ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1853

IoT and Cyber-Physical Systems: Problems with Security and Ways to Fix Them

Umar Abba[1]; Dr. Umema Ahmed[2]; Garima Joon[3];
Dr. Ahmad Ndanusa[4]; Dr. Jamilu Awwalu[5];
Abdurrahim Magaji[6]; Abba Yahaya[7]; Fatima Muhammad Adam[8]

[1,2,3,4,5,6,7,8] Forensic Science Department, Vivekananda Global University
Jaipur, Rajasthan, India.

Publication Date: 2026/04/09

Abstract: The proliferation of Internet of Things (IoT) devices and their integration into larger Cyber-Physical Systems (CPS) have ushered in an era of unprecedented connectivity and automation. From smart grids and industrial control systems to autonomous vehicles and healthcare monitoring, these systems are revolutionizing modern life. However, this rapid expansion has created a vast and complex attack surface, making security a paramount concern. The inherent characteristics of IoT/CPS, such as resource constraints, heterogeneity, and the tight coupling of the cyber and physical worlds, introduce unique security challenges that traditional IT security models are ill-equipped to address. This paper provides a comprehensive analysis of the security landscape for IoT and CPS. It begins by delineating the architectural components and identifying the unique vulnerabilities at each layer—the Perception Layer, Network Layer, and Application Layer. We then systematically categorize the primary threats, including device tampering, communication interception, data integrity attacks, and sophisticated malware like botnets. Crucially, the paper explores the tangible consequences of these cyber threats on the physical world, highlighting risks to public safety, critical infrastructure, and economic stability. Finally, we propose a holistic, multi-layered mitigation strategy framework. This framework encompasses secure device manufacturing, robust cryptographic protocols, lightweight intrusion detection systems, blockchain for data integrity, and comprehensive security policies. The paper concludes that securing the IoT/CPS ecosystem requires a collaborative, proactive, and layered approach that integrates security into the entire lifecycle of these systems.

Keywords: *Internet of Things (IoT), Cyber-Physical Systems (CPS), Cybersecurity, Critical Infrastructure, Mitigation Strategies, Botnets, Data Integrity.*

How to Cite: Umar Abba; Dr. Umema Ahmed; Garima Joon; Dr. Ahmad Ndanusa; Dr. Jamilu Awwalu; Abdurrahim Magaji; Abba Yahaya; Fatima Muhammad Adam (2026) IoT and Cyber-Physical Systems: Problems with Security and Ways to Fix Them. *International Journal of Innovative Science and Research Technology*, 11(3), 3740-3742. https://doi.org/10.38124/ijisrt/26mar1853

I. INTRODUCTION

The convergence of the digital and physical worlds is at the core of the Fourth Industrial Revolution. This convergence is primarily driven by two interconnected paradigms: the Internet of Things (IoT) and Cyber-Physical Systems (CPS). IoT refers to the vast network of interconnected, smart devices—from sensors and actuators to home appliances—that collect, transmit, and process data [1]. CPS, a broader concept, are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components [2]. In essence, IoT devices often serve as the sensory and actuation front-end for larger CPS.

The applications are transformative: smart cities optimize traffic and energy use, industrial IoT (IIoT) enhances manufacturing efficiency, and connected healthcare enables remote patient monitoring. However, this deep integration means that a vulnerability in the cyber component can have direct, and often dangerous, repercussions in the physical world. A compromised sensor in a smart grid can lead to widespread blackouts [3], a hacked autonomous vehicle can

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1853

cause accidents, and a breached medical device can jeopardize patient lives.

Traditional cybersecurity has focused on protecting data confidentiality, integrity, and availability (CIA triad) within information technology systems. IoT/CPS security must expand this triad to include Safety, Reliability, and Resilience [4]. The challenge is compounded by the resource-constrained nature of many IoT devices (limited processing power, memory, and battery life), which precludes the use of computationally intensive security solutions. Furthermore, the long lifecycle and heterogeneous nature of these devices create a persistent and varied attack surface.

This paper aims to dissect the security challenges inherent to IoT and CPS and propose a comprehensive framework for mitigation. The objective is to move beyond a siloed view of security and present an integrated approach that addresses vulnerabilities across the entire system stack.

II. BACKGROUND AND ARCHITECTURE

To understand the security challenges, one must first understand the typical layered architecture of an IoT/CPS, which is generally conceptualized in three layers:

- Perception Layer (Sensing/Physical Layer): This is the physical layer consisting of sensors, actuators, Radio-Frequency Identification (RFID) tags, and other devices that interact directly with the environment. They are responsible for collecting data (e.g., temperature, motion, location) and executing physical actions.
- Network Layer (Transmission Layer): This layer is responsible for connecting the perception layer devices to the application layer and to each other. It utilizes a variety of communication protocols such as Wi-Fi, Bluetooth, Zigbee, LoRaWAN, and cellular networks (4G/5G).
- Application Layer: This layer processes the data received from the network layer to deliver specific services to the end-user. Examples include smart home applications, industrial control system dashboards, and healthcare analytics platforms.
- Each of these layers presents a distinct set of vulnerabilities and is susceptible to specific types of attacks.

III. SECURITY CHALLENGES AND THREAT LANDSCAPE

The security challenges in IoT/CPS can be categorized by the layer they primarily affect.

➢ *Perception Layer Challenges*

- Physical Tampering: Attackers can physically capture, tamper with, or replace devices to extract cryptographic keys, inject false data, or disable them.
- Insecure Device Fabrication: Many low-cost devices are shipped with default, hard-coded passwords and lack secure boot mechanisms or hardware-based security modules (e.g., TPM).
- Side-Channel Attacks: Attackers can analyze power consumption, electromagnetic leaks, or timing information to extract secret keys from devices.

➢ *Network Layer Challenges*

- Eavesdropping and Traffic Analysis: Unencrypted or weakly encrypted communication channels can be intercepted, revealing sensitive data and system behavior.
- Man-in-the-Middle (MitM) Attacks: Attackers can position themselves between two communicating parties to intercept, alter, or inject malicious messages.
- Denial-of-Service (DoS) and Distributed DoS (DDoS): Attackers can flood devices or network gateways with traffic, rendering them unavailable. The Mirai botnet, which compromised millions of IoT devices to launch massive DDoS attacks, is a prime example [5].
- Protocol Exploitation: Vulnerabilities in wireless communication protocols (e.g., Zigbee, BLE) can be exploited to gain unauthorized access or disrupt services.

➢ *Application Layer Challenges*

- Insecure APIs: Application Programming Interfaces (APIs) that facilitate communication between devices, cloud services, and mobile apps are often vulnerable to injection attacks and broken authentication.
- Data Integrity and Privacy Violations: Data at the application layer can be corrupted, stolen, or misused, leading to privacy breaches and incorrect decision-making.
- Malicious Software and Botnets: Malware can infect the backend systems or devices themselves, enrolling them into botnets for large-scale attacks.

IV. CONSEQUENCES OF SECURITY BREACHES

The impact of IoT/CPS security failures extends far beyond data loss.

- Public Safety: Attacks on autonomous vehicles, medical devices (e.g., insulin pumps, pacemakers), or building management systems can directly lead to injury or loss of life.

- Economic Disruption: An attack on an industrial control system can halt production, leading to massive financial losses and supply chain disruptions. The 2021 Colonial Pipeline ransomware attack demonstrated how a cyber-attack can impact critical physical infrastructure [6].

- Critical Infrastructure Failure: Compromising a smart grid, water treatment facility, or transportation system can cripple essential services for millions of people, leading to social unrest and national security threats.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26mar1853

V. PROPOSED MITIGATION STRATEGIES: A LAYERED FRAMEWORK

A robust defense requires a multi-faceted approach that addresses each layer and the system as a whole.

➢ *Device-Level Mitigation (Perception Layer)*

- Secure Hardware Design: Incorporate hardware security modules (HSMs) and Physical Unclonable Functions (PUFs) for secure key storage and device identity.
- Secure Boot and Firmware Updates: Ensure devices boot only with trusted software and have a secure mechanism for receiving and installing patches over-the-air (OTA).
- Device Identity and Authentication: Implement strong, unique credentials for each device, moving beyond default passwords to certificate-based authentication.

➢ *Network-Level Mitigation (Network Layer)*

- Lightweight Cryptography: Use encryption and authentication protocols designed for resource-constrained devices (e.g., AES-128, ChaCha20, and Ed25519 for signatures).
- Network Segmentation: Isolate critical IoT/CPS networks from enterprise IT networks to limit the lateral movement of attackers.
- Intrusion Detection Systems (IDS): Deploy lightweight, anomaly-based IDS that can detect unusual network traffic patterns indicative of a botnet or MitM attack.

➢ *Application and Data-Level Mitigation (Application Layer)*

- Secure API Development: Implement robust authentication (OAuth 2.0), input validation, and rate limiting for all APIs.
- Data Encryption and Anonymization: Encrypt data both in transit and at rest. Use data anonymization techniques where possible to protect user privacy.
- Blockchain for Integrity: Leverage blockchain technology to create an immutable, tamper-evident ledger for recording critical sensor data and system events, ensuring data provenance and integrity [7].

➢ *Governance and Policy Mitigation*

- Security-by-Design: Integrate security considerations from the initial design phase of the product lifecycle, not as an afterthought.
- Regular Security Audits and Penetration Testing: Conduct periodic assessments to identify and remediate vulnerabilities.
- Industry-wide Standards and Regulations: Advocate for and adhere to emerging security standards and regulatory frameworks to ensure a baseline level of security across all products.

VI. CONCLUSION AND FUTURE WORK

The integration of IoT and CPS into the fabric of our society is irreversible and holds immense promise. However, this integration comes with significant security responsibilities. The unique characteristics of these systems—their physicality, resource constraints, and complexity—demand a security paradigm shift. This paper has outlined the critical vulnerabilities and threats across the architectural stack and proposed a comprehensive, layered mitigation framework.

No single solution can secure the entire IoT/CPS ecosystem. Effective security requires a collaborative effort from device manufacturers, network providers, software developers, system integrators, and end-users. It must be a continuous process of risk assessment, implementation of defenses, monitoring, and adaptation.

Future work will focus on the practical implementation and testing of the proposed framework in a simulated smart city environment. Research is also needed into the application of Artificial Intelligence (AI) and Machine Learning (ML) for real-time, predictive threat detection in large-scale, dynamic IoT/CPS networks. The battle for a secure and resilient cyber-physical future is ongoing, and it is one we cannot afford to lose.

REFERENCES

[1]. Ashton, K. (2009). That 'Internet of Things' Thing. RFID Journal.
[2]. Lee, E. A. (2008). Cyber Physical Systems: Design Challenges. 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC).
[3]. Cárdenas, A. A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. 3rd USENIX Workshop on Hot Topics in Security (HotSec).
[4]. Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-Physical Systems Security—A Survey. IEEE Internet of Things Journal, 4(6), 1802-1831.
[5]. Antonakakis, M., et al. (2017). Understanding the Mirai Botnet. 26th USENIX Security Symposium.
[6]. CISA. (2021). Cyber-Attack Against Colonial Pipeline. Alert (AA21-131A).
[7]. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Blockchain in Internet of Things: Challenges and Solutions. arXiv preprint arXiv:1608.05187.