systems deployed in critical infrastructure. The framework contributes to the advancement of secure edge-enabled robotic systems by integrating cyber resilience with edge intelligence, thereby providing a robust foundation for future research and practical deployment in cyber-physical environments. The study focuses on the design and evaluation of the proposed framework within the context of critical infrastructure. Its performance is assessed under representative cyberattack scenarios using key evaluation metrics, including security effectiveness, latency, resilience, and operational performance.

2 LITERATURE REVIEW

Autonomous Robotic Systems (ARS) in Critical Infrastructure: Autonomous robotic systems (ARS) are increasingly used in critical infrastructure to perform tasks such as inspection, monitoring, maintenance, and emergency response with minimal human intervention. Advances in AI, machine learning, sensors, and edge computing have improved their ability to operate efficiently and make real-time decisions across sectors including energy, manufacturing, transportation, healthcare, and oil and gas (Siciliano & Khatib, 2016; Santoso & Finn, 2024). Despite these benefits, greater connectivity has made robotic systems more vulnerable to cyber threats such as denial-of-service (DoS), malware, sensor spoofing, and false data injection, which can disrupt operations and compromise safety (Ansari et al., 2024).

Cyber-Physical Systems and Critical Infrastructure Security: Cyber-Physical Systems (CPS) integrate physical devices, communication networks, and computing technologies to monitor and control critical infrastructure in real time. The integration of operational technology (OT), information technology (IT), cloud computing, and edge computing has improved automation and operational efficiency but has also expanded the cyberattack surface (Harkat et al., 2024; Sun et al., 2024). To ensure reliable operation, CPS must provide not only confidentiality, integrity, and availability (CIA), but also safety, resilience, real-time performance, and rapid recovery from cyber incidents. However, vulnerabilities such as weak authentication, insecure protocols, legacy systems, and software flaws expose CPS to attacks including DoS, malware, sensor spoofing, and false data injection. Recent attacks on energy, water, manufacturing, and healthcare systems have highlighted these risks and reinforced the need for cyber-resilient architectures that integrate real-time threat detection, resilient control, and rapid recovery to maintain secure and uninterrupted operations (Sun et al., 2024; Fitzgerald & Morisset, 2024; Ji et al., 2024).

Edge Computing for Autonomous Robotics: Edge computing brings computing resources closer to robots and sensors, enabling faster data processing and real-time decision-making. A typical edge architecture consists of three layers: the device layer (robots and sensors), the edge layer (local processing and intelligence), and the cloud layer (data storage, model training, and large-scale analytics). This distributed approach reduces latency and improves the reliability of

autonomous robotic systems (Gill et al., 2025; Singh & Gill, 2023). Compared with cloud computing, edge computing processes time-sensitive tasks locally while the cloud handles computationally intensive operations such as AI model training and long-term data analysis. This combination improves response time, reduces bandwidth usage, enhances data privacy, and allows robots to continue operating even during network disruptions (Shi et al., 2016; Gill et al., 2025). Despite these advantages, edge deployment faces challenges including limited computing resources, device heterogeneity, security vulnerabilities, and the complexity of managing distributed AI models (Gill et al., 2025; Shi et al., 2016).

Edge Intelligence (Edge AI): Edge Intelligence (Edge AI) combines artificial intelligence with edge computing to enable data processing and decision-making directly on robots and other edge devices. Unlike cloud-based AI, Edge AI performs inference locally, reducing latency, saving bandwidth, improving data privacy, and enabling real-time responses in applications such as autonomous robotics, smart manufacturing, and intelligent transportation (Gill et al., 2025; Singh & Gill, 2023). By processing data at the edge, robots can quickly perform tasks such as object recognition, navigation, fault detection, and obstacle avoidance without relying on constant cloud connectivity. Lightweight AI models, including optimized neural networks, make it possible to deploy AI on resource-constrained edge devices while maintaining acceptable performance. Despite its advantages, most existing research focuses on improving AI efficiency rather than integrating Edge AI with cyber resilience, secure communication, and trust management (Santoso & Finn, 2024; Gill et al., 2025).

Cybersecurity Threats in Autonomous Robotic Systems: Autonomous robotic systems depend on interconnected sensors, communication networks, edge devices, and cloud platforms, making them vulnerable to cyber threats. Common attacks include Denial-of-Service (DoS/DDoS), false data injection, sensor and GPS spoofing, replay attacks, man-in-the-middle (MitM) attacks, malware, ransomware, and command hijacking. These threats can disrupt communication, manipulate sensor data, compromise navigation and control, cause equipment damage, and interrupt critical operations (Santoso & Finn, 2024; Ansari et al., 2024). Protecting autonomous robots requires secure communication, strong authentication, access control, AI-based threat detection, continuous monitoring, and resilient recovery mechanisms. However, most existing solutions focus on specific attacks rather than providing comprehensive protection. This highlights the need for integrated cyber-resilient edge intelligence frameworks that can detect, withstand, and recover from evolving cyber threats while ensuring safe and reliable robotic operation in critical infrastructure (Segovia-Ferreira et al., 2024; Gill et al., 2025).

Cyber Resilience for Robotic Systems: As autonomous robots become widely deployed in critical infrastructure, they must not only resist cyberattacks but also continue operating during and after an attack. Cyber resilience goes beyond traditional cybersecurity by enabling systems to anticipate, detect, respond to, recover from, and adapt to cyber incidents while maintaining essential functions (Ansari et al., 2024; Segovia-Ferreira et al., 2024). Cyber resilience combines secure system design, continuous monitoring, AI-based threat detection, fault tolerance, adaptive control, and rapid recovery to ensure operational continuity. Established frameworks such as the National Institute of Standards and Technology(NIST) Cybersecurity Framework (CSF 2.0), IEC 62443, and ISO/IEC 27001 provide valuable guidance for securing cyber-physical systems, but they do not fully address the real-time and autonomous requirements of robotic systems (International Electrotechnical Commission, 2023). This highlights the need for integrated cyber-resilient frameworks that combine edge intelligence, AI-driven security, and resilient robotic control to support safe and reliable operations in critical infrastructure (National Institute of Standards and Technology., 2024; Gill et al., 2025).

Artificial Intelligence for Robotic Cybersecurity: Artificial intelligence (AI) plays a vital role in robotic cybersecurity by enabling autonomous systems to detect, analyse, and respond to cyber threats in real time. Machine learning and deep learning improve intrusion and anomaly detection, while reinforcement learning supports adaptive cyber defence and resilient decision-making. In addition, Explainable AI (XAI) enhances the transparency of AI-driven security decisions, increasing trust and accountability in autonomous robotic systems (Santoso & Finn, 2024; Gill et al., 2025). Although AI has significantly strengthened robotic cybersecurity, challenges remain in deploying resource-intensive models on edge devices and integrating AI with cyber resilience, secure communication, and real-time autonomous control (Adadi et al, 2018). In cybersecurity and autonomous robotic systems, XAI enables operators to understand the rationale behind AI-based threat detection, anomaly identification, and autonomous decision-making. This enhances situational awareness, supports faster incident response, and facilitates compliance with ethical and regulatory requirements (Samek et al., 2021). XAI models provide insights into the factors influencing AI predictions (Ribeiro et al., 2016; Lundberg & Lee, 2017). Integrating XAI into cyber-resilient edge intelligence frameworks improves the transparency, reliability, and trustworthiness of AI-driven decisions, making autonomous robotic systems more secure and suitable for deployment in critical infrastructure environments (Adadi et al., 2018). Arrieta et al., 2020). These limitations highlight the need for intelligent, cyber-resilient frameworks that combine AI with edge computing to ensure secure and reliable robotic operations in critical infrastructure.

Secure Communication and Trust Management: Secure communication and trust management are essential for autonomous robotic systems, enabling safe data exchange among robots, sensors, edge devices, and cloud platforms. To

protect against threats such as eavesdropping, spoofing, replay attacks, and unauthorized access, robotic systems use secure communication protocols, encryption, authentication, and access control mechanisms (Santoso & Finn, 2024;). Trust management further enhances security by assessing the reliability of devices and detecting compromised nodes, while blockchain technology provides decentralized identity management, secure communication, and tamper-resistant record keeping. However, challenges such as computational overhead, scalability, and maintaining real-time performance remain, highlighting the need for lightweight and integrated security solutions for cyber-resilient robotic systems.

Existing Cyber-Resilient Robotic Frameworks: Existing cyber-resilient robotic frameworks combine AI, edge computing, blockchain, and resilient control to improve the security and reliability of autonomous robotic systems. AI-based frameworks enhance intrusion detection, edge computing enables real-time decision-making, blockchain strengthens trust and secure communication, and cyber resilience models support continuous monitoring, response, and recovery from cyber incidents (Santoso & Finn, 2024; Gill et al., 2025). Despite these advances, most frameworks focus on specific aspects of security rather than providing a fully integrated solution. Common limitations include limited support for adaptive recovery, operational continuity, trust management, and comprehensive validation across diverse critical infrastructure environments. These gaps highlight the need for unified cyber-resilient edge intelligence frameworks that combine AI, secure communication, trust management, and resilient control for autonomous robotic systems (Segovia-Ferreira et al., 2024).

Comparative Analysis: A review of existing studies shows that no single framework fully addresses the security, resilience, and real-time requirements of autonomous robotic systems. AI-based approaches provide effective threat detection, edge computing reduces latency, blockchain improves trust, and cyber resilience frameworks support recovery. However, these solutions are often developed independently and lack integration. This gap highlights the need for a unified Cyber-Resilient Edge Intelligence Framework that combines AI-driven threat detection, edge computing, secure communication, trust management, adaptive control, and rapid recovery to ensure secure and reliable robotic operations in critical infrastructure.

2.1 Empirical Review

Recent empirical studies highlight the increasing role of artificial intelligence (AI), edge computing, and cybersecurity in improving the performance and resilience of autonomous robotic systems. While these studies have made significant contributions in areas such as intrusion detection, edge intelligence, and cyber resilience, most focus on individual aspects rather than providing an integrated solution for secure and resilient robotic operations.

Santoso and Finn (2024) examined the use of AI-enhanced cybersecurity techniques for robotics, autonomous systems, and critical infrastructure. Through an extensive review of AI-based security approaches, they found that machine learning and deep learning algorithms significantly improved the detection of cyber threats such as malware, denial-of-service (DoS), and spoofing attacks. Despite these promising results, the study concentrated mainly on threat detection and did not develop a unified framework that integrates edge intelligence, cyber resilience, trust management, and adaptive robotic control.

Segovia-Ferreira et al. (2024) carried out a systematic review of cyber-resilience strategies for cyber-physical systems. Their findings showed that most existing frameworks emphasize prevention, detection, response, and recovery mechanisms. However, they observed that these approaches offer limited support for autonomous robotic systems operating under strict real-time conditions. The authors also identified the lack of integrated architectures capable of combining resilient control, AI-driven cybersecurity, and distributed edge intelligence.

Gill et al. (2025) developed a comprehensive taxonomy of Edge AI technologies and assessed their applications across intelligent systems. The study demonstrated that Edge AI significantly reduced inference latency, lowered bandwidth consumption, and enhanced real-time decision-making when compared with cloud-based architectures. However, the authors acknowledged that most current Edge AI solutions provide limited cybersecurity functionality and recommended the development of cyber-resilient edge architectures for safety-critical systems.

Ji et al. (2024) reviewed intrusion detection systems for industrial cyber-physical systems and confirmed the effectiveness of machine learning in detecting malicious network activities. Despite these advances, the authors concluded that many existing solutions depend heavily on centralized processing, making them unsuitable for resource-constrained edge environments where autonomous robots require fast local decision-making and immediate threat response.

Singh and Gill (2023) investigated Edge AI as a distributed computing paradigm for intelligent applications. Their findings showed that performing AI inference at the edge significantly improves response time, enhances privacy, and increases overall system efficiency. However, they also observed that most Edge AI implementations focus primarily on

computational optimization while giving limited attention to cyber resilience, secure communication, and trust management for autonomous robotic systems.

The reviewed studies demonstrate significant advances in AI-enabled cybersecurity, intrusion detection, edge computing, and cyber resilience for autonomous robotic systems. However, most existing solutions address these technologies independently, resulting in limited integration of AI-driven threat detection, secure communication, trust management, adaptive response, and real-time edge intelligence. Hence, there is a need for a unified cyber-resilient edge intelligence framework. This study addresses this gap by proposing an integrated architecture that combines these capabilities to enable secure, resilient, and continuous operation of autonomous robotic systems in critical infrastructure.

3 METHODOLOGY

This study adopts the Design Science Research (DSR) methodology to develop and validate a Cyber-Resilient Edge Intelligence Framework for Autonomous Robotic Systems in Critical Infrastructure. The methodology consists of the following phases:

3.1 Framework Requirements Analysis

These requirements provide the design specifications for the proposed Cyber-Resilient Edge Intelligence Framework and are classified into functional and non-functional requirements. The functional requirements define the core capabilities of the framework, which include: AI-based threat detection, edge intelligence, cyber resilience, secure communication; trust management, adaptive robotic control. The non-functional requirements specify the quality attributes of the framework including low latency, scalability, reliability, interoperability, security and privacy. These requirements ensure that the proposed framework is secure, resilient, efficient, and suitable for deployment in critical infrastructure environments.

3.2 Framework Design

The proposed Cyber-Resilient Edge Intelligence Framework is designed based on the identified functional and non-functional requirements. It adopts a layered architecture that integrates AI-based threat detection, edge intelligence, cyber resilience, secure communication, trust management, and adaptive robotic control. The designed framework is shown in Figure 1. The framework components work together to enable real-time threat detection, secure data exchange, low-latency decision-making, and resilient operation of autonomous robotic systems in critical infrastructure environments.

3.3 Framework Validation /Expert Evaluation Model

The proposed Cyber-Resilient Edge Intelligence Framework was validated through expert review. A panel of 5–10 experts with expertise in cybersecurity, artificial intelligence, robotics, edge computing, and critical infrastructure were selected to evaluate the framework. Their expertise ensure that the proposed architecture was assessed from both technical and practical perspectives. A structured evaluation questionnaire used to assess the framework based on five key criteria: *functionality, security, resilience, scalability, and applicability.* The experts rated each criterion using a 5-point Likert scale, where 5 = Excellent, 4 = Very Good, 3 = Good, 2 = Fair, and 1 = Poor. The collected responses were analysed using descriptive statistics, specifically the mean and standard deviation. A mean score of 3.50 or above will indicate that the framework is acceptable. The experts' comments and recommendations were used to refine and improve the framework before presenting the final validated architecture.

3.4 Evaluation and Refinement

The results of the expert review were evaluated using the mean scores and standard deviations obtained for each assessment criterion. The findings were used to determine the strengths and weaknesses of the proposed framework. Experts' comments and recommendations were incorporated to refine the framework by improving its functionality, security, resilience, scalability, and applicability. The refined framework serves as the final validated architecture for secure and resilient autonomous robotic systems in critical infrastructure.

3.5 Final Framework

The refined Cyber-Resilient Edge Intelligence Framework is presented as the final outcome of this study. The framework integrates AI-based threat detection, edge intelligence, cyber resilience, secure communication, trust management, and adaptive robotic control into a unified architecture. It is designed to support secure, resilient, and real-time operation of autonomous robotic systems in critical infrastructure, while addressing the limitations identified in existing studies.

3.6 Mathematical Methods

Expert Evaluation Model: The ratings provided by the experts serves as the basis for assessing the quality, relevance, and applicability of the proposed framework and was subsequently analysed using descriptive statistics. Suppose: E= Number of experts, C= Number of evaluation criteria, R_{ij}= Rating assigned by expert $i$to criterion j. The expert rating matrix is represented as:

$$R = \begin{bmatrix} R_{11} & R_{12} & \cdots & R_{1C} \\ R_{21} & R_{22} & \cdots & R_{2C} \\ \vdots & \vdots & \ddots & \vdots \\ R_{E1} & R_{E2} & \cdots & R_{EC} \end{bmatrix}$$ .....(1) where: $R_{ij} \in \{1,2,3,4,5\}$. This matrix forms the raw evaluation data collected from the experts.

3.7 Descriptive Statistics

(a) Mean Score for each evaluation criterion: $\bar{R}_j = \frac{1}{E}\sum_{i=1}^{E} R_{ij}$ .....(1) , where: $\bar{R}_j$= Mean score of criteria j , R_{ij}= Rating by expert i , E= Number of experts

(b) Overall Framework Mean Score: $\bar{R} = \frac{1}{C}\sum_{j=1}^{C} \bar{R}_j$ .....(2) where C= Number of evaluation criteria.

(c) The Standard Deviation determine the level of agreement among experts

$SD_j = \sqrt{\frac{\sum_{i=1}^{E}(R_{ij}-\bar{R}_j)^2}{E-1}}$ .....(3), where SD_j= Standard deviation for criterion j. A lower standard deviation indicates greater agreement among experts.

(d) The Decision Rule is defined as: accepted when $\bar{R}_j \geq 3.50$ and rejected when $\bar{R}_j < 3.50$

4 RESULTS

4.1 Proposed Cyber-Resilient Edge Intelligence Framework

The main outcome of this study is the development of a Cyber-Resilient Edge Intelligence Framework for autonomous robotic systems operating in critical infrastructure. The framework, which is further refined, with improvement as shown in Figure 2, as the final version of the framework, which integrates six core components: *Perception Layer, Edge Intelligence Layer, Cyber Resilience Layer, Secure Communication Layer, Trust Management Layer, and Adaptive Robotic Control Layer*. Together, these components enable real-time threat detection, secure communication, intelligent edge processing, adaptive decision-making, and resilient robotic operation. The framework addresses the limitations identified in previous studies by providing a unified architecture that combines AI-driven cybersecurity, edge computing, trust management, and cyber resilience. Figure 1 presents the final framework.

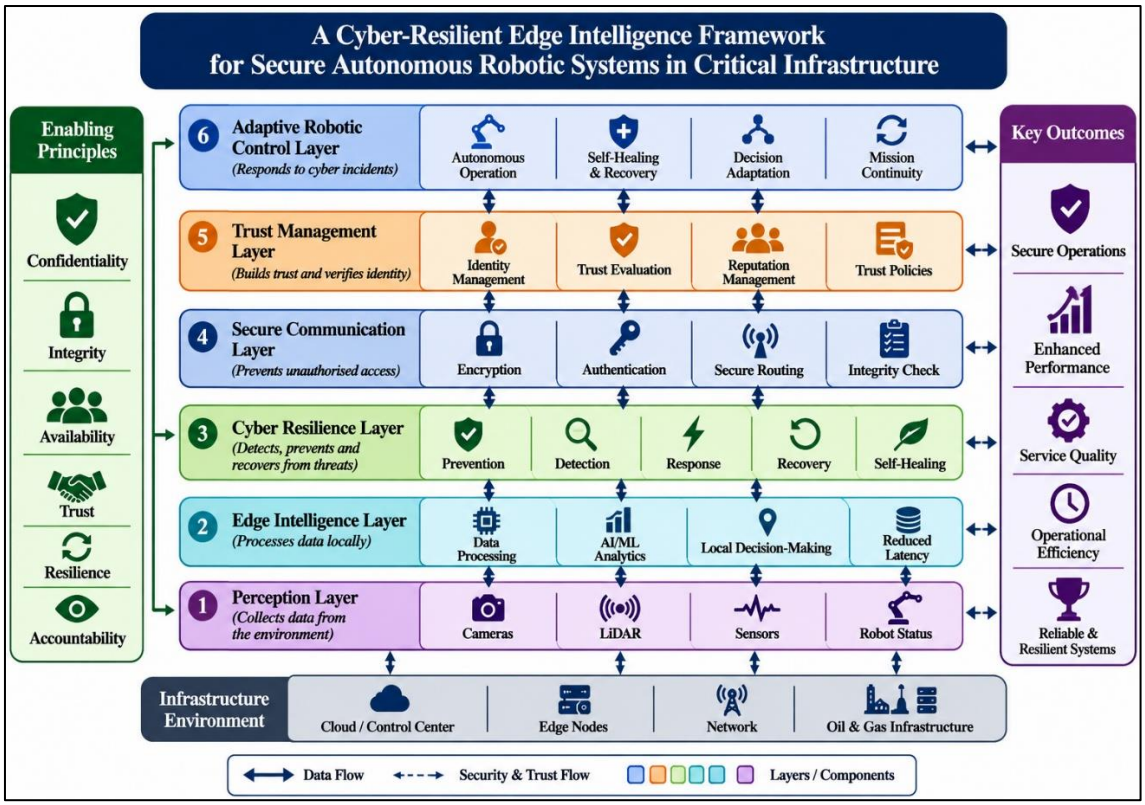


Figure 1: Final version of Cyber-Resilient Edge Intelligence Framework

4.2 Framework Description

(i) *The Perception Layer* acquires data from sensors, robots, and critical infrastructure devices. (ii) *The Edge Intelligence Layer* performs local AI-based processing for rapid threat detection and decision-making. (iii)*The Cyber Resilience Layer* continuously monitors the system and provides prevention, detection, response, and recovery capabilities against cyber threats. (iv)*The Secure Communication Layer* protects data exchange through authentication, encryption, and integrity verification, while the (v)*Trust Management Layer* evaluates the trustworthiness of devices and communication entities. Finally, (vi) *Adaptive Robotic Control Layer* enables autonomous robots to maintain safe and continuous operation by adapting to cyber incidents and system changes.

4.3 Expert Validation Results

The proposed framework was evaluated by experts using five criteria: functionality, security, resilience, scalability, and applicability. The evaluation result as indicated in Table 1. the framework satisfies the identified system requirements and is suitable for deployment in critical infrastructure environments.

Table 1: Expert Raw Evaluation Scores

Evaluation Criterion	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
Functionality	5	5	4	5	4	5	5	4	5	5
Security	5	5	5	4	5	5	5	5	4	5
Resilience	5	4	5	4	5	5	4	5	5	4
Scalability	4	5	4	4	5	4	5	4	5	5
Applicability	5	4	5	5	4	5	5	4	5	4

Table 2: Summary of Expert Evaluation

Evaluation Criterion	Mean	Std. Dev.	Decision
Functionality	4.70	0.48	Accepted
Security	4.80	0.42	Accepted
Resilience	4.60	0.52	Accepted
Scalability	4.50	0.53	Accepted
Applicability	4.60	0.52	Accepted
Overall	4.64	0.49	Accepted

**Decision Rule*: A criterion is accepted when its mean score is ≥ 3.50 and rejected < 3.50.

The raw evaluation results as shown in Table 2 indicate that all experts rated the proposed framework between 4 (Very Good) and 5 (Excellent) across the five evaluation criteria. All five evaluation criteria achieved mean scores above the acceptance threshold of 3.50. The overall mean score of 4.64, which exceeds the acceptance threshold of 3.50, indicates that the proposed Cyber-Resilient Edge Intelligence Framework (CREIF) is considered functional, secure, resilient, scalable, and applicable for deployment in critical infrastructure environments. The relatively low standard deviations, ranging from 0.42 to 0.53, are indicative of a high level of agreement among the experts regarding the quality and suitability of the framework.

5 DISCUSSION

The findings demonstrate that the proposed Cyber-Resilient Edge Intelligence Framework (CREIF) effectively addresses the limitations identified in previous studies by integrating AI-based threat detection, edge intelligence, cyber resilience, secure communication, trust management, and adaptive robotic control into a unified architecture. Unlike existing approaches, which primarily focus on individual aspects such as intrusion detection or edge computing, the proposed framework provides a comprehensive solution for secure and resilient operation of autonomous robotic systems in critical infrastructure.

The expert evaluation results indicate that the framework is functional, secure, resilient, scalable, and applicable for deployment in critical infrastructure environments. The high mean scores across all evaluation criteria suggest that the framework meets its intended objectives and is capable of supporting real-time threat detection, low-latency decision-making, secure communication, and continuous robotic operation during cyber incidents. The low standard deviations further indicate a high level of concordance among the experts regarding the suitability of the proposed framework.

These findings are consistent with previous studies that emphasized the importance of integrating AI, edge computing, and cybersecurity for autonomous robotic systems. However, the proposed framework extends existing research by providing a unified architecture that combines these technologies with trust management and adaptive robotic control. Therefore, the framework offers a more comprehensive approach to enhancing the security, resilience, and reliability of autonomous robotic systems operating in critical infrastructure.

The proposed framework makes both theoretical and practical contributions by providing a structured architecture that can guide future research and implementation of cyber-resilient autonomous robotic systems.

6 CONCLUSION

This study proposed a Cyber-Resilient Edge Intelligence Framework (CREIF) for autonomous robotic systems operating in critical infrastructure. The framework integrates AI-based threat detection, edge intelligence, cyber resilience, secure communication, trust management, and adaptive robotic control into a unified architecture to address the limitations of existing approaches.

The framework was developed using the Design Science Research (DSR) methodology and validated through expert evaluation. The validation results indicate that the proposed framework is functional, secure, resilient, scalable, and applicable for supporting the secure and continuous operation of autonomous robotic systems in critical infrastructure environments.

The study contributes to the existing body of knowledge by providing an integrated framework that combines key technologies required for cyber-resilient robotic systems. It also offers a practical foundation for researchers and practitioners seeking to enhance the security and reliability of autonomous robots.

Recommendations

Based on the findings of this study, the proposed Cyber-Resilient Edge Intelligence Framework (CREIF) should be implemented and validated in both simulation and real-world critical infrastructure environments to assess its effectiveness against cyber threats. Standardized security protocols and trust management mechanisms should also be adopted to ensure secure communication, interoperability, and reliable collaboration among autonomous robots, edge devices, and cloud platforms. Furthermore, the framework should be evaluated across sectors such as smart grids, healthcare, transportation, and industrial automation to verify its scalability and adaptability.

Future Work

Future work should focus on implementing and validating the proposed Cyber-Resilient Edge Intelligence Framework (CREIF) in simulation and real-world environments to evaluate its performance under cyberattack scenarios. Further research should integrate advanced AI techniques, such as deep learning, reinforcement learning, and federated learning, alongside emerging technologies including 5G/6G, blockchain, and digital twins, to enhance cyber resilience and autonomous decision-making. The framework should also be validated across different critical infrastructure sectors to assess its scalability, interoperability, and adaptability.

STATEMENTS ON COMPLIANCE WITH ETHICAL STANDARDS

Acknowledgments

The authors acknowledge the support of colleagues and institutional facilities that contributed to the completion of this study.

Disclosure of conflict of interest

The authors declare no conflicts of interest regarding this manuscript.

REFERENCES

[1] Adadi, A., & Berrada, M. (2018). *Peeking inside the black box: A survey on Explainable Artificial Intelligence (XAI).* IEEE Access, 6, 52138–52160. https://doi.org/10.1109/ACCESS.2018.2870052

[2] Ansari, I. S., et al. (2024). *A survey on cyber resilience: Key strategies, research challenges, and future directions.* ACM Computing Surveys, 56(8), Article 196. https://doi.org/10.1145/3649218

[3] Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). *Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI.* Information Fusion, 58, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

[4] Fitzgerald, J., & Morisset, C. (2024). *Can we develop holistic approaches to delivering cyber-physical systems security?* Research Directions: Cyber-Physical Systems.

[5] Gill, S. S., Golec, M., Hu, J., Xu, M., Du, J., Wu, H., et al. (2025). *Edge AI: A taxonomy, systematic review, and future directions.* Cluster Computing. https://doi.org/10.1007/s10586-024-04686-y

[6] Harkat, H., Camarinha-Matos, L. M., Goes, J., & Ahmed, H. F. T. (2024). *Cyber-physical systems security: A systematic review.* Computers & Industrial Engineering, 188, 109891.

[7] International Electrotechnical Commission. (2023). *IEC 62443: Industrial communication networks—Network and system security.*

[8] National Institute of Standards and Technology. (2024). *Cybersecurity Framework (CSF) 2.0.* https://www.nist.gov/cyberframework

[9] Santoso, F., & Finn, A. (2024). *An in-depth examination of artificial intelligence-enhanced cybersecurity in robotics, autonomous systems, and critical infrastructures.* IEEE Transactions on Services Computing, 17(3), 1293–1310. https://doi.org/10.1109/TSC.2023.3331083

[10] Segovia-Ferreira, M., Rubio-Hernan, J., Cavalli, A., & Garcia-Alfaro, J. (2024). *A survey on cyber-resilience approaches for cyber-physical systems.* ACM Computing Surveys, 56(8), Article 202. https://doi.org/10.1145/3652953

[11] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). *Edge computing: Vision and challenges.* IEEE Internet of Things Journal, 3(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

[12] Siciliano, B., & Khatib, O. (Eds.). (2016). *Springer handbook of robotics* (2nd ed.). Springer.

[13] Singh, R., & Gill, S. S. (2023). *Edge AI: A survey.* Internet of Things and Cyber-Physical Systems, 3, 71–92. https://doi.org/10.1016/j.iotcps.2023.02.004

[14] Zhou, Z., Chen, X., Li, E., Zeng, L., Luo, K., & Zhang, J. (2024). *Edge intelligence: Paving the last mile of artificial intelligence with edge computing.* Proceedings of the IEEE, 112(2), 198–223.

[15] Lundberg, S. M., & Lee, S.-I. (2017). *A unified approach to interpreting model predictions.* In *Advances in Neural Information Processing Systems* (Vol. 30, pp. 4765–4774).

[16] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). *"Why should I trust you?": Explaining the predictions of any classifier.* In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144).

[17] Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K.-R. (2021). *Explaining deep neural networks and beyond: A review of methods and applications.* Proceedings of the IEEE, 109(3), 247–278.

[18] Ji, R., Padha, D., Singh, Y., & Sharma, S. (2024). Review of intrusion detection systems in cyber-physical system-based networks: Characteristics, attacks, datasets, and challenges. *Transactions on Emerging Telecommunications Technologies*.

[19] Sun, Z., Chen, G., Ding, Y., & Yang, S.-H. (2024). *Joint safety and security risk analysis in industrial cyber-physical systems: A survey*. *IET Cyber-Physical Systems: Theory & Applications, 9*(4), 334–349. (IET Research Journal)