Grenze International Journal of Engineering and Technology, June Issue

Cyber-Attack Detection in Industrial IoT using Simulation

Amol Shankarrao Rane[1] and Khushi Sindhi[2]
[1]Research Scholar, Electronics and Telecommunication Engineering, Jhulelal Institute of Technology, Nagpur, Maharashtra, India
Email: asrane28@gmail.com
[2]Associate Professor, Electronics and Telecommunication Engineering, Jhulelal Institute of Technology, Nagpur, Maharashtra, India
Email: khushisindhi@sbjit.edu.in

***Abstract*— Industrial Internet of Things (IIoT) systems are transforming modern industries through real-time monitoring, automation, and intelligent decision-making. However, the increasing connectivity of sensors, controllers, and cloud platforms exposes IIoT infrastructures to sophisticated cyber-attacks that can disrupt operations, compromise data integrity, and threaten safety. This research focuses on developing a simulation-based framework for cyber-attack detection in Industrial IoT environments. The proposed work models an IIoT network consisting of sensors, actuators, gateways, and cloud servers within a simulated environment to emulate realistic industrial communication patterns. Various cyber-attack scenarios—such as Denial of Service (DoS), Man-in-the-Middle (MITM), data injection, and spoofing—are generated to analyze their impact on system behavior. Machine learning and anomaly detection techniques are applied to network traffic and device behavior data collected from the simulation to identify abnormal patterns indicative of cyber threats. Performance metrics such as detection accuracy, false positive rate, response time, and resource utilization are evaluated to validate the effectiveness of the proposed detection model. The simulation-driven approach enables safe testing, repeatability, and scalability without risking real industrial infrastructure. The outcome of this research contributes to enhancing the security, resilience, and reliability of IIoT systems by providing an intelligent cyber-attack detection mechanism suitable for real-time industrial environments.**

***Keywords*— Industrial IoT, Cyber-Attack Detection, Simulation, Anomaly Detection, Machine Learning, Network Security, DoS, MITM, Data Injection, IIoT Security.**

I. INTRODUCTION

A. Background

The Industrial Internet of Things (IIoT) has emerged as a transformative paradigm in modern industries by integrating sensors, actuators, controllers, communication networks, and cloud platforms to enable real-time monitoring, automation, and intelligent decision-making. Industries such as manufacturing, energy, transportation, healthcare, and smart infrastructure increasingly rely on IIoT systems to enhance operational efficiency, reduce downtime, optimize resource utilization, and improve safety.

Grenze ID: 01.GIJET.12.2.698_26

By enabling seamless connectivity among devices and systems, IIoT facilitates data-driven insights and predictive control strategies that were previously unattainable with conventional industrial setups.

Despite its numerous advantages, the rapid adoption of IIoT technologies has introduced significant cybersecurity challenges. Unlike traditional industrial control systems that operated in isolated environments, modern IIoT infrastructures are highly interconnected and often integrated with external networks, cloud services, and remote access platforms. This connectivity exposes critical industrial assets to a wide range of cyber threats, including Denial of Service (DoS) attacks, Man-in-the-Middle (MITM) attacks, data injection, spoofing, malware infiltration, and unauthorized access. Such attacks can lead not only to data breaches but also to operational disruptions, equipment damage, financial losses, and safety hazards for personnel.

Industrial environments are particularly vulnerable because many legacy devices and communication protocols were not originally designed with security in mind. Additionally, the heterogeneity of devices, real-time communication requirements, and resource constraints in IIoT networks make the implementation of traditional security mechanisms difficult. As a result, there is a growing need for intelligent and adaptive cyber-attack detection mechanisms that can monitor system behavior, identify anomalies, and respond promptly to potential threats without interrupting industrial operations.

Simulation-based approaches have gained attention as a practical and safe method for studying cyber-attacks and testing detection mechanisms in IIoT environments. Real-world experimentation on industrial systems is often risky, costly, and impractical due to safety concerns and potential operational disruptions. Simulation enables researchers to model realistic industrial networks, communication patterns, and attack scenarios in a controlled environment. This allows for the generation of large volumes of data under both normal and malicious conditions, which is essential for training and evaluating machine learning-based detection models.

Machine learning and anomaly detection techniques offer promising solutions for identifying cyber threats in IIoT systems. By analyzing patterns in network traffic, device behavior, and communication flows, these techniques can detect deviations from normal operations that may indicate an attack. Unlike rule-based security systems, machine learning models can adapt to evolving threats and complex attack strategies. When combined with simulation-generated datasets, these models can be rigorously tested and optimized for real-time deployment in industrial settings.

This research focuses on developing a simulation-based framework for cyber-attack detection in Industrial IoT systems. The framework models IIoT components such as sensors, actuators, gateways, and cloud servers, and simulates various attack scenarios to analyze their impact on system performance. The collected data is used to train and evaluate machine learning models for effective anomaly detection. By leveraging simulation and intelligent detection techniques, the proposed approach aims to enhance the security, resilience, and reliability of IIoT infrastructures, ensuring safe and uninterrupted industrial operations in the face of emerging cyber threats.

B. Literature Survey

Naima Samout et al. proposed an Explainable Artificial Intelligence (XAI)-based intrusion detection system for large-scale Wireless Sensor Networks (WSNs). The study integrates machine learning models with explainability frameworks such as SHAP and LIME to improve transparency in intrusion detection decisions. Hybrid models including LSTM-XGBooster and DNN-Random Forest were evaluated using the NSL-KDD dataset for detecting cyber-attacks such as DoS and injection attacks. The results demonstrated high accuracy, precision, recall, and interpretability, making the framework suitable for scalable IoT and industrial environments. [1]

Gagandeep Kaur, Vipin Balyan, and Sindhu Hak Gupta presented a comprehensive overview of deep learning techniques for Big Data IoT applications. The paper discusses IoT architectures, characteristics of IoT-generated big data, and the role of deep learning in analyzing heterogeneous and high-volume IoT data streams. The authors also explored cloud, edge, and fog computing infrastructures along with various deep learning models applicable to smart IoT systems. The study highlighted research challenges related to scalability, real-time analytics, and resource-constrained IoT environments. [2]

Mettu Jhansi Lakshmi and Arram Mahesh Babu proposed a Federated Deep Reinforcement Learning (F-DRL) framework for adaptive routing, congestion control, and energy minimization in Cognitive Radio Networks (CRNs). The proposed approach combines federated learning with deep reinforcement learning to enable privacy-preserving collaborative routing and dynamic spectrum management. The framework integrates cross-layer optimization using network, MAC, and physical layer parameters to improve packet delivery ratio, reduce delay, and optimize energy utilization. Simulation results demonstrated superior performance compared to conventional DRL-based routing methods in dynamic wireless environments. [3]

Barbhaya et al. states that the rapid integration of network-based control systems vulnerabilities within Industrial Control Systems (ICS) has increased exposure to sophisticated cyberattacks, especially in the chemical process industry. Adversaries exploit these systems by manipulating sensor data, disrupting operations, and compromising safety while remaining undetected by conventional fault detection mechanisms. Cyberattacks on critical infrastructure have become the new normal, with the World Economic Forum (WEF) ranking cyber threats as the seventh highest global risk in terms of likelihood over the next decade. [4]

Ragab et al. states that in Industry 4.0, information and communication technology (ICT) was employed in numerous significant infrastructures, like financial networks, smart factories, and power plants, to automate and certify industrial systems. In power control systems, ICT technologies such as IIoT have improved automated monitoring, but legacy methods, originally autonomous, now connect with external networks. This progress has presented safety vulnerabilities from legacy ICT systems. Hence, various cybersecurity approaches are developed and examined to deal with cyberattacks and vulnerabilities. Utilizing new cybersecurity models in power control systems poses risks due to their uncertified safety. [5]

Alkhafaji et al. mentioned that the cyber-attack detection within Industrial Internet of Things (IIoT) environments presents unique challenges due to the complex, resource-constrained, and real-time nature of these networks. Traditional detection techniques often struggle to adapt to the dynamic environment of IIoT. For instance, many existing methods rely on signature-based detection, which fails to identify evolving threats. Other approaches, such as anomaly-based detection, can generate a high rate of False Positives, leading to inefficiencies in threat management. To address these challenges, we propose a novel detection and classification model specifically tailored for IIoT environments. The proposed model integrates Genetic Algorithms (GA) and Deep Learning (DL) to enhance cyber-attack detection within IIoT environments. [6]

TABLE I: COMPARISON WITH EXISTING RESEARCH DN PROPOSED RESEARCH IN TERMS OF VARIOUS

Ref.	Paper Title	Methodology Used	How It Is Useful for Our Research
[1]	Explainable AI-based Innovative Models for Intrusion Detection in Big Data WSN	Hybrid ML/DL models such as LSTM-XGBooster and DNN-Random Forest with SHAP and LIME explainability techniques using NSL-KDD dataset	Useful for integrating explainable AI techniques and hybrid deep learning models into cyber-attack detection in IIoT environments. Helps improve transparency and interpretability of intrusion detection systems.
[2]	An Overview of Deep Learning Techniques for Big Data IoT Applications	Comparative analysis of deep learning models, IoT architectures, cloud-edge-fog computing, and big data analytics	Provides foundational knowledge on IoT architectures, deep learning approaches, and big data processing techniques applicable for simulation-based IIoT security frameworks.
[3]	Federated Deep Reinforcement Learning for Cross-Layer Congestion Control and Energy Minimization in Cognitive Radio Networks	Federated Deep Reinforcement Learning (F-DRL), cross-layer optimization, adaptive routing, and privacy-preserving collaborative learning	Useful for understanding adaptive AI-based optimization and federated learning approaches that can enhance scalable and secure IIoT cyber-defense systems.
[4]	A Deep Learning Framework for Cyberattack Detection and Classification in Industrial Control Systems	Deep learning-based cyberattack detection and classification for Industrial Control Systems (ICS)	Helps in understanding advanced deep learning approaches for detecting cyberattacks in industrial environments and identifying vulnerabilities in IIoT systems.
[5]	Artificial Intelligence Driven Cyberattack Detection System Using Integration of Deep Belief Network with Convolution Neural Network on Industrial IoT	Deep Belief Network (DBN) integrated with Convolution Neural Network (CNN) for attack detection	Useful for implementing AI-driven attack detection mechanisms in IIoT networks with improved classification accuracy and automated threat analysis.

C. Problem Statement

The rapid integration of Industrial Internet of Things (IIoT) technologies into critical industrial operations has significantly improved automation, monitoring, and decision-making capabilities. However, this increased connectivity among sensors, controllers, gateways, and cloud platforms has also expanded the attack surface of industrial environments, making them highly vulnerable to sophisticated cyber threats. Traditional industrial control systems were designed to operate in isolated settings with minimal consideration for cybersecurity, and many legacy devices and communication protocols in IIoT networks still lack built-in security mechanisms.

Existing security solutions in industrial environments are largely rule-based, signature-dependent, or reactive in nature. These approaches struggle to detect emerging and unknown cyber-attacks such as Denial of Service (DoS), Man-in-the-Middle (MITM), data injection, spoofing, and insider threats, especially in dynamic and

heterogeneous IIoT ecosystems. Moreover, real-time industrial operations impose strict latency and resource constraints, limiting the applicability of conventional security frameworks.

D. Research Gaps

Recent investigations into the topic of cybersecurity for the Internet of Things (IoT) have concentrated mostly on the following three areas: deep learning-based intrusion detection, anomaly detection, and AI-driven threat analysis. These are the primary concerns that need to be addressed. Despite the fact that these methods offer a high level of detection accuracy, there are still a number of constraints that have not been resolved and have not been addressed. These constraints have not been addressed. There are a lot of studies that rely on benchmark datasets rather than realistic industry simulations, which makes it difficult for them to be applicable to situations that are common in the real world. Specifically, this is due to the fact that benchmark datasets are more accurate than actual industrial simulations. In addition, the implementation of specific methods is challenging in IIoT devices that have limited resources since these methods require a significant number of processing resources. This makes the implementation of these methods somewhat difficult.

E. Objectives

The main objectives of the research are:

- To study and analyze security vulnerabilities and attack surfaces.
- To identify and classify common cyber-attacks.
- To develop a realistic simulation environment.
- To design and implement cyber-attack detection mechanisms

II. METHODOLOGY

The proposed research adopts a simulation-driven and data-centric methodology to design, implement, and evaluate a cyber-attack detection framework for Industrial Internet of Things (IIoT) environments. The methodology is structured into systematic phases to ensure realistic modeling, reliable data generation, and effective evaluation of detection techniques.

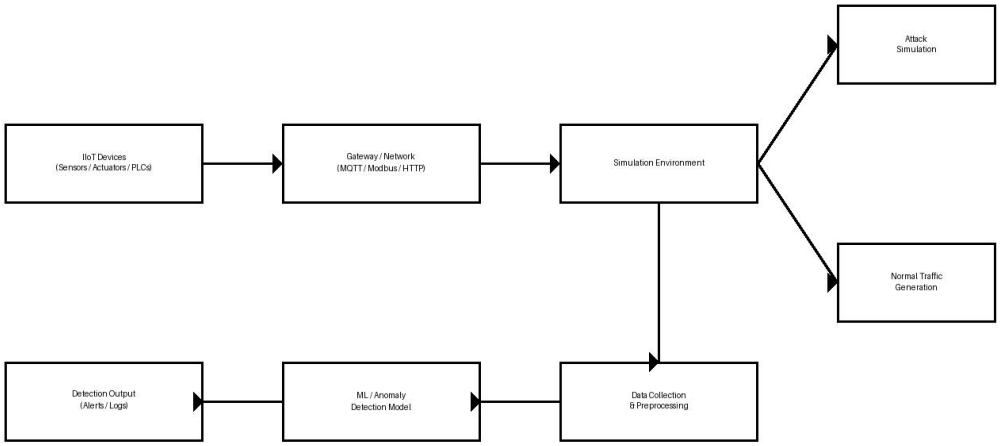

Fig. 1 Block diagram of the prosed research work

A. Design of IIoT Simulation Environment

A virtual IIoT network is created to replicate a typical industrial setup consisting of sensors, actuators, programmable logic controllers (PLCs), gateways, and cloud servers. Industrial communication protocols such as MQTT, Modbus/TCP, or HTTP are emulated to simulate real-time data exchange between devices. The simulation environment models normal operational behavior, including periodic sensing, control signaling, and data transmission patterns.

B. Modeling of Normal System Behavior

Baseline data representing legitimate IIoT operations is generated by running the simulation under attack-free conditions. Parameters such as packet size, transmission interval, device response time, bandwidth usage, and CPU/memory utilization are recorded. This dataset forms the reference for identifying deviations caused by cyber-attacks.

C. Simulation of Cyber-Attack Scenarios

Multiple cyber-attack scenarios are introduced into the simulated network to study their impact on IIoT communication and device behavior. These attacks include:

- Denial of Service (DoS) to overwhelm network resources
- Man-in-the-Middle (MITM) to intercept and manipulate data
- Data injection and spoofing to alter sensor readings
- Unauthorized access and replay attacks

Each attack is executed under controlled conditions while continuously capturing system and network parameters.

D. Data Collection and Preprocessing

Network traffic logs, device status logs, and communication metrics are collected from both normal and attack scenarios. The data is cleaned, labeled (normal/attack), normalized, and transformed into a structured dataset suitable for machine learning analysis. Feature extraction is performed to identify relevant attributes that influence detection performance.

E. Implementation of Machine Learning-Based Detection

Supervised and/or unsupervised machine learning algorithms such as Random Forest, Support Vector Machine, K-Nearest Neighbors, or Neural Networks are applied to the prepared dataset. These models learn patterns of normal and malicious behavior from the simulation data. Anomaly detection techniques are also explored to identify previously unseen attacks.

F. Training and Testing of Detection Models

The dataset is divided into training and testing subsets. Models are trained using the training data and validated using testing data to evaluate their generalization capability. Cross-validation techniques are used to improve reliability and avoid overfitting.

G. Performance Evaluation

The effectiveness of the detection framework is assessed using performance metrics such as accuracy, precision, recall, F1-score, false positive rate, detection time, and computational overhead. Comparative analysis of different algorithms is conducted to identify the most suitable model for IIoT environments.

H. Analysis and Optimization

Based on evaluation results, the detection model is optimized to reduce false alarms and improve detection speed. The scalability and adaptability of the framework for different industrial scenarios are also analyzed.
This methodology ensures a safe, repeatable, and scalable approach to developing an intelligent cyber-attack detection system tailored for Industrial IoT environments using simulation and machine learning techniques.

III. Expected Outcomes

- Comprehensive Understanding of Security Vulnerabilities and Attack Surfaces: The study will provide a detailed analysis of system vulnerabilities, weak network points, software flaws, and possible entry points that attackers may exploit. It will help in understanding how different components of a digital infrastructure contribute to overall security risks.
- Identification and Classification of Common Cyber-Attacks: The project will successfully identify and categorize major cyber-attacks such as phishing, malware, ransomware, denial-of-service (DoS), SQL injection, brute-force attacks, and man-in-the-middle attacks. This classification will improve awareness of attack patterns, characteristics, and their impact on systems.
- Development of a Realistic Cybersecurity Simulation Environment: A practical simulation environment will be created to emulate real-world cyber-attack scenarios. The environment will enable safe testing and analysis of attacks without affecting actual systems, allowing researchers and learners to study attacker behavior and system responses effectively.

IV. Discussion

An intelligent cyber-attack detection framework that is simulation-driven is presented by the research that is being provided. This framework was specifically created for environments that are related with the Industrial

Internet of Things (IIoT). Additionally, this framework is designed to be utilized in settings that are related with the Internet of Things (IoT). Unlike traditional intrusion detection systems, which are typically based on static rule-based or signature-based approaches, the framework that has been proposed combines simulation modeling with anomaly detection that is driven by machine learning in order to increase flexibility against developing cyber threats. This is done in order to protect against those threats. This action is taken in order to address the reality that cyber threats are always changing and becoming more sophisticated.

V. CONCLUSION

This research presented a simulation-based framework for cyber-attack detection in Industrial Internet of Things (IIoT) environments. With the rapid adoption of connected sensors, controllers, gateways, and cloud platforms in industrial systems, cybersecurity has become a critical challenge due to the increasing risk of sophisticated cyber threats. The proposed work successfully analyzed security vulnerabilities and attack surfaces within IIoT infrastructures and demonstrated how cyber-attacks can affect industrial operations, communication reliability, and data integrity. A realistic IIoT simulation environment was developed to emulate industrial communication and operational behavior under different attack conditions. Multiple cyber-attack scenarios, including Denial of Service (DoS), Man-in-the-Middle (MITM), spoofing, and data injection attacks, were simulated to evaluate their impact on the system. This simulation-based approach enabled safe, scalable, and repeatable testing without compromising actual industrial infrastructure. Furthermore, machine learning and anomaly detection techniques were implemented to monitor network traffic and device behavior for identifying abnormal activities associated with cyber threats.

The proposed detection mechanisms achieved effective performance in detecting malicious activities with improved detection accuracy and acceptable false positive rates. Key evaluation parameters such as response time, resource utilization, and reliability validated the effectiveness of the developed framework for real-time industrial applications. Overall, the research contributes toward enhancing the security, resilience, and reliability of Industrial IoT systems by providing an intelligent and practical cyber-attack detection solution. The developed framework can serve as a foundation for future advancements in real-time intrusion detection, adaptive cybersecurity systems, and AI-driven industrial security architectures.

REFERENCES

[1] Naima Samout, Thouraya Gouasmia, and Nejah Nasri, “Explainable AI-based innovative models for intrusion detection in Big Data WSN,” Procedia Computer Science, vol. 270, pp. 5065–5072, 2025. DOI: https://doi.org/10.1016/j.procs.2025.09.633

[2] Gagandeep Kaur, Vipin Balyan, and Sindhu Hak Gupta, “An Overview of Deep Learning Techniques for Big Data IoT Applications,” International Journal of Communication Systems, vol. 39, no. 4, e70418, 2026. DOI: https://doi.org/10.1002/dac.70418

[3] Mettu Jhansi Lakshmi and Arram Mahesh Babu, “Federated Deep Reinforcement Learning for Cross-Layer Congestion Control and Energy Minimization in Cognitive Radio Networks,” Peer-to-Peer Networking and Applications, vol. 19, no. 69, 2026. DOI: https://doi.org/10.1007/s12083-026-02219-5

[4] Malhar Barbhaya, Purushottama Rao Dasari, Seshu Kumar Damarla, Rajagopalan Srinivasan, Biao Huang, A deep learning framework for cyberattack detection and classification in Industrial Control Systems, Computers & Chemical Engineering, Volume 202, 2025, 109278, ISSN 0098-1354.

[5] Mahmoud Ragab, Mohammed Basheri, Nasser N. Albogami, Alanoud Subahi, Omar A. Abdulkader, Hashem Alaidaros, Hassan Mousa, Abdullah AL-Malaise AL-Ghamdi, Artificial intelligence driven cyberattack detection system using integration of deep belief network with convolution neural network on industrial IoT, Alexandria Engineering Journal, Volume 110, 2025, Pages 438-450, ISSN 1110-0168

[6] Nadia Alkhafaji1,2 · Thiago Viana1 · Ali Al-Sherbaz. Integrated Genetic Algorithm and Deep Learning Approach for Effective Cyber-Attack Detection and Classification in Industrial Internet of Things (IIoT) Environments. Arabian Journal for Science and Engineering (2025) 50:12071–12095

[7] Mohammad Al Rawajbeh, Amala Jayanthi Maria Soosai, Lakshmana Kumar Ramasamy, Firoz Khan. Trustworthy Adaptive AI for Real-Time Intrusion Detection in Industrial IoT Security. IoT 2025, 6, 53

[8] QawsarGulzar, Khurram Mustafa. Interdisciplinary framework for cyber-attacks and anomaly detection in industrial control systems using deep learning. Scientific Reports | (2025) 15:26575

[9] Yifan Liu, Shancang Li, Sarah Bin Hulayyil. Intelligent Detection of Cyber Attack Patterns in Industrial IoT Using Pretrained Language Models. Electronics 2025, 14, 4094

[10] Saima Siraj Qureshi, Jingsha He, Siraj Uddin Qureshi, Nafei Zhu, Ahsan Wajahat, Ahsan Nazir, Faheem Ullah, Abdul Wadud, Advanced AI-driven intrusion detection for securing cloud-based industrial IoT, Egyptian Informatics Journal, Volume 30, 2025, 100644, ISSN 1110-8665

[11] Afrah Gueriani, Hamza Kheddar, Ahmed Cherif Mazari, Mohamed Chahine Ghanem, A robust cross-domain IDS using BiGRU-LSTM-attention for medical and industrial IoT security, ICT Express, 2025, ISSN 2405-9595.
[12] Siddhesh Pimpale. A Comprehensive Study on Cyber-Attack Vectors in EV Traction Power Electronics. Journal of Information Systems Engineering and Management 2023, 8(2) e-ISSN: 2468-4376
[13] Vita Santa Barletta, Vito Bavaro, Miriana Calvano, Antonio Curci, Antonio Piccinno, Davide Pio Posa. Enabling Cyber Security Education through Digital Twins and Generative AI. arXiv:2507.17518
[14] Saad Alqithami. Hierarchical Adversarially-Resilient Multi-Agent Reinforcement Learning for Cyber-Physical Systems Security. arXiv:2506.22445
[15] Rohit Trivedi, Sandipan Patra, Shafi Khadem, Data-centric explainable artificial intelligence techniques for cyber-attack detection in microgrid networks, Energy Reports, Volume 13, 2025, Pages 217-229, ISSN 2352-4847
[16] S Gouri Kiran Kumar, Dr Raavi Satya Prasad. SecuIIoT: Hyper-Tuned Adaptive Learning for Cognitive Detection of Industrial IoT (IIoT) Cyber Threats. IJSAT25026199 Volume 16, Issue 2, April-June 2025
[17] Matthew Boeding, Michael Hempel, Hamid Sharif. End-to-End Framework for Identifying Vulnerabilities of Operational Technology Protocols and Their Implementations in Industrial IoT. Future Internet 2025, 17, 34
[18] Lavanya Vemulapalli, P. Chandra Sekhar. A Customized Temporal Federated Learning Through Adversarial Networks for Cyber Attack Detection in IoT. Journal of Robotics and Control (JRC) Volume 6, Issue 1, 2025 ISSN: 2715-5072