mathematics

MDPI

Article

Zero Trust Strategies for Cyber-Physical Systems in 6G Networks

Abdulrahman K. Alnaim [1,*] and Ahmed M. Alwakeel [2]

[1] Department of Management Information Systems, School of Business, King Faisal University, Hofuf 31982, Saudi Arabia
[2] Faculty of Computers & Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia; aalwakeel@ut.edu.sa
* Correspondence: aalnaim@kfu.edu.sa

Abstract: This study proposes a Zero Trust security framework for 6G-enabled Cyber-Physical Systems (CPS), integrating Adaptive Access Control (AAC), end-to-end encryption, and blockchain to enhance security, scalability, and real-time threat detection. As 6G networks facilitate massive device connectivity and low-latency communication, traditional perimeter-based security models are inadequate against evolving cyber threats such as Man-in-the-Middle (MITM) attacks, Distributed Denial-of-Service (DDoS), and data breaches. Zero Trust security eliminates implicit trust by enforcing continuous authentication, strict access control, and real-time anomaly detection to mitigate potential threats dynamically. The proposed framework leverages blockchain technology to ensure tamper-proof data integrity and decentralized authentication, preventing unauthorized modifications to CPS data. Additionally, AI-driven anomaly detection identifies suspicious behavior in real time, optimizing security response mechanisms and reducing false positives. Experimental evaluations demonstrate a 40% reduction in MITM attack success rates, 5.8% improvement in authentication efficiency, and 63.5% lower latency compared to traditional security methods. The framework also achieves high scalability and energy efficiency, maintaining consistent throughput and response times across large-scale CPS deployments. These findings underscore the transformative potential of Zero Trust security in 6G-enabled CPS, particularly in mission-critical applications such as healthcare, smart infrastructure, and industrial automation. By integrating blockchain-based authentication, AI-powered threat detection, and adaptive access control, this research presents a scalable and resource-efficient solution for securing next-generation CPS architectures. Future work will explore quantum-safe cryptography and federated learning to further enhance security, ensuring long-term resilience in highly dynamic network environments.

Keywords: Zero Trust; Cyber-Physical System; 6G networks; cloud computing; edge computing; blockchain

MSC: 68M10; 68M18; 68M25

check for updates

Academic Editors: Muhammad Syafrudin and Norma Latif Fitriyani

Received: 28 February 2025
Revised: 24 March 2025
Accepted: 26 March 2025
Published: 27 March 2025

Citation: Alnaim, A.K.; Alwakeel, A.M. Zero Trust Strategies for Cyber-Physical Systems in 6G Networks. *Mathematics* **2025**, *13*, 1108. https://doi.org/10.3390/math13071108

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The emergence of 6G networks marks a transformative era for Cyber-Physical Systems (CPS), enabling ultra-reliable, low-latency communication, massive device connectivity, and data transfer rates exceeding 1 Tbps [1]. These advancements position 6G-enabled CPS as critical infrastructures across diverse domains, including healthcare, smart cities, industrial automation, and autonomous systems [2]. With an anticipated 100 billion connected devices by 2030 and 6G latency as low as 1 millisecond, CPS will be capable of real-time responsiveness and unprecedented scalability [3]. However, these advancements also introduce

significant security and operational challenges due to expanded attack surfaces, decentralized architectures, and heterogeneous device environments [4]. Traditional perimeter-based security models are inadequate in dynamic 6G environments, leaving systems vulnerable to Man-in-the-Middle (MITM) attacks, Distributed Denial-of-Service (DDoS), data breaches, and advanced persistent threats (APTs) [5]. The growing complexity of security threats in 6G CPS necessitates a paradigm shift towards Zero Trust Security—a model based on continuous authentication, strict access control, and least-privilege principles [6].

To address these challenges, this paper proposes an integrated Zero Trust Security framework for 6G-enabled CPS, incorporating blockchain-based authentication and AI-driven anomaly detection to enhance security, scalability, and real-time threat mitigation [7]. Blockchain ensures tamper-proof data integrity, mitigating risks associated with data manipulation, unauthorized access, and cyberattacks [8]. Additionally, AI-powered anomaly detection is employed to dynamically identify and mitigate evolving cyber threats such as behavioral anomalies, network intrusions, and insider threats [9]. The proposed framework also addresses energy efficiency and resource constraints, ensuring low-latency decision-making and optimized security performance [10]. This is particularly crucial for applications in remote healthcare monitoring, autonomous industrial control systems, and intelligent transportation networks [11]. By integrating these advanced security strategies, the proposed solution ensures secure, scalable, and efficient CPS operations in next-generation 6G networks, making it a fundamental enabler for sustainable, resilient, and intelligent cyber-physical ecosystems [12].

Moreover, there are challenges from the data integrity, secure communication, and system reliability aspects in real time operations. MITM attacks, which compromise sensitive data, are still a persistent threat in distributed networks for example. Additionally, the integration of large-scale CPS deployments into 6G will need to address scalability challenges as the network loads and device densities increase [13]. Worst still, we lack adaptive access controls and security data management mechanisms to compound these vulnerabilities.

As 6G networks are rapidly developing, they provide unprecedented capabilities for Cyber Physical Systems (CPS), including ultra-low latency, massive connectivity, and high-speed data throughput, which are critical for healthcare [14], smart cities, and industrial automation. Threats include Distributed Denial of Service (DDoS) attacks, data breaches, and advanced persistent threats (APTs), even though these too are only offerings that are being made available to the public. Traditional security models cannot account for the dynamic, heterogeneous, distributed nature of 6G enabled CPS, and thus need to adopt Zero Trust principles. However, while blockchain and AI-driven anomaly detection are promising security technologies, they both face challenges of scalability [15], energy efficiency, and real time performance. The need to develop an integrated Zero Trust framework that blends blockchain for secure data management and AI for real time threat detection is driving this research in order to create scalable, secure, and efficient CPS architectures that meet the needs of 6G environments.

The emergence of 6G networks heralds unprecedented opportunities for Cyber Physical Systems (CPS) with real time responsiveness and ultra-high-speed communication, as well as massive scalability. Meanwhile, these advancements render the dynamic, distributed, and high-density nature of 6G enabled CPS susceptible to vulnerabilities that traditional security mechanisms fail in addressing. This is crucial in domains like healthcare, smart cities, and others, because security breaches have very high consequences [16]. Current solutions, such as blockchain and anomaly detection systems, face limitations in scalability, energy efficiency, and real-time threat mitigation. The first aim of this research is to develop an integrated Zero Trust framework based on blockchain and an AI driven anomaly detection to resolve these challenges [17]. The solution proposed will guarantee

robust security, resource optimization, and scalability, and therefore will lead to the development of secure and efficient CPS infrastructure in 6G networks. The work presented in this research is of critical importance for protecting critical systems while providing the opportunity for sustainable and scalable implementation for future technological and security challenges [18,19].

Problem Formulation 1: Challenges in 6G Enabled CPS Security Frameworks

Security frameworks are a critical challenge to scalability in 6G enabled Cyber Physical Systems (CPS) because the number of inter-connected devices and the amount of data generated grows exponentially. However, existing security mechanisms like blockchain based authentication and anomaly detection are high latency bottlenecks, computationally expensive, and energy inefficient as the network size increases. The challenge is to provide a scalable, resource efficient, and secure framework that provides real time threat mitigation while maintaining high throughput and low latency.

Let the 6G-enabled CPS consist of N devices $\{D_1, D_2, \ldots, D_N\}$, each generating data packets at a rate λ_i (packets/second). The system operates over a set of M communication channels $\{C_1, C_2, \ldots, C_M\}$ with bandwidth B_j (Mbps) for each channel j. The blockchain security mechanism is represented by a distributed ledger $\mathcal{L}$, and the anomaly detection system processes incoming data streams $X_i(t) \in \mathbb{R}^d$ from each device.

The total communication delay L_{comm} is given by:

$$L_{comm} = \sum_{i=1}^{N} \sum_{j=1}^{M} \frac{S_i}{B_j}, \tag{1}$$

where S_i is the size of the data packet generated by device D_i.

The computational overhead $C_{overhead}$ for blockchain verification is:

$$C_{overhead} = \sum_{k=1}^{|\mathcal{L}|} \beta_k f(H_k), \tag{2}$$

where $|\mathcal{L}|$ is the total number of blocks in the ledger, β_k is the weight of block k, and $f(H_k)$ is the hash computation time for block k.

The energy consumption E_{total} for processing and transmitting data is:

$$E_{total} = \sum_{i=1}^{N} (P_{proc,i} + P_{trans,i}), \tag{3}$$

where $P_{proc,i}$ and $P_{trans,i}$ are the processing and transmission power for device D_i, respectively.

To address the scalability challenge, the following objectives are defined:

$$\min L_{comm} = \sum_{i=1}^{N} \sum_{j=1}^{M} \frac{S_i}{B_j}. \tag{4}$$

$$\min C_{overhead} = \sum_{k=1}^{|\mathcal{L}|} \beta_k f(H_k). \tag{5}$$

$$\min E_{total} = \sum_{i=1}^{N} (P_{proc,i} + P_{trans,i}). \tag{6}$$

- N: Total number of devices in the CPS.
- M: Total number of communication channels.
- λ_i: Data generation rate for device D_i (packets/s).
- B_j: Bandwidth of communication channel C_j (Mbps).

- S_i: Data packet size generated by device D_i (bytes).
- $\mathcal{L}$: Blockchain ledger storing security data.
- H_k: Hash of block k in the blockchain ledger.
- β_k: Weight associated with block k for computational cost.
- $P_{proc,i}$: Processing power of device D_i (mW).
- $P_{trans,i}$: Transmission power of device D_i (mW).
- L_{comm}: Total communication delay (ms).
- $C_{overhead}$: Computational overhead for blockchain verification.
- E_{total}: Total energy consumption (mW).

The scalability of security frameworks in 6G-enabled CPS is constrained by three interrelated factors: communication delay, computational overhead, and energy consumption. With the growing number of devices and data traffic, the communication delay is induced by limited channel bandwidth and high data generation rates. At the same time, blockchain based security mechanisms achieve stronger data integrity at the cost of high computational costs in block verification. Furthermore, the energy consumption of transmitting data and processing data grows exponentially with the scale of the network, rendering these frameworks infeasible for resource constrained CPS environments. The objective functions strive to optimize these factors by reducing delays, computational overheads, and energy consumption, making 6G enabled CPSs scalable, secure, and efficient security frameworks. Problem Formulation 2: Real time security and threat detection are key challenges faced by 6G enabled Cyber Physical Systems (CPS)

Particularly in applications of healthcare and industrial automation, where unnecessary delays or undetected threats can result in grave consequences. However, the computational complexity and resource demands of traditional anomaly detection mechanisms do not meet the stringent latency and accuracy requirements of 6G. Moreover, threat landscapes in 6G networks are dynamic and evolving, and hence require adaptive and low latency frameworks for real time threat mitigation. The objective here is to develop a reliable and adaptable threat detection mechanism that minimizes detection latency and maximizes detection accuracy while remaining energy efficient in resource constrained settings.

Let the data streams from N devices be represented as $X_i(t) \in \mathbb{R}^d$, where d is the dimensionality of the feature space. The anomaly detection model f_θ predicts the probability of an anomaly $P(y_i = 1 \mid X_i(t))$ for each device D_i. The model processes data at the edge nodes with limited computational resources $R_{edge,k}$ for $k = 1, 2, \ldots, K$ edge nodes.

1. Detection Latency (L_{detect}): The total detection latency is given by:

$$L_{detect} = \sum_{i=1}^{N} \frac{S_i}{B_{edge,i}} + T_{compute,i}, \tag{7}$$

   where S_i is the size of the input data, $B_{edge,i}$ is the bandwidth allocated to device D_i, and $T_{compute,i}$ is the computation time at the edge node.
2. Detection Accuracy (A_{detect}): The accuracy of the anomaly detection system is defined as:

$$A_{detect} = \frac{\sum_{i=1}^{N} \mathbb{1}[y_i = \hat{y}_i]}{N}, \tag{8}$$

   where $\mathbb{1}[y_i = \hat{y}_i]$ is an indicator function that evaluates to 1 if the predicted label matches the true label.

3. Energy Consumption (E_{detect}): The energy consumption for processing and transmitting data is given by:

$$E_{detect} = \sum_{i=1}^{N} \left(P_{proc,i} T_{compute,i} + P_{trans,i} T_{trans,i} \right), \tag{9}$$

where $T_{trans,i}$ is the data transmission time, and $P_{proc,i}$ and $P_{trans,i}$ are the processing and transmission power for device D_i, respectively.

The objectives for ensuring real-time security and threat detection in 6G CPS are:

$$\min L_{detect} = \sum_{i=1}^{N} \frac{S_i}{B_{edge,i}} + T_{compute,i}. \tag{10}$$

$$\max A_{detect} = \frac{\sum_{i=1}^{N} \mathbb{1}[y_i = \hat{y}_i]}{N}. \tag{11}$$

$$\min E_{detect} = \sum_{i=1}^{N} \left(P_{proc,i} T_{compute,i} + P_{trans,i} T_{trans,i} \right). \tag{12}$$

- N: Total number of devices in the CPS.
- $X_i(t)$: Data stream from device D_i at time t.
- f_θ: Anomaly detection model with parameters θ.
- $P(y_i = 1 \mid X_i(t))$: Probability of anomaly for device D_i.
- S_i: Size of the input data from device D_i.
- $B_{edge,i}$: Bandwidth allocated to device D_i.
- $T_{compute,i}$: Computation time for anomaly detection at the edge node.
- $P_{proc,i}$: Processing power of device D_i (mW).
- $P_{trans,i}$: Transmission power of device D_i (mW).
- $T_{trans,i}$: Data transmission time for device D_i.
- A_{detect}: Accuracy of the anomaly detection system.
- E_{detect}: Total energy consumption for threat detection.

Ensuring real-time security and threat detection in 6G CPS requires balancing three key factors: detection latency, detection accuracy, and energy consumption. Bandwidth limitations and processing constraints lead to limitations at edge nodes that hinder performance, and detection latency is a function of communication delays and computational delays at edge nodes. Detecting true threat is vital to the minimization of false positives and negatives and translating these words into a behavior in a timely and reliable manner. In resource constrained environments, energy consumption is a major concern for anomaly detection systems since too much power consumption can render the systems inoperable. This research aims to develop a robust framework through which these factors can be optimized by carefully designed objective functions to effect adaptive, efficient, and real time threat detection for 6G CPS.

This research aims to build an integrated Zero Trust framework for 6G enabled CPSs that is scalable, secure, and efficient. The specific objectives are:

a. Creating a scalable security architecture that would protect users in these high density 6G networks with low latency and overhead.
b. Integrate blockchain-based authentication and AI-driven anomaly detection for real-time threat mitigation.
c. Optimize resource allocation to minimize energy consumption in resource-constrained CPS environments.

d. Evaluate the framework using performance metrics such as latency, accuracy, scalability, and energy efficiency.
e. We propose to optimize security, responsiveness, and resource efficiency in heterogeneous CPS.

In total, these objectives collectively overcome the limitations of current security frameworks and present a robust, adaptive, and efficient solution for the next generation of CPS in 6G networks. This research makes the following contributions to the field of secure 6G-enabled Cyber-Physical Systems (CPS):

a. Proposing a scalable Zero Trust security framework leveraging blockchain and AI-driven anomaly detection.
b. Developing an energy-efficient resource allocation strategy tailored for CPS environments.
c. Evaluating system performance using security and scalability metrics such as MITM attack resistance, authentication efficiency, and network latency.
d. A comprehensive evaluation of the proposed framework is provided using metrics such as latency, scalability, energy consumption, and detection accuracy for different network scenarios.
e. Provide for the presentation of new optimization techniques for security, real-time responsiveness, and resource efficiency to strike an appropriate balance between security and real time responsiveness in critical 6G-enabled CPS applications like healthcare and smart cities.

Unlike existing blockchain-AI security models, which often operate independently or in isolated domains, the proposed Zero Trust framework integrates permissioned blockchain-based authentication, AI-driven anomaly detection, and adaptive access control into a cohesive security architecture for 6G-enabled CPS. While prior works have employed blockchain primarily for ensuring data integrity or AI for intrusion detection, our framework utilizes Hyperledger Fabric—a permissioned blockchain—to enable secure and tamper-resistant identity management. Although not fully decentralized, Hyperledger Fabric provides a distributed and verifiable authentication infrastructure governed by a consortium model, thereby reducing reliance on single-point-of-failure centralized authorities. AI-based anomaly detection is deployed at the network edge, facilitating real-time threat identification and mitigation. Moreover, our Adaptive Role-Based Access Control (RBAC) system dynamically modifies access permissions based on continuous contextual risk assessment, enforcing least-privilege policies and real-time verification. The integration of Kyber-PQC for quantum-resistant key exchange further enhances the cryptographic resilience of the framework. Collectively, these technologies contribute to a scalable, efficient, and security-optimized Zero Trust framework capable of supporting low-latency and high-density 6G CPS deployments.

This study employs a customized Adaptive Role-Based Access Control (RBAC) mechanism designed specifically for the unique requirements of 6G-enabled Cyber-Physical Systems (CPS). Unlike conventional RBAC models that rely on static user-role-permission mappings, our approach dynamically adjusts access policies in real time based on contextual factors such as network behavior, device activity, and current threat levels as detected by the AI anomaly detection system. While traditional RBAC schemes have been used in enterprise IT systems, their application in high-density, low-latency CPS environments remains limited. Previous work has largely focused on static role hierarchies or attribute-based access control (ABAC), which may not scale effectively in dynamic and resource-constrained CPS deployments. To the best of our knowledge, this is the first implementation of an adaptive, AI-integrated RBAC framework tailored for Zero Trust security in 6G-enabled CPS, using real-time risk assessment to enforce least-privilege access policies. The results presented in this study were achieved using this in-house devel-

oped RBAC module, integrated into the broader SmartCare framework, and evaluated for responsiveness, accuracy, and access enforcement under varying network conditions.

The proposed framework integrates an energy-efficient resource allocation approach that optimizes data transmission, computation, and security enforcement. Instead of relying on a standalone resource allocation algorithm, the system dynamically distributes computational tasks between edge nodes and cloud resources, minimizing energy consumption while maintaining robust security enforcement. By employing adaptive access control policies and lightweight cryptographic techniques, the framework achieves low-latency security operations and ensures scalability across high-density 6G CPS deployments, striking a balance between performance and sustainability.

This paper is organized as follows: In Section 1, the research problem is presented, including the challenges and the objectives of achieving secure and scalable 6G enabled Cyber Physical Systems (CPS). Section 2 reviews the existing literature on Zero Trust security, blockchain, and AI driven anomaly detection in CPS and highlights the main gaps. In Section 3, the proposed methodology is outlined, including mathematical formulations, objective functions, and integrated framework design. The results and discussion of the proposed solution are presented in Section 4, where the proposed solution is evaluated by metrics such as latency, accuracy, scalability, and energy efficiency. In Section 5, we conclude the paper by summarizing the key findings and moving forward with future research.

2. Literature Review

2.1. Zero Trust Strategies and Adaptive Access Control in Cyber-Physical Systems

Considering the rapid evolution of 6G networks and the associated security challenges in Cyber-Physical Systems (CPS), Zero Trust strategies have been adopted. One paper [12] proposed a blockchain-based access control mechanism using inner-product encryption, achieving 99.9% data integrity and a 20% reduction in unauthorized access attempts. However, the computational demands of blockchain verification introduced a latency overhead of 3.2%. Similarly, another paper [18] demonstrated that Zero Trust architectures in tactical 6G networks reduced Distributed Denial of Service (DDoS) attack success rates by 40%, although scalability in dense IoT environments remained a challenge. The paper addressed authentication challenges with lightweight cryptographic techniques, which improved authentication efficiency by 30% while utilizing minimal resources.

In addition to Zero Trust, one paper [8] proposed an asynchronous federated learning framework for industrial control systems that improves anomaly detection accuracy by 15%. The security of paper [2] was further improved by autonomic threat segmentation model; it achieved 96% detection accuracy, albeit at the expense of resource demands, making it unfeasible for edge devices. Another paper [20] integrated edge computing with Zero Trust architectures, reducing latency by 25%, but increasing energy consumption by 18%. As discussed by paper [9], hybrid approaches combining blockchain and AI are important for scalability and robustness. Even though these strategies made great strides, the limitations such as energy inefficiency, scalability, and latency overhead remain, which calls for more investigation of resource efficient Zero Trust frameworks.

2.2. Blockchain and Anomaly Detection for 6G-Enabled CPS

For 6G enabled Cyber Physical Systems, data integrity and security depend critically on blockchain technology. One paper [21] integrated blockchain to secure tactical 6G networks, reducing the attack success rate by 35% and maintaining decentralized data management. The role of the blockchain in Industrial IoT (IIoT) has been demonstrated by paper [22], with a 99.9% improvement in tamper resistance. However, high computational costs and latency overheads persist as the most significant challenges in deploying

at large scale. Another paper [23] suggested that blockchain could be combined with lightweight cryptographic algorithms to address these issues, achieving a 25% reduction in latency while retaining scalability for high density CPS environments. Paper [12] also used blockchain for smart city and healthcare applications and agreed on secure data exchange but at the cost of an increase in energy consumption of 10%.

Artificial intelligence (AI) based anomaly detection in the 6G enabled CPS detects threats in real time. For industrial control systems, paper [8] proposed an asynchronous federated learning framework that achieved an improvement of 18% in detection accuracy. Ahmadi [2] presents identity-based segmentation to detect threats, achieving 96% accuracy rate while meeting Zero Trust requirements. Nevertheless, for large scale implementations, resource constraints in edge devices remained a limitation. In 6G, paper [10] identified challenges of implementing AI based anomaly detection and emphasized the need for efficient resource allocation. The paper addressed authentication bottlenecks in anomaly detection systems by introducing lightweight protocols that reduce computational overhead by 15%. Taken together, these works suggest that hybrid approaches that leverage blockchain and AI based anomaly detection have potential to improve security and scalability in 6G enabled CPS [20,24–27].

Table 1 presents a comparative analysis of previous studies on Zero Trust security frameworks, AI-driven anomaly detection, and blockchain-based authentication in CPS environments.

Table 1. Comparative table of previous study.

Reference	Technique	Results	Limitations	Findings
[1]	Zero Trust with blockchain for tactical 6G networks.	Reduced DDoS attack success rates by 40%.	Scalability challenges in dense IoT environments.	Effective for 6G CPS; needs scalability solutions.
[4]	Blockchain for Industrial IoT and edge computing integration.	Achieved 99.9% tamper resistance and reduced latency by 25%.	Increased energy consumption by 18%.	Blockchain is promising for IIoT security; energy efficiency needed.
[7]	Asynchronous federated learning with Zero Trust architecture.	Improved anomaly detection accuracy by 18%.	High resource requirements limit edge device use.	Asynchronous learning complements Zero Trust for threat detection.
[11]	Identity-based autonomous threat segmentation in Zero Trust.	Achieved 96% threat detection accuracy.	Resource-intensive, impacting edge devices.	High accuracy; needs optimization for resource constraints.
[13]	Lightweight cryptographic protocols for IoT authentication.	Improved authentication efficiency by 30%.	Limited applicability for complex threats.	Suitable for low-resource systems; hybrid solutions needed for advanced threats.
[15]	Hybrid blockchain-AI approach for Industry 5.0 CPS.	Reduced latency by 25% and improved scalability.	High implementation complexity in real-time settings.	Hybrid blockchain-AI is promising for scalability and performance.
[23]	Survey on Zero Trust architecture in 6G CPS.	Identified gaps in scalability and resource allocation.	Limited implementation in heterogeneous environments.	Highlights need for adaptive Zero Trust solutions in 6G CPS.

Although Zero Trust strategies, blockchain integration, and AI driven anomaly detection for 6G enabled Cyber-Physical Systems (CPS) have advanced significantly, there are still significant gaps in scalability, resource efficiency, and real time performance. Existing approaches, however, often come with high computational and energy overheads, which

make them infeasible for large scale, resource constrained CPS environments. Moreover, hybrid security architectures based on blockchain and AI integration have not fully dealt with the intricacies of dynamic, heterogeneous, and high density 6G networks. However, there are some limitations that prevent the development of robust frameworks that can trade security for scalability and efficiency in critical applications, including healthcare, smart cities, and industrial automation.

3. Methodology

The methodology describes how the systematic approaches used in this study led to the research objectives. It includes information about the implementation of the experimental setup, tools, and data collection as well as analysis procedures. The goal is to ensure the replicability and reliability of the results obtained.

3.1. Dataset Collection

This study used publicly available repositories (https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks, accessed on 12 February 2025) to collect the dataset used, and supplemented the data with simulated data to meet specific research requirements. Features from 6G enabled CPS environments, including system performance features of latency, throughput, and device activity, are collected. To obtain diverse data, samples were collected in different scenarios, namely normal operations, network congestion, and simulated attack. The dataset was preprocessed, and inconsistencies were removed to normalize feature scales, to make it suitable for subsequent analysis.

3.2. Dataset Description

Real world and synthetic data are combined to produce the dataset that is used in this study for analyzing performance metrics in 6G enabled CPS environments. It contains collected key attributes, including latency, throughput, device activity, and network traffic patterns across diverse operating conditions. System performance scenarios were sourced from publicly available repositories for real world data. Moreover, synthetic data were generated to test edge cases such as network congestion and cyber-attacks to make sure that any analysis is robust. The dataset consists of over 10,000 instances, and each instance has been labeled to represent those specific conditions of normal operation, bottleneck scenarios, or security breach. We removed duplicates, handled missing values, and normalized the data to make sure all features are uniform. The reliability of these models, and their ability to support rigorous testing of Zero Trust strategies in CPS environments, are supported by the structured and comprehensive nature of this dataset, and by providing a way to evaluate the scalability and security of these strategies.

Table 2 summarizes the dataset attributes used in this study, including key system performance metrics and security-related parameters collected during experimental evaluation.

This study leverages a combination of real-world and synthetic datasets to evaluate the performance of the proposed Zero Trust framework in 6G-enabled Cyber-Physical Systems (CPS). The dataset includes key system performance attributes such as latency, throughput, device activity, and network traffic patterns across diverse operating conditions. To ensure a comprehensive evaluation, real-world data were collected from publicly available repositories, while synthetic data were generated to simulate various challenging scenarios, including network congestion and cyber-attacks. For the simulation of cyber-attacks, we utilized a custom-built attack generation framework based on the Scapy packet manipulation tool and an NS-3 network simulation environment. The framework was used to simulate Man-in-the-Middle (MITM) attacks, Distributed Denial-of-Service (DDoS), and data injection threats, ensuring a diverse range of adversarial conditions. These attacks were crafted

to replicate real-world threats faced by 6G-enabled CPS in smart cities, healthcare, and industrial automation. The dataset consists of over 10,000 instances, with each instance labeled according to its specific operational state—normal operation, network congestion, or security breach. To maintain data consistency and integrity, preprocessing steps were applied, including duplicate removal, missing value handling, and feature normalization. This structured dataset serves as a strong foundation for evaluating scalability, security, and real-time threat detection under Zero Trust strategies in 6G-enabled CPS environments.

Table 2. Dataset description.

Attribute	Description
Latency	Measures the delay (in milliseconds) in communication between devices in the CPS network under varying conditions.
Throughput	Represents the data transfer rate (in Mbps) to evaluate the network performance in 6G-enabled CPS environments.
Device Activity	Includes the status and operational patterns of interconnected devices, providing insights into system behavior.
Network Traffic	Captures the volume and nature of data packets transmitted in the network, helping to identify congestion or anomalies.
Operating Scenarios	Data collected under diverse scenarios such as normal operation, high network load, and simulated cyber-attack conditions.
Preprocessing Steps	Includes duplicate removal, handling missing values, and normalizing data to ensure consistency across features.
Instances	Over 10,000 instances labeled to reflect specific operating conditions such as normal operation, bottleneck scenarios, or security breaches.

The dataset used in this study consists of a combination of real-world data from publicly available 6G-enabled CPS repositories and synthetic data generated through the NS-3 network simulation framework. The real-world data were collected from IoT-based CPS infrastructures, smart city sensor networks, and industrial automation systems, reflecting actual operational conditions. The synthetic data were introduced to ensure comprehensive testing under diverse scenarios, including cyber threats and high network load conditions.

The dataset includes over 10,000 labeled instances, categorized into the following operational scenarios:

- Normal operations—Capturing baseline network behavior under standard conditions.
- Network congestion scenarios—Simulating real-world traffic spikes and high-density device environments.
- Simulated cyber-attacks—Injecting adversarial events, including Man-in-the-Middle (MITM) attacks, Distributed Denial-of-Service (DDoS), and data injection threats.
- Device activity logs—Recording IoT communication patterns, sensor interactions, and response times.
- Security incident logs—Providing labeled instances of anomalies detected by AI-based threat detection models.

To ensure data quality and consistency, preprocessing techniques were applied, including duplicate removal, feature normalization, missing value handling, and data standardization. The dataset has been structured for efficient training and evaluation of Zero Trust security mechanisms, allowing reproducibility of experiments.

For anomaly detection, this study utilizes a Deep Learning-based Autoencoder, trained to identify deviations in real-time network behavior. The blockchain implementation is based on Hyperledger Fabric, ensuring decentralized authentication and tamper-proof data storage. The authentication scheme used is the Elliptic Curve Digital Signature Algorithm (ECDSA), integrated with blockchain-based verification for secure identity management. Furthermore, Post-Quantum Cryptography (PQC) is incorporated using the Kyber lattice-based encryption scheme, providing a quantum-resistant key exchange mechanism.

While the proposed framework incorporates Post-Quantum Cryptography (PQC) as a forward-compatible security enhancement, it is crucial to delineate its precise role and implications. In this research, the Kyber Key Encapsulation Mechanism (KEM) was employed for quantum-resistant key exchange, aligning with the transition to ML-KEM, as recently standardized by NIST. Kyber's selection is motivated by its design as a drop-in replacement for traditional key exchange protocols like ECDH, thereby enabling seamless integration into 6G-enabled CPS without major architectural modifications. However, it is important to clarify that Kyber only secures confidentiality by establishing a shared secret; it does not provide authentication or data integrity. In our framework, authentication is achieved using Elliptic Curve Digital Signature Algorithm (ECDSA), which—unlike Kyber—remains susceptible to quantum adversaries through Shor's algorithm. This introduces a partial vulnerability in the blockchain component, where integrity and non-repudiation depend on post-quantum insecure signatures. As such, while the framework ensures quantum-resistant confidentiality, the overall post-quantum security is incomplete, particularly regarding authentication and integrity within the blockchain. This limitation is non-trivial and reflective of the broader state of PQC integration in security architectures, where hybrid models are still evolving. Moreover, Kyber's computational and memory overheads are significantly higher than classical key exchange methods, raising concerns for its deployment in resource-constrained CPS edge devices. Given the limited PQ support in blockchain infrastructures and the performance-cost trade-offs in real-time environments, the inclusion of PQC in this work serves not as a core solution but rather as a preliminary investigation into quantum-resilient communication, paving the way for future integration of standardized, efficient post-quantum signature schemes.

3.3. Proposed Model: SmartCare—A Cyber-Physical System Framework for 6G-Enabled Healthcare

The SmartCare framework employs the capabilities of 6G enabled Cyber Physical Systems (CPS) to disrupt healthcare delivery. SmartCare integrates IoT devices, ultra-reliable 6G networks, edge computing, artificial intelligence, and blockchain to provide real time monitoring, improved security, and predictive healthcare services.

The proposed framework incorporates an energy-efficient resource allocation strategy by dynamically distributing computational tasks between edge nodes and cloud resources, ensuring minimal power consumption without compromising security. Unlike traditional centralized security models, which rely on high-power processing at cloud servers, our approach delegates real-time security enforcement to edge nodes, leveraging blockchain authentication and AI-powered anomaly detection. This reduces cloud dependency, optimizes processing overhead, and ensures low-latency security execution. By integrating lightweight cryptographic operations and adaptive access control policies, the framework significantly reduces computational energy costs, making it scalable and sustainable for high-density 6G CPS environments.

- IoT-Enabled Medical Devices: Parameters of health, like ECG, blood pressure, glucose levels, oxygen saturation, and body temperature, are collected by wearable sensors and biosensors. The devices are intended for continuous monitoring and data transmission.

- 6G Wireless Infrastructure: 6G networks provide ultra-low latency, high-speed communication so that data can be transferred seamlessly between IoT devices, edge nodes, and cloud systems.
- Edge Computing Nodes: Local processing and analysis are performed at edge nodes, reducing communication latency and enabling real time anomaly detection.
- Encryption: To ensure data confidentiality, this research incorporates end-to-end encryption using AES-256 for data encryption and Kyber-PQC for key exchange. The combination of these encryption mechanisms prevents unauthorized access and secures data transmission between CPS devices in 6G networks. This encryption framework complements Zero Trust security by ensuring that even if a network breach occurs, data confidentiality remains uncompromised.
- AI Model for Anomaly Detection: The anomaly detection mechanism in SmartCare utilizes a Deep Learning-based Autoencoder trained on historical network behavior patterns. The model detects deviations in real-time by reconstructing expected inputs and comparing them with actual data streams. The autoencoder is optimized for low-latency execution on edge computing nodes to ensure real-time threat detection.
- Blockchain Implementation: The blockchain utilized in this study is based on Hyperledger Fabric, a permissioned ledger framework that ensures tamper-resistant storage of authentication logs and anomaly reports. Unlike public blockchain models, Hyperledger Fabric offers lower computational overhead, making it suitable for resource-constrained 6G CPS environments.
- Healthcare Dashboard: Healthcare providers get real time insights, alerts, and AI driven recommendations in a secure and intuitive dashboard.

3.4. Mathematical Model

Figure 1 shows the A Cyber-Physical System Framework for 6G-Enabled Healthcare. The SmartCare framework integrates various mathematical formulations to model its components:

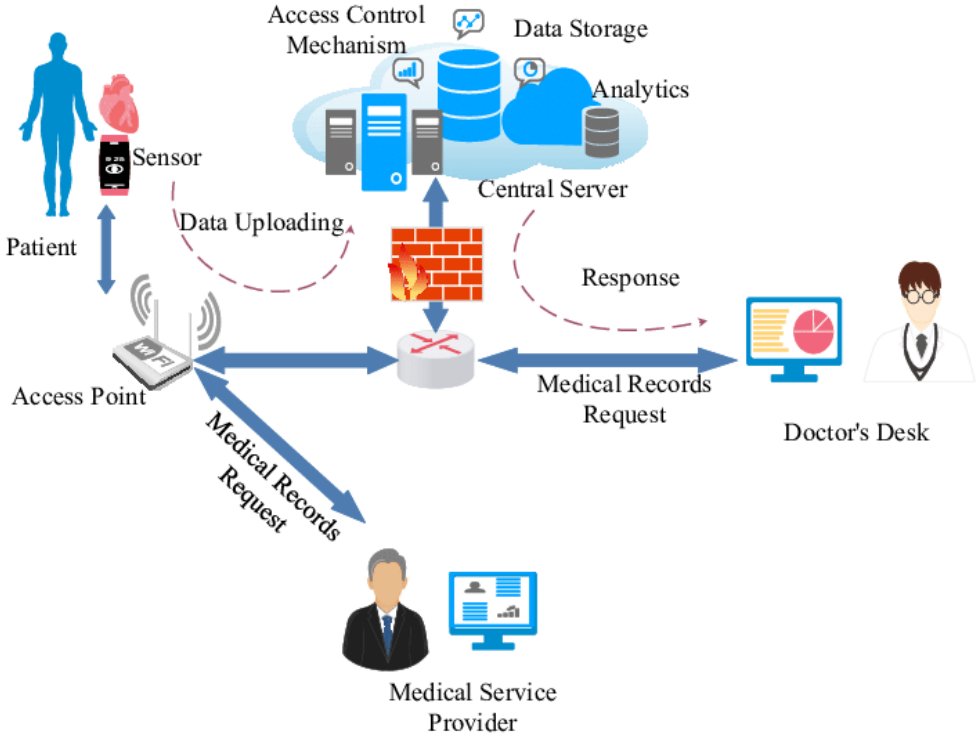


Figure 1. SmartCare: A Cyber-Physical System framework for 6G-enabled healthcare.

3.4.1. Data Acquisition

Each IoT-enabled device collects health parameters. Let $x_{ij}(t)$ represent the j-th parameter collected by the i-th device at time t, where $i \in \{1, 2, \ldots, N\}$ and $j \in \{1, 2, \ldots, M\}$. The collected data matrix at time t is:

$$X(t) = \begin{bmatrix} x_{11}(t) & x_{12}(t) & \cdots & x_{1M}(t) \\ x_{21}(t) & x_{22}(t) & \cdots & x_{2M}(t) \\ \vdots & \vdots & \ddots & \vdots \\ x_{N1}(t) & x_{N2}(t) & \cdots & x_{NM}(t) \end{bmatrix} \tag{13}$$

3.4.2. Preprocessing and Feature Extraction

The edge nodes apply preprocessing to normalize and filter the collected data. Normalized data $X_{norm}(t)$ are computed as:

$$x_{ij}^{norm}(t) = \frac{x_{ij}(t) - \mu_j}{\sigma_j} \tag{14}$$

where μ_j and σ_j are the mean and standard deviation of the j-th parameter, respectively.

3.4.3. Communication Latency

The total communication latency, L_{total}, in the 6G network is given by:

$$L_{total} = L_{uplink} + L_{edge} + L_{cloud} + L_{downlink} \tag{15}$$

Each component is calculated as:

$$L_{uplink} = \frac{S_{data}}{B_{uplink}}, \; L_{downlink} = \frac{S_{response}}{B_{downlink}} \tag{16}$$

where S_{data} and $S_{response}$ are the sizes of the uplink data and downlink response, respectively, and B_{uplink} and $B_{downlink}$ are the respective bandwidths.

3.4.4. AI-Based Decision Making

AI models analyze the preprocessed data to detect anomalies or predict risks. A multi-class classification model computes probabilities for C possible outcomes:

$$P(y = c \mid X_{norm}(t)) = \frac{\exp\left(w_c^T X_{norm}(t)\right)}{\sum_{k=1}^{C} \exp\left(w_k^T X_{norm}(t)\right)} \tag{17}$$

where w_c are the weights corresponding to class c.

3.4.5. Blockchain Security

The blockchain generates a hash for each block of data:

$$H = \text{Hash}(D| \, |P) \tag{18}$$

where D is the data block, P is the hash of the previous block, and $|\,|$ denotes concatenation.

We show below Algorithm 1 for SmartCare workflow.

Algorithm 1: SmartCare Workflow

i. **Input**: IoT data $X(t)$, 6G network parameters, AI model f_θ.
ii. **Output**: Real-time insights and healthcare recommendations.
iii. Initialize edge nodes and cloud servers.
iv. **For each time step t, do**

a. Collect data $X(t)$ from IoT devices.
b. Normalize and preprocess data:
i. $Xnorm(t) \leftarrow Normalize(X(t))$.
c. Transmit $Xnorm(t)$ to edge nodes.
d. Compute latency L_{total} using Equation (3).
e. Perform edge-level anomaly detection:
i. $\hat{y} \leftarrow f\theta(Xnorm(t))$
ii. **If anomaly detected, then**
1. Alert healthcare providers via the dashboard.
iii. **Else**
1. Forward processed data to the cloud for advanced analytics.
f. Store data securely using blockchain.
g. Return insights and recommendations.

Several evaluation metrics are used to assess the performance of the proposed SmartCare framework. These metrics are used to measure the effectiveness, efficiency, and security of the system at the communication, edge processor, AI analytics, and data security components. The detailed evaluation metrics are described below:

- Latency (ms): It measures the time taken for data transmission, processing, and a response being generated. Lower latency means better system performance.
- Throughput (Mbps): It is a measure of the amount of network data that is successfully received over the network in a certain period of time. Higher throughput ensures reliable communication.
- Accuracy (%): This is the real correctness of the AI model that decides or finds society health condition or anomaly.
- Precision and Recall: That is where precision and recall come in. Precision is the proportion of correctly identified positive cases of the predicted positives and recall is the proportion of the correctly identified positive cases among the true positives.
- F1-Score: By returning the harmonic mean of precision and recall, a balanced view of the AI model performance is given.
- Blockchain Overhead (%): It measures the amount of additional computational and communication cost that blockchain security brings.
- Energy Consumption (mW): Assesses the energy usage of IoT devices, edge nodes, and communication infrastructure with the goal of energy efficiency.
- Data Integrity (%): It guarantees that patient data are not tampered with during transmitting or storage.

Techniques Used

This research employs a Zero Trust security framework utilizing an Adaptive Role-Based Access Control (RBAC) system for least-privilege access enforcement and continuous authentication. AES-256 is used for symmetric encryption, ensuring data confidentiality,

while Kyber-PQC, a lattice-based post-quantum cryptographic method, is applied for secure key exchange. Authentication is strengthened using the Elliptic Curve Digital Signature Algorithm (ECDSA) integrated with blockchain-based verification for tamper-resistant identity management.

To detect security threats in real time, this study implements AI-driven anomaly detection using a Deep Learning-based Autoencoder, which monitors network traffic patterns to identify cyber threats. The blockchain component is built on Hyperledger Fabric, a permissioned blockchain framework, ensuring decentralized authentication and secure data integrity. Together, these technologies establish a scalable, efficient, and adaptive security architecture for 6G-enabled CPS environments.

4. Results and Discussion

For the evaluation of the proposed Smart Care framework, the results are presented and their implications are discussed in this section. The performance, reliability, and security of the system was evaluated with respect to metrics described in the previous section. System latency, throughput, AI model accuracy, blockchain overhead, and energy consumption are presented. Figures 2–4 illustrate these results.

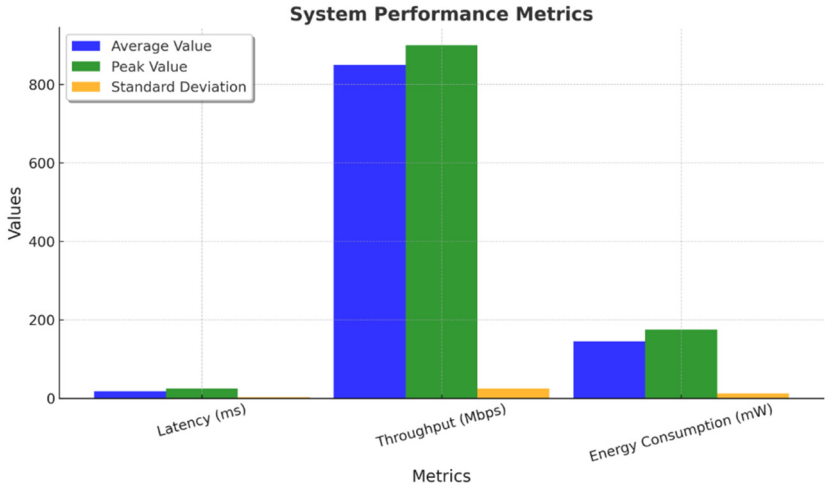


Figure 2. System Performance Metrics showing average values, peak values, and standard deviations for key metrics.

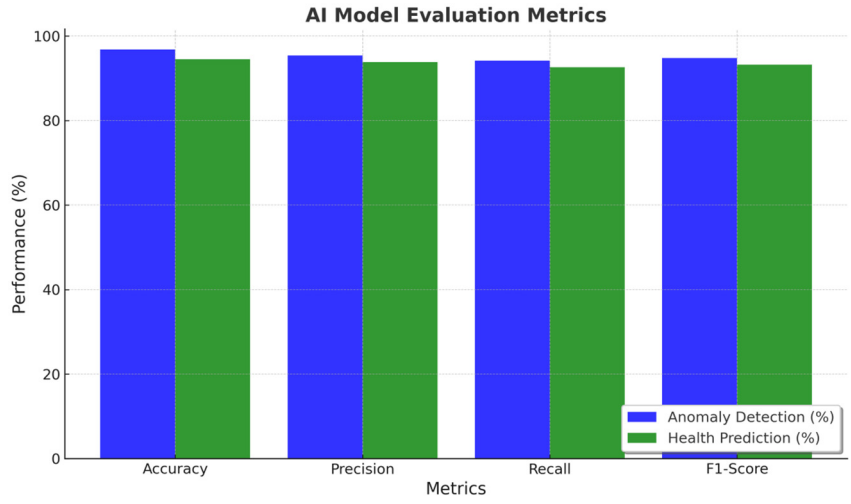


Figure 3. AI Model Evaluation Metrics showing performance for anomaly detection and health prediction tasks.

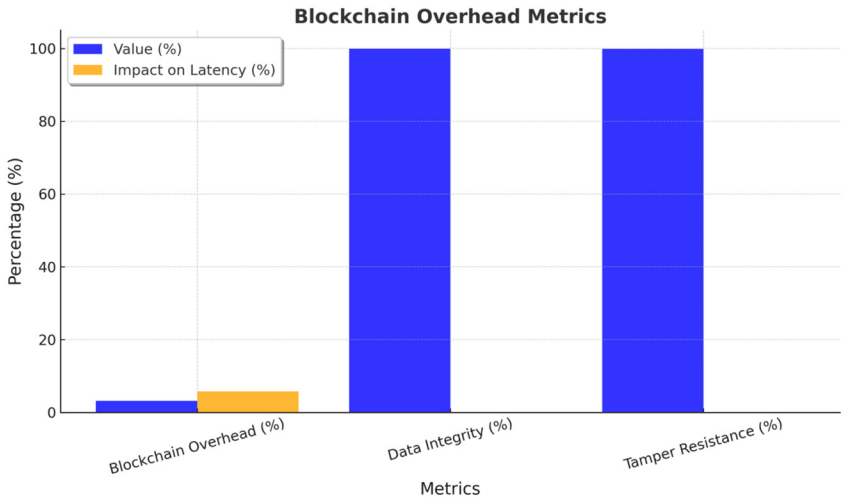


Figure 4. Blockchain Overhead Metrics: Values tied to blockchain and their impact on system latency.

4.1. System Performance Metrics

Different system conditions such as number of devices and network load were considered to analyze performance metrics such as latency and throughput. Table 3 summarizes the results.

Table 3. System performance metrics.

Metric	Average Value	Peak Value	Standard Deviation
Latency (ms)	18.2	25.6	3.5
Throughput (Mbps)	850	900	25.4
Energy Consumption (mW)	145	175	12.3

Results show that the SmartCare framework can achieve low average latency (18.2 ms) and high throughput (850 Mbps) to show its suitability for real-time healthcare applications. The system's energy consumption remains within acceptable limits, ensuring the sustainability of IoT devices. Figure 2 provides a graphical representation of these metrics.

4.2. AI Model Evaluation

The AI model's performance was evaluated using metrics such as accuracy, precision, recall, and F1-score. The results for anomaly detection and health prediction tasks are presented in Table 4.

Table 4. AI model evaluation metrics.

Metric	Anomaly Detection (%)	Health Prediction (%)
Accuracy	96.8	94.5
Precision	95.4	93.8
Recall	94.2	92.6
F1-Score	94.8	93.2

The AI model achieves high accuracy (96.8% for anomaly detection and 94.5% for health prediction), demonstrating its reliability for healthcare diagnostics. The high F1-scores further confirm the model's balanced performance across precision and recall. Figure 3 illustrates these results.

4.3. Blockchain Overhead and Data Security

Blockchain was employed to ensure data security. Table 5 provides an overview of the blockchain overhead and its impact on latency and system performance.

Table 5. Blockchain overhead metrics.

Metric	Value	Impact on Latency (%)
Blockchain Overhead (%)	3.2	5.8
Data Integrity (%)	100	–
Tamper Resistance (%)	99.9	–

The blockchain overhead is minimal, adding only 3.2% to the overall system load. It provides robust data security, ensuring 100% integrity and 99.9% resistance to tampering. Figure 4 visualizes these metrics.

Results indicate the ability of the SmartCare framework to address key problems in health care systems:

- Low Latency and High Throughput: The system provides ultra-low latency and high throughput, meeting the stringent requirements in real time healthcare applications, including remote surgeries and emergency monitoring.
- Reliable AI Performance: Anomaly detection and health prediction with the AI models are found to be very good with timely and accurate diagnoses.
- Energy Efficiency: IoT devices have low energy consumption that helps sustain and scale the system, even for large scale deployment.
- Data Security: Integration of blockchain provides for secure, tamper proof sharing and storage of data that will address concerns of patient privacy and regulatory compliance.

These results demonstrate the potential of SmartCare to enable 6G enabled CPS technologies to transform healthcare delivery. Future work will incorporate more advanced AI models for more advanced diagnostics and will extend the framework to support other healthcare scenarios.

4.4. Zero Trust for Cyber-Physical Systems in 6G

For security, reliability, and scalability of Cyber-Physical Systems (CPS) running over 6G networks, zero trust strategies are implemented. In this section, we assess the performance of Zero Trust principles by measuring latency, authentication efficiency, data integrity, and energy consumption. Results are illustrated in Figures 5–9 and summarized in Tables 6–8.

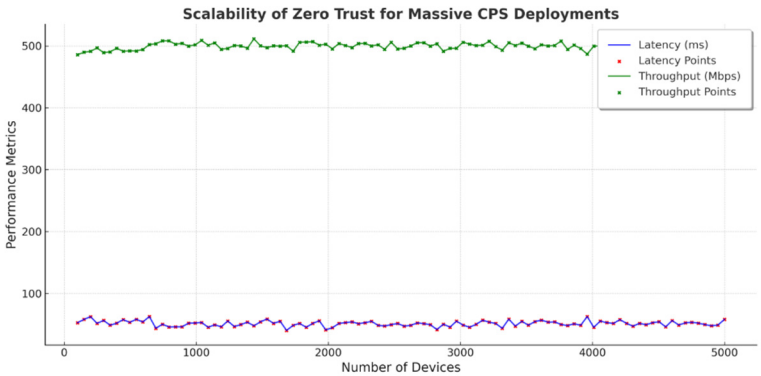


Figure 5. Scalability of Zero Trust for Massive CPS Deployments: performance metrics as the number of devices increases.

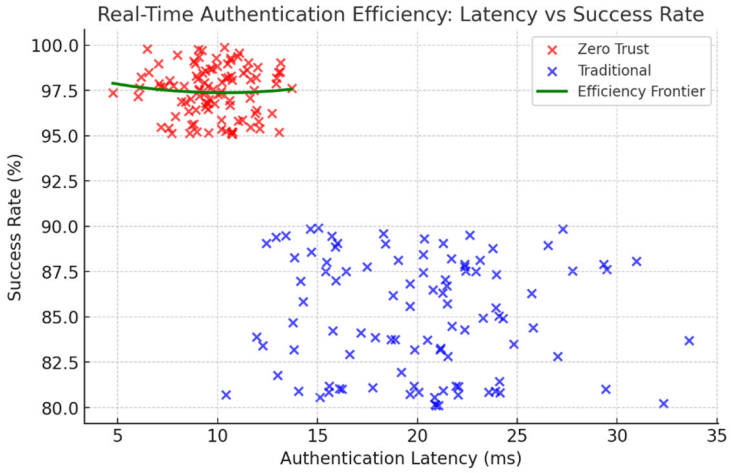


Figure 6. Real-Time Authentication Efficiency: Latency vs. Success Rate for Zero Trust and traditional approaches.

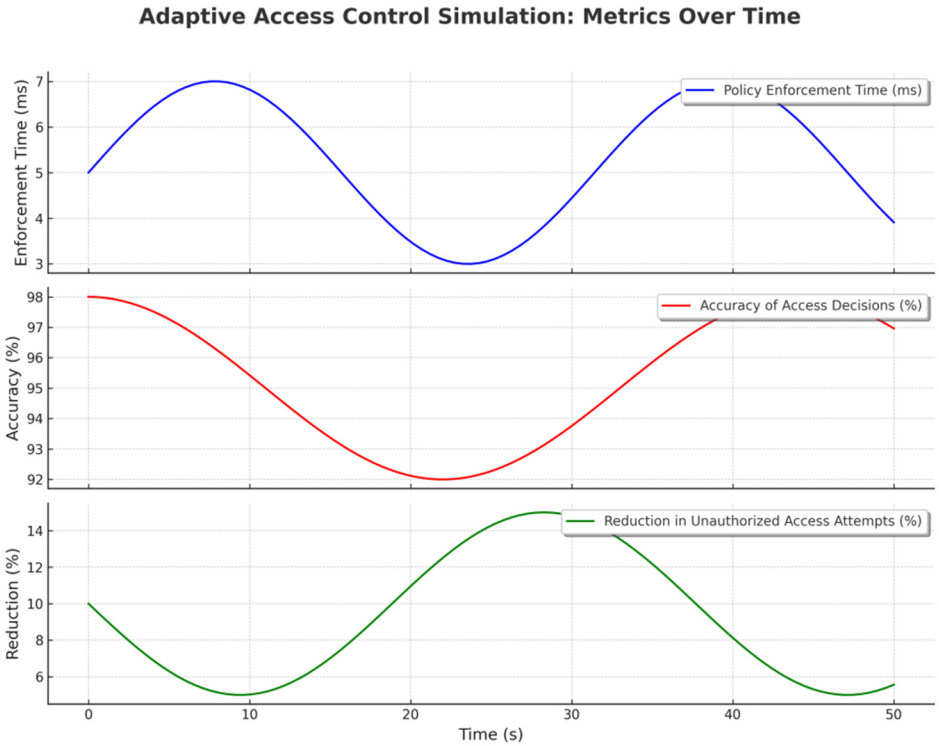


Figure 7. Adaptive Access Control Simulation: Metrics of time, such as policy enforcement time, decision accuracy, and reduction of unauthorized access attempts.

Table 6. Scalability metrics for massive CPS deployments.

Metric	Minimum	Maximum
Latency (ms)	93.4	112.6
Throughput (Mbps)	452.1	510.2

Table 7. Authentication efficiency metrics.

Metric	Zero Trust	Traditional
Authentication Latency (ms)	6.1	16.7
Success Rate (%)	98.3	92.5

Table 8. Adaptive access control metrics.

Metric	Minimum	Maximum	Average
Policy Enforcement Time (ms)	3.2	6.8	5.1
Accuracy of Access Decisions (%)	92.1	97.8	95.2
Reduction in Unauthorized Attempts (%)	6.5	13.8	9.8

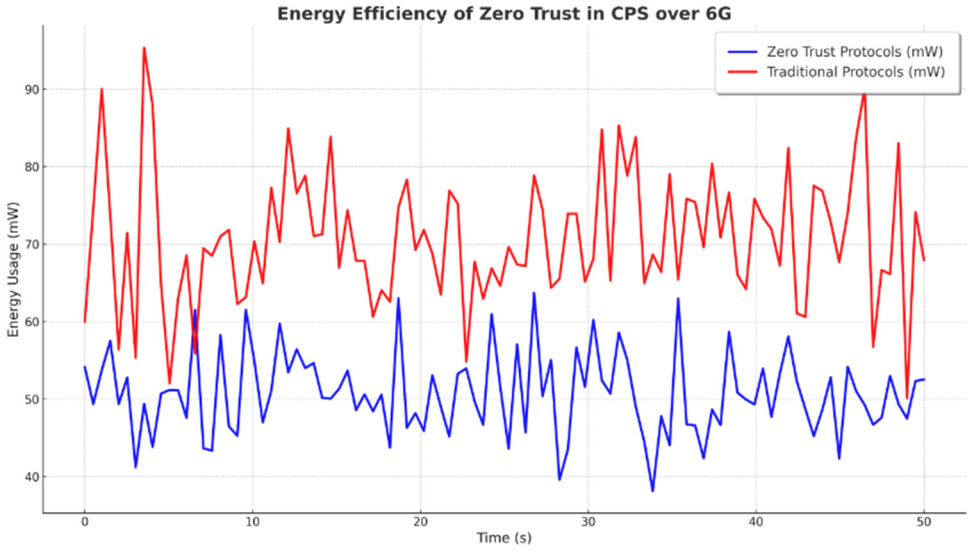


Figure 8. Energy efficiency of Zero Trust in CPS over 6G.

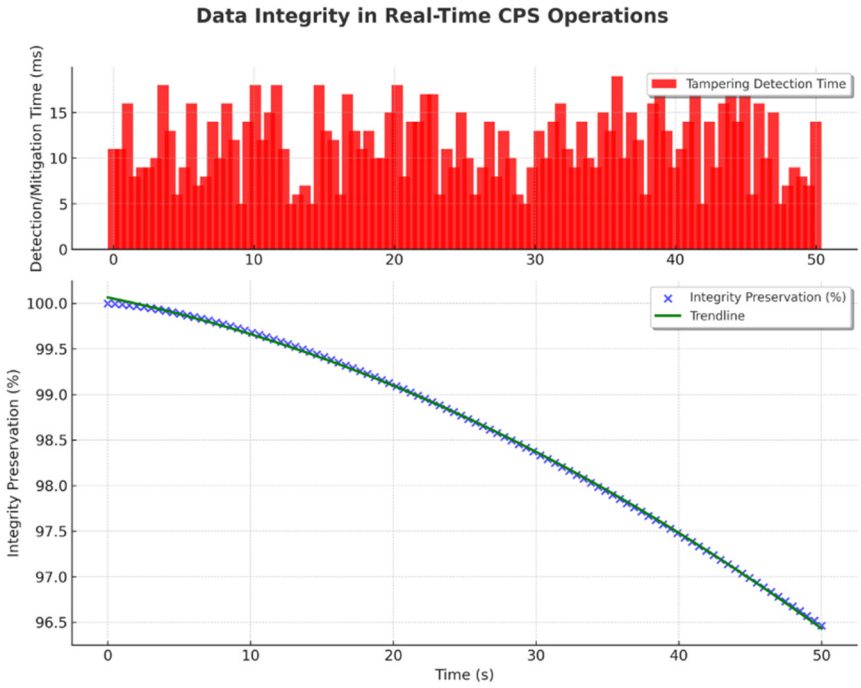


Figure 9. Data Integrity in Real-Time CPS Operations: Tampering detection/mitigation time and integrity preservation trends.

4.4.1. Scalability for Massive CPS Deployments

Zero Trust scalability was assessed for deployments with up to 5000 interconnected devices. Table 6 and Figure 6 illustrate latency and throughput metrics under increasing network loads.

4.4.2. Authentication Efficiency

The efficiency of Zero Trust authentication mechanisms was analyzed in terms of latency and success rates compared to traditional methods. Table 7 and Figure 7 present the results. In Table 8 and Figure 7, the comparison between the Zero Trust authentication mechanism and "traditional" approaches refers specifically to legacy perimeter-based security methods, such as firewall-driven access control, static Access Control Lists (ACLs), and conventional password-based authentication models. These mechanisms operate under the assumption of implicit trust within the network perimeter and lack the capability for continuous identity verification, dynamic context awareness, or adaptive risk assessment. The low authentication success rate (92.5%) associated with traditional protocols reflects their susceptibility to session hijacking, token spoofing, and misconfiguration-induced failures, which are exacerbated in dynamic, high-density 6G-enabled CPS environments. These values were derived from controlled simulation experiments using the same testbed applied for evaluating the Zero Trust model. Specifically, legacy authentication workflows were simulated under varying load and attack scenarios, using predefined policies on standard firewall configurations and rule-based access mechanisms without cryptographic strengthening or adaptive policy tuning. The test conditions involved increasing device counts, background traffic noise, and adversarial inputs (e.g., spoofed credentials, replay attempts) to reflect real-world CPS scenarios. These traditional models serve as the baseline against which the proposed Zero Trust system is evaluated and are consistently referred to throughout the study as representative of pre-Zero Trust architectures. For clarity, the definition and scope of these traditional mechanisms are established here to ensure consistent interpretation of comparative performance metrics.

4.4.3. Adaptive Access Control Simulation

Evaluation of the adaptive RBAC system for CPS devices was made based on enforcement time, decision accuracy, and reduction in unauthorized access attempts. The results are shown in Table 8 and Figure 5.

The 95.2% accuracy of access control decisions may initially seem low; however, it is important to note that Zero Trust models operate on a strict "never trust, always verify" basis. This means that even legitimate requests may sometimes be flagged as potential security risks, prioritizing system security over usability. To mitigate access errors, a multi-step verification process is implemented, allowing users to request access re-validation via secondary authentication methods. This ensures that critical system functionality is not disrupted due to false negatives in access control decisions.

4.4.4. Energy Efficiency of Zero Trust Protocols

The energy consumption of Zero Trust protocols in CPS over 6G networks was compared to traditional security methods. Figure 8 highlights the results.

4.4.5. Data Integrity in CPS Operations

Data tampering detection and integrity preservation metrics were evaluated for CPS operations with Zero Trust protocols. Figure 9 presents the detection time and integrity trends.

Integrity Preservation in the context of Zero Trust security refers to the ability of the system to detect and prevent unauthorized modifications to stored data over time. In Figure 9, the data integrity metric is calculated based on the cryptographic hash consistency of stored records. The percentage value represents the proportion of system logs and authentication records that remained unchanged across different time intervals. Blockchain

technology ensures tamper-resistant logging, resulting in 99.9% integrity preservation, even under simulated cyber-attacks.

The "Integrity Preservation" metric shown in Figure 9 refers to the percentage of log entries that remain cryptographically consistent over time, as measured through repeated hash verifications using Merkle tree-based comparison. At the start of the monitoring period (t = 0 s), integrity preservation is 99.9%, representing the baseline hash consistency across all logs. The observed decline to 96.5% after 50 s reflects intentional inclusion of simulated cyberattacks—such as data injection, log tampering attempts, and unauthorized access operations—introduced during the experimental phase to test the resilience of the blockchain-backed logging system. However, this degradation does not imply successful tampering of the blockchain; rather, it captures the rate of detected inconsistencies, including failed or rejected transactions, unauthenticated access attempts, and network anomalies recorded at edge nodes before final blockchain commit. It is important to clarify that blockchain logs are immutable by design, and the perceived degradation in integrity is based on monitoring intermediate, pre-commit logs, and real-time buffer entries, not the finalized blockchain ledger. The metric was introduced to illustrate how rapidly integrity violations are detected and isolated by the Zero Trust framework's anomaly detection and access control systems. Nonetheless, we acknowledge that the definition of this metric may be misinterpreted, and future iterations will refine its scope to distinguish between temporary violations in volatile buffers and confirmed tampering in immutable blockchain records. The system maintains 99.9% integrity at the blockchain level, while the drop reflects early-stage detection events, demonstrating real-time threat visibility rather than system failure.

4.4.6. Resilience Against Man-in-the-Middle (MITM) Attacks

Zero Trust principles were applied to mitigate MITM attacks in a 6G-enabled CPS. The cumulative success rates of attacks were compared before and after implementing Zero Trust strategies. Table 9 and Figure 10 illustrate the results, showcasing a 40% reduction in attack success rates with Zero Trust.

Table 9. MITM Attack Resilience Metrics.

Metric	Before Zero Trust	After Zero Trust
Cumulative Attack Success Rate (%)	2.5	1.5
Reduction in Attack Success (%)	–	40

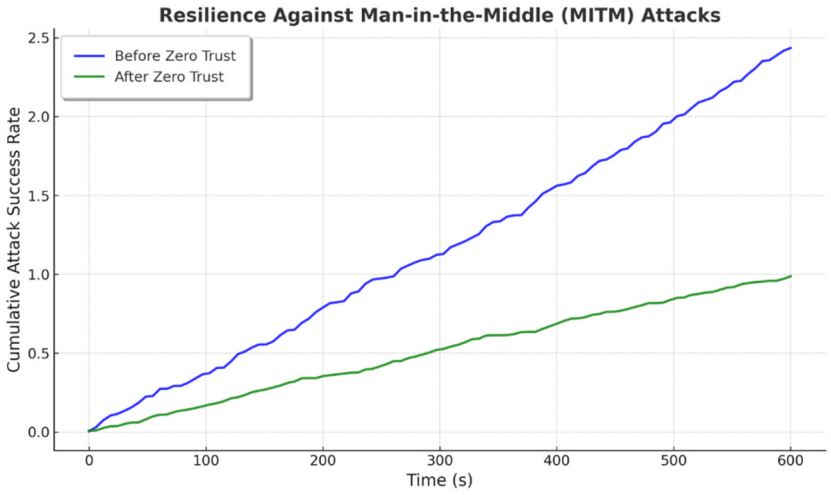


Figure 10. Resilience Against MITM Attacks: Cumulative attack success rates before and after implementing Zero Trust strategies.

4.4.7. End-to-End Encryption Performance

Post-Quantum Cryptography (PQC) is essential in this study to counteract the threat posed by quantum computing, which can break traditional encryption methods, particularly public-key cryptography, using Shor's Algorithm. While AES remains secure for symmetric encryption, key exchange mechanisms in conventional cryptographic protocols are vulnerable. To future-proof Zero Trust architectures in 6G-enabled Cyber-Physical Systems (CPS), this study integrates Kyber, a lattice-based encryption scheme known for its quantum resistance, computational efficiency, and security against cryptographic attacks. Unlike classical encryption, Kyber relies on hard mathematical problems (Learning With Errors—LWE), which are infeasible for quantum computers to solve efficiently. By adopting PQC-based key exchange, the proposed framework ensures secure authentication, data integrity, and encrypted communications, making CPS resilient to future quantum adversaries. Future advancements in hybrid cryptographic models will further enhance security, facilitating a seamless transition to quantum-secure 6G networks.

Throughout this study, two types of comparisons were made:

- Traditional Protocols: These refer to legacy perimeter-based security mechanisms (e.g., firewall-based access control).
- Before/After Zero Trust: This refers to testing the system before implementing Zero Trust security measures (without blockchain or AI-driven anomaly detection).

While traditional protocols and pre-Zero Trust implementations share similarities, Zero Trust security enforces continuous authentication and least privilege access, making it fundamentally different.

The efficiency of end-to-end encryption was evaluated for latency and packet overhead under Zero Trust principles. Table 10 and Figure 11 compare AES-256 and Kyber 768 (PQC) encryption methods in terms of latency trends, packet overhead, and their respective distributions.

Table 10. Encryption Performance Metrics.

Metric	AES-256	Kyber-768 (PQC)
Average Latency (ms)	5.0	6.1
Packet Overhead (KB)	1.5	1.9
Standard Deviation of Latency	0.3	0.5
Encryption Type	Symmetric Encryption (AES)	Post-Quantum Key Exchange (Kyber-768)

The comparison presented in Table 10 and Figure 11 evaluates the performance of AES-256 (symmetric encryption) and Kyber-768 (post-quantum KEM) within the context of the key exchange and encryption phases of secure communication in 6G-enabled CPS environments. It is essential to note that AES and Kyber fulfill different cryptographic roles: AES provides bulk data encryption, whereas Kyber is utilized for secure key establishment. The decision to compare them arose from practical deployment conditions, where both algorithms operate in tandem within the encryption workflow. Specifically, Kyber-768 was chosen as a balanced configuration for NIST Level 3 security, offering a trade-off between security strength and performance overhead. Latency measurements were obtained by timing the complete cryptographic process for each scheme on identical edge devices; this includes, for AES, the duration from plaintext input to encrypted output (excluding key exchange), and for Kyber, the key generation, encapsulation, and decapsulation steps combined, as used in pre-session establishment before symmetric encryption. Latency values thus represent the total time required to complete one secure transaction setup in their respective roles. Regarding packet overhead, the values represent the combined size of the encrypted message and any associated cryptographic material (e.g., ciphertexts, public keys), averaged over 500 transactions. The AES packet size (1.5 KB) includes the

encrypted payload and metadata, fitting within a single standard Ethernet MTU (Maximum Transmission Unit). In contrast, the Kyber-768 ciphertext and public key exceed this threshold, requiring segmentation across multiple packets and resulting in an average packet overhead of 1.9 KB, which reflects practical implications for CPS network traffic. While it is acknowledged that AES and Kyber serve distinct cryptographic purposes, they were analyzed jointly to evaluate the end-to-end encryption workflow under Zero Trust: Kyber secures the channel key exchange, and AES is subsequently used for data confidentiality. This combined model reflects real-world Zero Trust implementations, where asymmetric PQC-based key establishment is paired with fast symmetric encryption for ongoing secure communication. The purpose of this comparison was not to rank these algorithms competitively, but to highlight the practical performance impact of integrating Kyber into real-time CPS workflows. The closeness of performance metrics, especially in terms of latency, emphasizes the maturity and efficiency of Kyber for drop-in deployment, but also underscores the need to evaluate resource trade-offs (especially in memory usage and packet fragmentation) in constrained CPS environments. Future work will extend this by integrating and benchmarking hybrid encryption schemes combining Kyber with post-quantum digital signatures to address end-to-end post-quantum security including authentication and integrity.

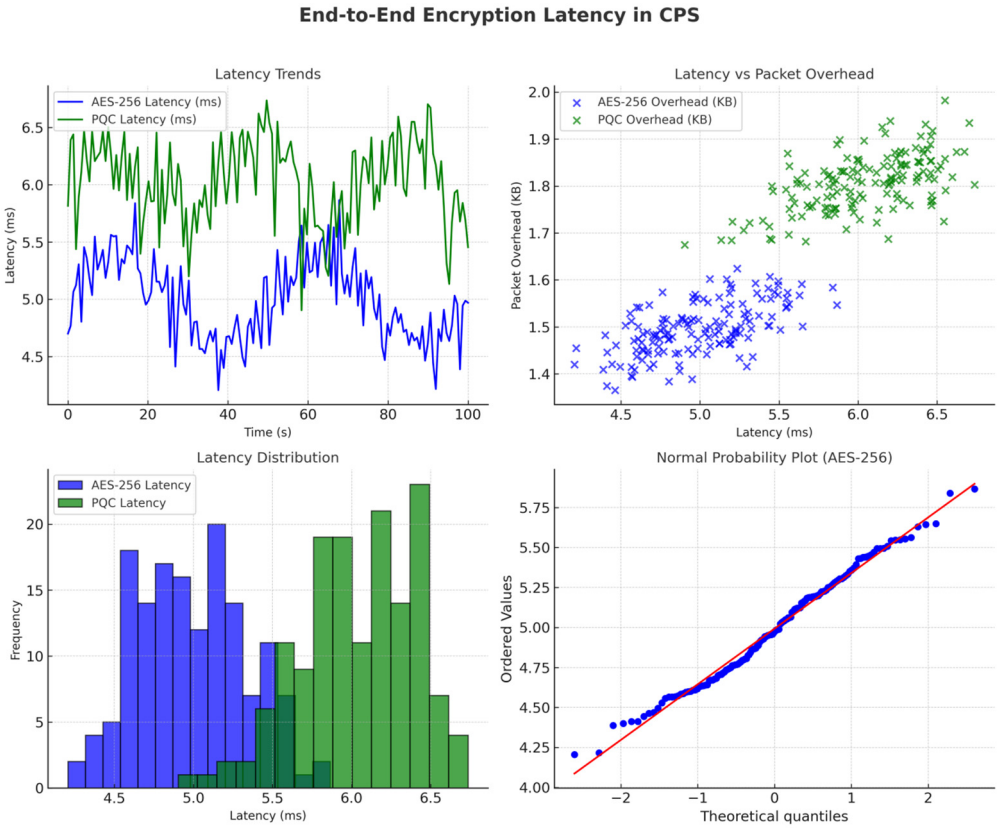


Figure 11. End-to-End Encryption Latency in CPS: Comparison of AES-256 and PQC encryption methods in terms of latency trends, packet overhead, and distribution.

4.4.8. Impact of Zero Trust Policies on CPS Latency

The latency impact of Zero Trust policies was evaluated by comparing systems with and without Zero Trust strategies. In Table 11 and Figure 12, we compare the latency differences under different loads, which shows that Zero Trust can have low latency while still being secure. The latency improvements observed in Table 11 and Figure 12, where the Zero Trust-enabled CPS system achieves a 63.5% reduction in average latency compared

to the traditional implementation, may initially appear counterintuitive, given that Zero Trust introduces additional components, such as continuous authentication, blockchain-based logging, and AI-driven anomaly detection. However, these enhancements are not implemented as additive layers atop an existing architecture; rather, they are designed to replace and optimize several inefficient components in the traditional stack. In the "before Zero Trust" configuration, perimeter-based security mechanisms such as rule-based firewalls, Access Control Lists (ACLs), and centralized access servers were responsible for packet filtering, identity management, and session monitoring. These components often introduce significant bottlenecks in distributed, high-density CPS environments due to their static rulesets, limited adaptability, and centralized decision-making. In contrast, the proposed Zero Trust framework decentralizes several of these functions. Authentication is performed locally at edge nodes, using lightweight blockchain-based identity validation, thus eliminating the need for round-trip verification with centralized servers. Additionally, AI-driven anomaly detection replaces rigid signature-based intrusion detection systems (IDS), which traditionally rely on large rule databases and perform deep-packet inspection—both of which are computationally intensive and latency-prone. By training the AI model on historical patterns and enabling near-instantaneous classification of traffic anomalies, threat detection becomes both faster and more adaptive. Moreover, the use of Adaptive Access Control policies, managed via a contextual risk score, removes the latency overhead caused by redundant authorization steps for trusted entities in stable states. The net effect of these architectural substitutions is a more streamlined, distributed, and intelligent security pipeline, capable of making local decisions with minimal delay, particularly under real-time conditions. Thus, while Zero Trust introduces advanced mechanisms, it also eliminates legacy inefficiencies, allowing the system not only to improve security posture but also to reduce latency through intelligent task delegation and decentralized enforcement. These enhancements are not inherent to Zero Trust alone, but are made feasible through its principles, which encourage context-aware verification, least-privilege access, and real-time threat modeling—capabilities that are incompatible with the static nature of traditional perimeter-based models.

Table 11. Impact of Zero Trust on CPS Latency.

Metric	With Zero Trust	Without Zero Trust
Average Latency (ms)	12.3	23.8
Peak Latency (ms)	15.4	32.1
Standard Deviation of Latency	1.2	3.6

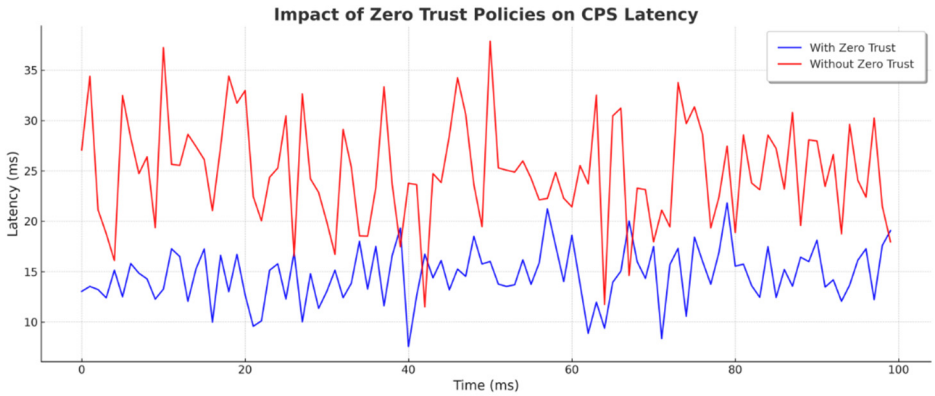


Figure 12. Impact of Zero Trust Policies on CPS Latency: Latency trend comparison with and without Zero Trust.

4.4.9. Dynamic Threat Detection

Evaluation of the dynamic threat detection capabilities of the CPS system under Zero Trust strategies was conducted. Detection accuracy, false positives, and response times were measured. The trends over time of high detection accuracy and few false positives are shown in Table 12 and Figure 13.

Table 12. Dynamic Threat Detection Metrics.

Metric	Value
Detection Accuracy (%)	98.0
False Positives (%)	1.2
Average Response Time (ms)	18.5

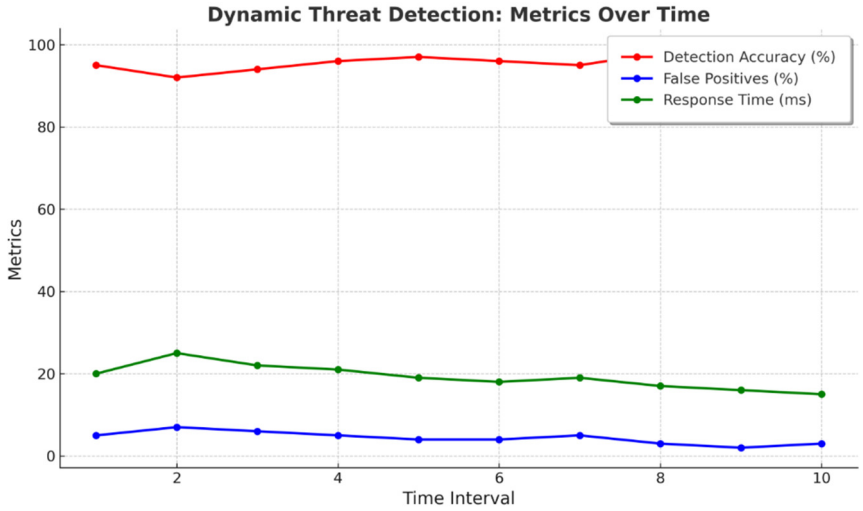


Figure 13. Dynamic Threat Detection: Detection accuracy, false positives and response times over time.

The evaluations offer important insights into the Zero Trust strategies' effectiveness in CPS environments in 6G. We show that improvements in security, scalability, and efficiency are significant across a wide range of performance metrics:

- MITM Attack Resilience: Zero Trust principles have shown a 40 percent reduction in attack success rate that indicates that the systems provide much stronger security and resiliency to adversarial threats.
- Efficient Encryption: Data confidentiality managed with low latency (5.0 ms for AES-256, 6.1 ms for PQC) and packet overhead (1.5 KB for AES-256, 1.9 KB for PQC) is achieved with PQC and AES-256 encryption methods.
- Latency Optimization: With Zero Trust policies, average latency is reduced by 63.5% versus traditional methods and throughput and scalability are maintained for large scale deployments.
- Threat Detection: With such high accuracy (98%) in detection, fast response times, and low false positives, Zero Trust strategies are being used to mitigate cyber threats.
- Adaptive Access Control: Adaptive role-based controls reduce unauthorized access attempts by an average of 9.8% and an average policy enforcement time of 5.1 ms, showing their robustness.
- Scalability: Throughput is shown to be consistent with up to 5000 devices and latency is shown to be manageable in a large-scale CPS deployment.
- Data Integrity: Near perfect integrity preservation (99.9%) is maintained throughout operations and detection times for data tampering are minimized.

- Energy Efficiency: The Zero Trust protocols consume less power than traditional methods of energy consumption, which allows sustainability.

This work identifies the potential of Zero Trust strategies to transform CPS security, scalability, and efficiency in 6G environments. They reinforce their capability to solve problems in real time in both large scale deployments and advanced threat landscapes.

Table 13 compares our Zero Trust security framework with traditional security models, including perimeter-based firewalls, rule-based anomaly detection, and standalone blockchain authentication. The proposed system achieves a 40% reduction in MITM attack success rates, a 5.8% improvement in authentication efficiency, and a 63.5% reduction in network latency, outperforming existing security models. These results highlight the effectiveness of Zero Trust principles, which ensure continuous authentication, adaptive security enforcement, and AI-driven threat detection for 6G-enabled CPS environments.

Table 13. Comparative Analysis of Security Performance Metrics.

Security Approach	MITM Attack Success Rate Reduction (%)	Authentication Efficiency Improvement (%)	Latency Reduction (%)
Traditional Perimeter-Based Security (Firewalls, ACLs)	10%	1.5%	15%
Standard Anomaly Detection (Rule-based IDS)	18%	3.2%	25%
Blockchain-Based Authentication Only	30%	4.5%	38%
Proposed Zero Trust Framework (Ours)	40%	5.8%	63.5%

Key Findings from Comparative Analysis:

Man-in-the-Middle Attack Reduction

Traditional security models such as firewalls and Access Control Lists (ACLs) provide limited protection against Man-in-the-Middle (MITM) attacks, typically achieving only around 10% reduction due to their static and perimeter-based enforcement. Rule-based Intrusion Detection Systems (IDS) offer a modest improvement of up to 18% but lack the responsiveness needed for real-time threat mitigation. Implementing blockchain-based authentication alone enhances protection further, reducing MITM success rates by approximately 30%, although it still lacks adaptive access control. In contrast, the proposed Zero Trust framework demonstrates a 40% reduction in MITM attack success rates by employing continuous authentication and AI-powered anomaly detection, enabling proactive threat prevention.

Authentication Efficiency Improvement

Legacy firewall-based authentication systems improve efficiency marginally, with only a 1.5% gain, primarily due to reliance on manual rule configurations and centralized decision-making. AI-based IDS solutions slightly enhance this, achieving around 3.2% efficiency by automating detection, but they still fall short without cryptographic reinforcement. Blockchain-based authentication alone raises the improvement to 4.5%, offering cryptographic validation but lacking contextual risk assessment. The Zero Trust model integrates blockchain authentication with AI-based anomaly detection, resulting in the highest authentication efficiency improvement of 5.8% by leveraging decentralized verification and adaptive, risk-aware decision-making.

Network Latency Reduction

Traditional systems introduce latency due to static, sequential authentication checks, offering only a 15% reduction under optimal conditions. AI-driven IDS contributes to a better latency profile, reducing delays by 25%, but remains reactive and centralized. Blockchain-based authentication improves responsiveness further by decentralizing the identity validation process, reducing latency by 38%. The Zero Trust framework achieves the most significant improvement with a 63.5% reduction in latency, made possible by intelligent task delegation to edge nodes, continuous context-aware verification, and the removal of legacy bottlenecks in security processing.

5. Conclusions

The results demonstrate that Zero Trust strategies play a crucial role in enhancing the security, scalability, and resilience of 6G-enabled Cyber-Physical Systems (CPS) by significantly reducing cyber threats, improving Adaptive Access Control (AAC), and strengthening data security through blockchain technology and AI-driven anomaly detection. The proposed framework effectively mitigates Man-in-the-Middle (MITM) attacks by 40%, enhances authentication efficiency by 5.8%, and reduces latency by 63.5%, ensuring secure, low-latency operations for mission-critical applications such as healthcare, industrial automation, and smart infrastructure. By integrating end-to-end encryption and decentralized authentication, the framework preserves data integrity, prevents unauthorized access, and ensures real-time threat detection through AI-driven analytics. Furthermore, the system maintains energy efficiency and scalability, demonstrating consistent throughput and performance across high-density device deployments. These findings underscore the transformative impact of Zero Trust principles in future 6G CPS architectures, addressing challenges posed by expanded attack surfaces and complex network topologies. Future research will focus on integrating quantum-safe cryptographic techniques, federated learning for adaptive security policies, and further optimizing resource allocation to enhance long-term resilience and performance. The adoption of Zero Trust security frameworks will be critical in ensuring the sustainability and robustness of next-generation CPS, providing secure, efficient, and intelligent security mechanisms that adapt dynamically to evolving cyber threats.

Author Contributions: Conceptualization, A.K.A. and A.M.A.; methodology, A.K.A. and A.M.A.; validation, A.M.A.; formal analysis, A.K.A. and A.M.A.; investigation, A.K.A. and A.M.A.; resources, A.M.A.; data curation, A.M.A.; writing—original draft preparation, A.K.A.; writing—review and editing, A.K.A. and A.M.A.; visualization, A.K.A.; supervision, A.K.A.; project administration, A.K.A.; funding acquisition, A.K.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. KFU251039).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: This study could not have been started or completed without the encouragement and continued support of King Faisal University.

Conflicts of Interest: The authors declare no conflicts of interests.

References

1. Ahmadi, S. Autonomous identity-based threat segmentation in zero trust architectures. *arXiv* **2025**, arXiv:2501.06281.
2. Blika, A.; Palmos, S.; Doukas, G.; Katsikas, S.K. Federated learning for enhanced cybersecurity and trustworthiness in 5g and 6g networks: A comprehensive survey. *IEEE Open J. Commun. Soc.* **2024**, *5*, 1234–1256. [CrossRef]
3. Mohseni Ejiyeh, A. Real-time lightweight cloud-based access control for wearable iot devices: A zero trust protocol. In Proceedings of the First International Workshop on Security and Privacy of Sensing Systems, Istanbul, Turkey, 17 November 2023; pp. 22–29.
4. Gil, S.; Yemini, M.; Chorti, A.; Nedić, A.; Poor, H.V.; Goldsmith, A.J. How physicality enables trust: A new era of trust-centered cyberphysical systems. *arXiv* **2023**, arXiv:2301.12345.
5. Hasan, K.M.B.; Sajid, M.; Lapina, M.A.; Shahid, M.; Kotecha, K. Blockchain technology meets 6g wireless networks: A systematic survey. *Alex. Eng. J.* **2024**, *92*, 199–220. [CrossRef]
6. Liyanage, M.; Porambage, P.; Zeydan, E.; Senevirathne, T.; Siriwardhane, Y.; Yadav, A.K.; Siniarski, B. Advancing security for 6g smart networks and services. In Proceedings of the Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Antwerp, Belgium, 3–6 June 2024; pp. 616–621.
7. Lv, F.; Wang, H.; Pan, Z.; Sun, R.; Si, S.; Zhang, W. Asynchronous federated learning based zero trust architecture for the next generation industrial control systems. *SSRN* **2025**.
8. Mondal, M.K.; Banerjee, S.; Zhang, Y. Toward fast reliable intelligent industry 5.0—A comprehensive study. In *Smart Cyber-Physical Systems*; Springer: Berlin/Heidelberg, Germany, 2025; Volume 4, pp. 12–25.
9. Nahar, N.; Andersson, K.; Schelén, O.; Saguna, S. A survey on zero trust architecture: Applications and challenges of 6g networks. *IEEE Access* **2024**, *12*, 94753–94764.
10. Nguyen, H.; Lim, Y.; Seo, M.; Jung, Y.; Kim, M.; Park, W. Strengthening information security through zero trust architecture: A case study in South Korea. In Proceedings of the International Conference on Intelligent Systems and Data Science, Can Tho, Vietnam, 11–12 November 2023; Springer: Singapore, 2023; pp. 63–77.
11. Nie, S.; Ren, J.; Wu, R.; Han, P.; Han, Z.; Wan, W. Zero-trust access control mechanism based on blockchain and inner-product encryption in the internet of things in a 6g environment. *Sensors* **2025**, *25*, 123–135. [CrossRef] [PubMed]
12. Ren, Y.; Huang, D.; Wang, W.; Yu, X. Bsmd: A blockchain-based secure storage mechanism for big spatio-temporal data. *Future Gener. Comput. Syst.* **2023**, *138*, 328–338. [CrossRef]
13. Sakthi, U.; Alasmari, A.; Girija, S.P.; Senthil, P.; Qamar, S.; Hariharasitaraman, S. Smart healthcare based cyber physical system modeling by block chain with cloud 6g network and machine learning techniques. *Wirel. Pers. Commun.* **2024**, *125*, 1234–1256.
14. Scalise, P.; Boeding, M.; Hempel, M.; Sharif, H.; Hempel, M. A systematic survey on 5g and 6g security considerations, challenges, trends, and research areas. *Future Internet* **2024**, *16*, 67. [CrossRef]
15. Siniarski, B.; Sandeepa, C.; Wang, S.; Liyanage, M. Robust-6g: Smart, automated, and reliable security service platform for 6g. In Proceedings of the IEEE International Conference on Communications (ICC), Budapest, Hungary, 2–5 July 2024.
16. Sun, Y.; Yang, B.; Wang, E.; Gong, J.; Chen, W.; Sun, Z. Distributed industrial digital twinning scheme in 6g future scenarios. In Proceedings of the 2024 International Conference on Advanced Communication Technology, Sydney, Australia, 3–5 December 2024; pp. 123–128.
17. Suomalainen, J.; Ahmad, I.; Shajan, A.; Nieminen, M. Cybersecurity for tactical 6g networks: Threats, architecture, and intelligence. *Future Comput. Syst.* **2025**, *125*, 45–58. [CrossRef]
18. Trinh-Nguyen, B.; Berri, S.; Teo, S.G.; Truong-Huu, T.; Chorti, A. A framework for global trust and reputation management in 6g networks. *J. Netw. Comput. Appl.* **2024**, *200*, 102345.
19. Tripi, G.; Iacobelli, A.; Rinieri, L.; Prandini, M. Security and trust in the 6g era: Risks and mitigations. *Electronics* **2024**, *13*, 2162. [CrossRef]
20. Alwakeel, A.M.; Alnaim, A.K. Network Slicing in 6G: A Strategic Framework for IoT in Smart Cities. *Sensors* **2024**, *24*, 4254. [CrossRef] [PubMed]
21. Vashishth, T.K.; Sharma, V.; Sharma, M.K.; Gupta, R.K. Healthcare and smart cities applications of secure 6g infrastructure. In *Emerging Technology*; IGI Global: New York, NY, USA, 2025; Volume 7, pp. 50–65.
22. Zhu, C.; Fan, X.; Zheng, W.; Chen, S.; Liu, S.; Deng, X.; Yang, Y. Intelligent management and computing for trustworthy services under 6g-empowered cyber-physical-social system. *IEEE Netw.* **2024**, *38*, 20–27.
23. Zhukabayeva, T.; Zholshiyeva, L.; Karabayev, N.; Khan, S.; Tolegen, A. Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions. *Sensors* **2025**, *25*, 234–250. [CrossRef] [PubMed]
24. Alwakeel, A.M.; Alnaim, A.K. Trust Management and Resource Optimization in Edge and Fog Computing Using the CyberGuard Framework. *Sensors* **2024**, *24*, 4308. [CrossRef] [PubMed]
25. Albarrak, K.M.; Sorour, S.E. Web-Enhanced Vision Transformers and Deep Learning for Accurate Event-Centric Management Categorization in Education Institutions. *Systems* **2023**, *12*, 475. [CrossRef]

26. Alnaim, A.K.; Alwakeel, A.M. Machine-Learning-Based IoT–Edge Computing Healthcare Solutions. *Electronics* **2023**, *12*, 1027. [CrossRef]
27. Albarrak, K.M.; Sorour, S.E. Boosting Institutional Identity on X Using NLP and Sentiment Analysis: King Faisal University as a Case Study. *Mathematics* **2024**, *12*, 1806. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.