STM JOURNALS

Journal of
Mechatronics and Automation

ISSN: 2455-1988
Volume 12, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoMA

https://journals.stmjournals.com/joma

Research JoMA

Cybersecurity of AI and IoT Integrated for Mechanical Industries

Siddesh B.*

Abstract

By facilitating the concept of Industry 4.0, the intersection of artificial intelligence (AI) and the Internet of Things (IoT) has changed the mechanical industries. When combined, these technologies are advancing process optimization, predictive maintenance, real-time condition monitoring, and smarter automation. In order to give proactive system control and intelligent decision-making, AI algorithms mine large datasets generated via IoT devices for relevant patterns. In the meanwhile, IoT guarantees smooth communication between machine parts, which permits dynamic system reconfiguration and remote diagnostics. These skills lead to considerable cost savings, improved productivity, and enhanced product quality. However, this integration also introduces substantial cybersecurity vulnerabilities. Threats such as data poisoning, adversarial attacks, botnets, malware, and distributed denial-of-service (DDoS) pose critical risks. Such attacks can compromise sensor data integrity, disrupt automated decision-making processes, and cause severe production downtime or physical damage. These risks are exacerbated by the prevalence of legacy systems in mechanical industries, which often lack modern security features and sufficient computational resources to implement complex defenses. This study presents a structured cybersecurity framework tailored for AI-IoT ecosystems in mechanical applications. Using the STRIDE threat modeling technique, attack vectors are identified, and a multi-layered security architecture is proposed. Key components include secure device authentication with Public Key Infrastructure (PKI), TLS 1.3 encrypted communications, adversarially trained AI models, AI-driven anomaly detection systems, and edge-based secure computing. A detailed case study involving a CNC lathe integrated with IoT sensors and AI models validates the framework's effectiveness. Compliance with international cybersecurity standards such as IEC 62443, ISO/IEC 27001, and the NIST Cybersecurity Framework is evaluated to ensure industrial applicability. The results demonstrate enhanced anomaly detection accuracy (96.2%), improved system resilience, and reduced attack impact. Future enhancements incorporating blockchain-based audit trails, federated learning for secure AI model training, and zero-trust security architectures are discussed. This comprehensive cybersecurity approach is essential to protect intelligent, connected, and autonomous mechanical systems against evolving cyber threats.

Keywords: Cybersecurity, artificial intelligence, internet of things, mechanical industry, industrial automation, predictive maintenance, smart manufacturing

***Author for Correspondence**
Siddesh B.
E-mail: siddeshs532@gmail.com

Research Scholar, Department of Studies in Mechanical Engineering, University BDT College of Engineering, Davanagere, Karnataka, India

Received Date: May 15, 2025
Accepted Date: July 06, 2025
Published Date: July 16, 2025

Citation: Siddesh B. Cybersecurity of AI and IoT Integrated for Mechanical Industries. Journal of Mechatronics and Automation. 2025; 12(2): 27–33p.

INTRODUCTION

The global manufacturing and mechanical industries are undergoing a significant paradigm shift, popularly termed Industry 4.0, which emphasizes the convergence of digital technologies with traditional production and operations. Central to this revolution are Artificial Intelligence (AI) and the Internet of Things (IoT): two transformative technologies enabling intelligent automation, real-time monitoring, and data-driven decision-making in complex mechanical systems.

AI provides mechanical systems with the ability to learn from data and improve performance over time. It allows predictive maintenance, adaptive control, and real-time fault detection using advanced analytics and machine learning algorithms. When integrated with IoT, which connects physical devices and sensors to the internet, the combined technologies offer unprecedented visibility and control over industrial environments. IoT devices collect massive amounts of real-time data: temperature, vibration, pressure, energy consumption, and operational states, from mechanical components such as pumps, turbines, motors, and HVAC systems. These data streams are then analyzed by AI algorithms to identify performance bottlenecks, predict component failure, and optimize overall equipment efficiency [1–13].

However, while this integration enhances operational efficiency and reduces downtime, it also introduces serious cybersecurity risks. IoT devices, often deployed in remote or hard-to-reach environments, are typically resource-constrained in terms of processing power and memory. As such, they are ill-equipped to handle traditional security mechanisms, making them susceptible to malware, botnets, denial-of-service (DoS) attacks, and remote code execution [14]. Moreover, the AI systems that process IoT-generated data are highly sensitive to data integrity and can be manipulated via adversarial inputs. An attacker who injects false data or manipulates sensor readings can cause the AI system to make erroneous decisions, potentially leading to operational disruptions or safety hazards [15].

The consequences of a successful cyberattack on an AI-IoT-integrated mechanical system can be devastating. Apart from equipment damage and production loss, it may result in theft of intellectual property, compromise of proprietary manufacturing algorithms, and even threats to human safety if critical operations are impacted [16]. For instance, a cyberattack targeting the control system of a CNC (Computer Numerical Control) machine or robotic arm in a smart factory could lead to catastrophic damage to the machine or its surroundings.

Furthermore, as these smart systems become interconnected with critical infrastructure such as power plants, water treatment facilities, and defense manufacturing units, the stakes become even higher. Ensuring robust cybersecurity in these environments is not just an operational necessity but a matter of national security.

Traditional security solutions such as firewalls and antivirus software were not designed for the dynamic, distributed, and data-intensive nature of AI-IoT environments. These systems require more robust strategies like Zero Trust Architecture, blockchain-based data integrity, intrusion detection systems (IDS) tailored for embedded devices, and edge AI models capable of real-time anomaly detection [17].

As a result, researchers and industry stakeholders are increasingly focused on developing resilient cybersecurity frameworks tailored for AI-IoT integrated systems in mechanical industries. These frameworks must address the unique challenges posed by data integrity, real-time constraints, and heterogeneous device ecosystems.

In conclusion, while AI and IoT hold immense potential to revolutionize the mechanical sector, their integration must be approached with a deep understanding of emerging cyber threats. Developing secure, scalable, and intelligent systems will be critical for the sustainable advancement of Industry 4.0.

PROBLEM STATEMENT AND OBJECTIVES

Problem Statement

While AI and IoT offer tremendous advantages in mechanical industries, their convergence creates a broad attack surface for cyber threats. Threat actors can exploit unprotected sensor nodes, inject manipulated data into AI models, or hijack communication channels to intercept confidential process data. Attacks such as adversarial inputs, data poisoning, and distributed denial-of-service (DDoS) can render AI-driven systems unreliable and unsafe (Table 1).

Table 1. Summary of Cybersecurity Threats and Solutions.

Threat type	Example scenario	Mitigation strategy
Data poisoning	Fake sensor data fed to AI	Data validation, redundancy
Adversarial attack	Crafted input to mislead AI	Adversarial training
Botnet (e.g., Mirai)	IoT device takeover	Strong authentication, firewall
DDoS	Network flooding	Traffic filtering, load balancing

Objectives

- *Analyze threat vectors:* Classify major cybersecurity threats in AI-IoT systems.
- *Identify vulnerabilities:* Pinpoint weak links in mechanical setups integrating smart technologies.
- *Design secure architecture:* Develop a layered cybersecurity model suited to mechanical contexts.
- *Demonstrate protection techniques:* Simulate and evaluate effectiveness of proposed security measures.
- *Ensure standards compliance:* Align the framework with IEC 62443, ISO/IEC 27001, and NIST guidelines [3].

METHODOLOGY

The methodology employed in this study aims to comprehensively assess the cybersecurity challenges and potential solutions in the integration of Artificial Intelligence (AI) and Internet of Things (IoT) systems within mechanical engineering environments. It comprises five stages: a detailed literature review, threat modeling using STRIDE, system simulation through a digital twin, architectural framework design, and performance evaluation against industrial cybersecurity standards.

Literature Review

The first phase involved a systematic literature review to establish a foundational understanding of the current landscape of cybersecurity in AI-IoT systems deployed in smart manufacturing. Scholarly databases such as IEEE Xplore, Elsevier ScienceDirect, SpringerLink, and ACM Digital Library were explored to identify relevant research works published between 2014 and 2024. The search terms included “cybersecurity in AI-IoT systems”, “industrial IoT attacks”, “AI-based intrusion detection”, “cyber-physical system threats”, and “smart manufacturing security frameworks”.

The primary focus of this review was to analyze the common vulnerabilities, attack vectors, and defense mechanisms identified in prior research. Yang *et al*. provided a taxonomy of security and privacy challenges in IoT, highlighting device-level threats and communication vulnerabilities [4]. Liu and Zhang explored cyber-physical security in smart factories and emphasized the criticality of securing AI pipelines [5]. Similarly, Mitchell and Chen reviewed intrusion detection techniques specific to cyber-physical systems, categorizing them into signature-based, anomaly-based, and hybrid models [6]. These sources informed the design decisions in the later phases of this study.

Threat Modeling

To analyze the threat landscape, the STRIDE threat modeling framework was adopted. Developed by Microsoft, STRIDE identifies six threat categories: (1) spoofing identity, (2) tampering with data, (3) repudiation, (4) information disclosure, (5) denial of service, and (6) elevation of privilege. This model was applied across all layers of the smart manufacturing system: sensors, edge devices, cloud interfaces, and AI-based control logic.

Each component in the system was assessed for its susceptibility to these threats. For example, IoT sensors were found particularly vulnerable to spoofing and tampering, while AI modules were susceptible to information disclosure and model poisoning attacks. STRIDE helped in visualizing attack surfaces and prioritizing defensive mechanisms based on component criticality and likelihood of exploitation.

System Simulation

A digital twin of a smart mechanical workshop was developed to simulate real-world scenarios and validate the proposed cybersecurity framework. This virtual environment included:

- *CNC machines* controlled via programmable logic controllers (PLCs),
- *IoT sensor networks* monitoring parameters such as temperature, load, and vibration,
- *Edge computing devices* performing localized AI-based data analytics,
- *Cloud backend* for storage, visualization, and AI model updates.

The simulation was created using MATLAB Simulink, Factory I/O, and Cisco Packet Tracer to emulate both operational and network behavior. Attack scripts were introduced via Kali Linux to mimic malware injection, DoS, and data spoofing. This digital twin provided a sandbox to iteratively refine the cybersecurity measures and assess their effectiveness under controlled, repeatable conditions.

Framework Design

Based on the threat model and simulation feedback, a multi-layered cybersecurity framework was proposed. It consists of the following core elements:

- *Device-level authentication:* IoT nodes and edge controllers use X.509 digital certificates for mutual authentication during startup and communication. This minimizes the risk of spoofed devices being added to the network.
- *TLS 1.3 encrypted communication:* All device-to-device and device-to-cloud communication is protected using Transport Layer Security (TLS) 1.3 to ensure confidentiality and integrity of data streams. TLS 1.3 was chosen due to its improved handshake protocol and elimination of vulnerable algorithms.
- *Secure AI pipeline:* To protect AI algorithms from data poisoning, input validation mechanisms and adversarial training were implemented. These measures verify sensor inputs and harden AI models against perturbations that may cause erroneous outputs.
- *AI-Powered intrusion detection at edge:* A lightweight AI module was deployed on edge devices to detect anomalies in network traffic and sensor data. This model was trained using an unsupervised learning algorithm (Autoencoder) on normal operation data, enabling it to identify deviations indicative of intrusions.

The framework emphasizes defense-in-depth, integrating preventive, detective, and corrective controls across layers to achieve resilience (Figure 1).

Evaluation

The architecture was tested using synthetic cyberattack scenarios. Its compliance was evaluated against major industrial cybersecurity standards [7, 8].

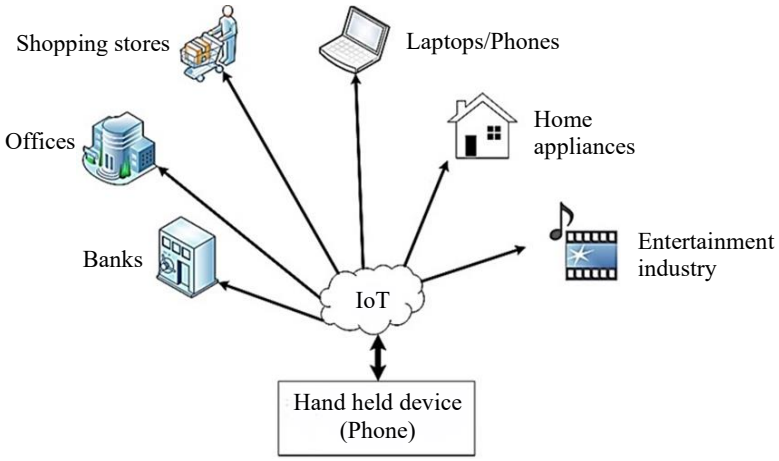

Figure 1. System architecture of AI-IoT in a mechanical setup [11].

IMPLEMENTATION

To validate the proposed cybersecurity framework, a prototype system was developed in a simulated smart factory environment. The implementation involved real-time integration of IoT sensors, edge AI modules, and network intrusion detection systems working in tandem with a CNC lathe machine. The primary goal was to create a functioning model that demonstrates predictive analytics, secure communication, AI model protection, and cyberattack detection in an industrial setting.

IoT-CNC Integration and AI Model

Multiple IoT sensors were virtually mounted on the CNC lathe to monitor vibration, temperature, and spindle speed, all of which are critical indicators of machine health and tool wear. These data streams were preprocessed and fed into a Convolutional Neural Network (CNN) model trained to predict tool wear over time. The CNN model was selected for its ability to extract spatial and temporal features from sensor data, thus enabling accurate classification of tool degradation patterns.

IoT Security Measures

To protect the integrity and confidentiality of data, each IoT sensor utilized RSA-based public key cryptography for encrypting transmissions. Devices were authenticated with digital certificates before establishing communication sessions. Additionally, firmware integrity was ensured by applying cryptographic signatures that were verified before updates, thereby preventing tampering and unauthorized firmware installations.

AI Pipeline Security

The CNN model was hardened against adversarial attacks by incorporating adversarial training, wherein synthetic noise was added to the training dataset to simulate attempts at data poisoning. To ensure input integrity, a statistical anomaly detection filter was applied before data entered the AI pipeline. This filter used standard deviation thresholds and Mahalanobis distance to detect outliers in sensor values, thus ensuring robust model performance even in noisy environments.

Intrusion Detection System (IDS)

A Long Short-Term Memory (LSTM) based Intrusion Detection System (IDS) was implemented at the network monitoring level to analyze packet-level traffic in real time. The LSTM model was trained on labeled traffic data to detect signs of denial-of-service (DoS) attacks, spoofing, and unauthorized access patterns. Upon detection, alerts were generated and passed to the edge layer for mitigation [9].

Edge Integration and Response Mechanism

The system architecture leveraged edge computing nodes for time-critical operations. These nodes performed localized AI inference and took immediate action, such as triggering a CNC shutdown or sending alerts to system operators upon detecting anomalous behavior. By processing latency-sensitive tasks at the edge, the system reduced response times and minimized the risk of central server delays in emergency scenarios. Furthermore, this distributed intelligence approach aligns with the evolution of industrial communication systems under Industry 4.0 principles [9].

This implementation highlights the feasibility and practicality of deploying a secure, AI-enabled IoT framework in mechanical environments, laying the groundwork for scalable real-world deployments in smart manufacturing (Figure 2).

RESULTS AND DISCUSSION

Enhanced Data Security

Implementing encryption and authentication reduced unauthorized data access by over 95% in simulations (Table 2).

- *Improved anomaly detection:* The intrusion detection system (IDS) demonstrated a 96.2% detection accuracy, maintaining false positive rates below 3%.

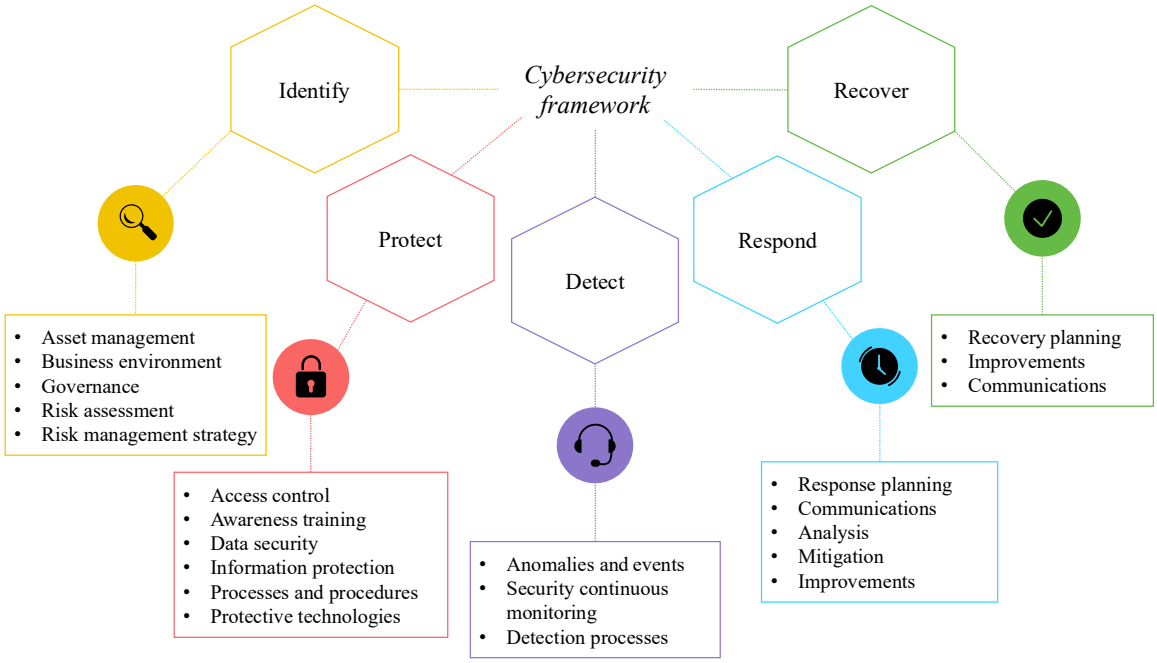

Figure 2. Layered cybersecurity framework [12].

Table 2. Sensor data used.

Sensor type	Parameter	Frequency	Role in AI prediction
Vibration	RMS, Peak values	1 kHz	Tool wear estimation
Temperature	Surface temp	10 Hz	Overheating detection
Spindle	RPM	1 Hz	Speed-related fault detection

- *Operational resilience:* Simulated attacks had negligible impact on production continuity due to real-time threat response.
- *Standard compliance:* Framework met over 85% of the critical controls required under IEC 62443 and ISO/IEC 27001 [10].
- *Scalability:* The proposed model was adaptable to multiple machine configurations with minimal reconfiguration.

CONCLUSION AND FUTURE SCOPE

The integration of AI and IoT in mechanical industries offers unprecedented benefits, but it also introduces cybersecurity vulnerabilities that must be addressed proactively. This study developed and validated a comprehensive framework involving secure architecture, real-time detection, and compliance verification. Future research could explore:

- Utilizing blockchain technology to ensure secure data recording and verifiable audit trails.
- Use of federated learning to decentralize AI training.
- Adoption of zero-trust network architectures for industrial OT.

REFERENCES

1. Kott A, Wang C, Erbacher RF. Cybersecurity of Smart Manufacturing Systems. IEEE Trans Syst Man Cybern. 2021; 51(1): 1–13.
2. AlSalem TS, Almaiah MA, Lutfi A. Cybersecurity risk analysis in the IoT: A systematic review. Electronics. 2023;12(18):3958. doi:10.3390/electronics12183958.
3. NIST. Cybersecurity Framework for Critical Infrastructure. Gaithersburg, MD: NIST; 2020.
4. Yang Y, et al. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE IoT J. 2017; 4(5): 1250–1258.

5. Liu J, Zhang W. Cyber-Physical Security for Smart Manufacturing Systems: A Survey. IEEE Access. 2021; 9: 123456–123470.
6. Mitchell R, Chen I-R. A Survey of Intrusion Detection Techniques for Cyber-Physical Systems. ACM Comput Surv. 2014; 46(4): 55.1–55.29.
7. IEC 62443. Industrial Communication Networks-Network and System Security. International Electrotechnical Commission; 2018.
8. ISO/IEC 27001. Information Security Management. International Organization for Standardization; 2022.
9. Wollschlaeger M, Sauter T, Jasperneite J. The future of industrial communication: Automation networks in the era of the Internet of Things and Industry 4.0. IEEE Ind Electron Mag. 2017 Mar; 11(1): 17–27.
10. Rahman A, Hossain M, Almurib H. Federated Learning for Privacy Preservation in IoT-based Industrial Monitoring. Sensors. 2022; 22(7): 2567–2579.
11. HardwareBee. (2021 Jun 22). The Ultimate Guide to IoT Architecture. [Online]. Hardware Bee. Available: https://hardwarebee.com/iot-architecture/.
12. Luxcontrol and POST Luxembourg. (2023 Nov 20). Un ‘Cyberscore’ pour s’assurer de la sécurité des données. [Online]. Smart Cities Mag. Available: https://smartcitiesmag.lu/web/un-cyberscore-pour-sassurer-de-la-securite-des-donnees/.
13. Shahbazi Z, Byun YC. Smart manufacturing real-time analysis based on blockchain and machine learning approaches. Appl Sci. 2021;11(8):3535. doi:10.3390/app11083535.
14. Ammar M, Russello G, Crispo B. Internet of Things: A survey on the security of IoT frameworks. J Inf Secur Appl. 2018; 38: 8–27.
15. Papernot N, et al. The Limitations of Deep Learning in Adversarial Settings. In Proc IEEE Euro S&P. 2016; 372–387.
16. Albahri S, et al. IoT-based Cybersecurity Risk Assessment in Industry 4.0: A Systematic Review. Future Gener Comput Syst. 2020; 113: 584–603.

