# AI-BASED CYBERSECURITY SYSTEM

Siddesh K B<sup>1</sup>, Divya B S<sup>2</sup>, Hema B T<sup>3</sup>, Sathish K<sup>4</sup>, Moinuddin T A<sup>5</sup>

Department of Electronics and Communication Engineering, SJM Institute of Technology, Chitradurga 577502,Karnataka, India <u>Kondapur.b@gmail.com, divyashivakumar9379@gmail.com, hemaacharya2003@gmail.com, ks3465317@gmail.com,</u> <u>moinuddinsonu05@gmail.com</u>

## Abstract

In the evolving landscape of industrial automation and smart manufacturing, security has become a critical concern. With the rise of wireless communication technologies in Industrial Internet of Things (IIoT) systems, there is an increasing threat of cyber-attacks that can compromise machine data, interrupt operations, or lead to intellectual property theft. This project presents a simulation of a secure industrial environment using ESP8266 microcontrollers to demonstrate machine-to-hub communication and highlight potential vulnerabilities exploited by hackers. The system comprises two secure industrial machines (each powered by ESP8266) that generate simulated machine data, including parameters like pressure and temperature. These values are displayed locally using OLED displays and transmitted wirelessly to a secure hub using the ESP-NOW protocol, known for its low- latency, peer-to-peer communication. A TFT display at the secure hub aggregates and displays all machine data in real time. To emulate cyber vulnerabilities, a hacker hub (also based on ESP8266) is introduced with the ability to launch various types of attacks: passive sniffing, replay attacks, false data injection, and command hijacking. Each attack type can be triggered via dedicated push buttons, and the corresponding behavior is reflected in the secure hub asimulated machines.

## **I INTRODUCTION**

In the modern era of industrial automation, the integration of IoT (Internet of Things) and embedded systems has led to the development of highly efficient, connected, and intelligent factories. These smart industrial environments leverage real-time data exchange between machines, controllers, and cloud services to maximize productivity, reduce costs, and improve system reliability. However, this increased connectivity also introduces significant cybersecurity challenges, especially in protecting the integrity, confidentiality, and availability of machine data. This project, titled "AI-Based Cybersecurity System for Ethical Industry," focuses on simulating a secure industrial setup using ESP microcontrollers (ESP8266 and ESP-01), where ethical machines exchange sensitive operational data such as temperature and pressure with a secure hub. The project also demonstrates real-time simulation of cyber-attacks using a "Hacker Hub" that attempts to intercept and manipulate this data. The ethical hub, embedded with AI-based intrusion detection mechanisms and network protection modes, can detect and prevent these attacks to ensure system safety.

A user-friendly OLED display is utilized on each machine and hub to showcase real-time data and security notifications, enhancing the transparency and monitoring capabilities of the system. The goal is to present a full-stack embedded system capable of detecting unauthorized access and demonstrating four types of hacking attacks in a controlled simulation environment.

# **II LITERATURE SURVEY**

The increasing integration of IoT and embedded systems in industrial automation has raised significant concerns regarding the security of machine-to-machine communication. A literature review was conducted to understand the current state of industrial cybersecurity, embedded hardware communication protocols, and existing intrusion detection or prevention systems in resource-constrained environments like those using ESP8266 microcontrollers.

ESP8266-Based Wireless Sensor Network(2021), Focused on using ESP8266 for smart agriculture monitoring. Highlighted advantages of ESP-NOW protocol for local communication. Did not address any intrusion or data tampering threats[1]

Simulation of Cyber-Attacks on SCADA Systems (2020), Simulated replay and injection attacks on critical infrastructure. Targeted SCADA systems using software tools, not low-cost embedded microcontrollers. [2]

Machine Data Security in IIoT using Lightweight Protocols (2022)Discussed encryption overhead in microcontrollers. Suggested lightweight authentication but did not cover physical or behavioral attacks.

ESP-NOW Protocol Evaluation for IoT Applications (2020) Analyzed performance of ESP-NOW in peer-to-peer and broadcast

setups. Concluded that ESP-NOW is suitable for low-latency, short-range device communication.[3]

Modern industrial environments rely heavily on IoT-enabled devices to automate processes and collect real-time data from machinery. However, this level of connectivity opens up multiple vulnerabilities:

•Unencrypted communication between devices

•Lack of physical access protection

•Insecure firmware updates

•Absence of robust intrusion detection systems

•Devices often being operated in unmonitored or unattended environments

### **III METHODOLOGY**

The diagram illustrates two contrasting network scenarios: a secure ethical industry network and a compromised network infiltrated by hackers. In the ethical industry network, two machines—Machine 1 and Machine 2—are connected to a central hub, an ESP32 microcontroller, which communicates with displays and machine tools. This setup ensures controlled and secure interactions within the industry. However, the lower portion of the diagram showcases a hacker network breach, where malicious entities attempt to infiltrate the secure industry network. The hacker network consists of two compromised machines, Hacker Machine 1 and Hacker Machine 2, each with its own ESP32 hub. These hacked devices replicate the legitimate network structure but introduce vulnerabilities, gaining unauthorized access to the ethical industry network. The diagram visually emphasizes the significance of cybersecurity in interconnected systems, warning against the consequences of unsecured network hubs and unauthorized access to critical components. It highlights the necessity of implementing robust authentication measures, encryption, and secure communication protocols to safeguard industrial networks from malicious breaches.



Step-by-Step Process Flow

1. System Initialization

ESP8266 nodes initialize their Wi-Fi and ESP-NOW configurations.

Secure Hub registers machine nodes and hacker hub as peers.

Displays initialize and buzzer is set off.

2. Start Operation

Operator presses "Start" button on Secure Hub.

A signal is sent to both machine nodes to simulate operation.

3. Machine Data Generation Machines generate: Spindle Speed X, Y, Z Axis Values Pressure Temperature Production Count Displayed on OLED screens and transmitted to Secure Hub. 4. Secure Hub Monitoring Secure hub displays machine data on TFT. If network protection is enabled, any suspicious ESP-NOW transmission is blocked and buzzer triggers. If protection is disabled, the hacker hub can steal data. 5. Hacking Simulation Hacker presses any of the four attack buttons. Machine data is intercepted, replayed, or modified. Hacker machine OLEDs display cloned data, simulating stolen machine operations. 6. Attack Detection & Response If network protection is ON, secure hub blocks unauthorized packets. Updates display and activates buzzer alarm. Status of the protection is shown on screen.

# IV WORKING PROCESS

This system functions by utilizing multiple hardware nodes, each integrated with sensors, microcontrollers like NodeMCU or ESP32, and OLED displays, to monitor a network environment. Each node continuously gathers data on network activity and applies AI-based algorithms to analyze this data in real-time. The AI identifies unusual patterns such as repeated unauthorized access attempts or irregular signals that could indicate a security threat.

Upon detecting any suspicious behavior, the system instantly activates visual and audio alerts to inform users. It also isolates the compromised node to stop the threat from spreading within the network. The nodes communicate with each other continuously, allowing them to share information and coordinate their responses effectively. This collaborative approach enables the system to act as a smart intrusion detection network that proactively detects and counters cyber threats.

1. Deployment of Hardware Nodes

Multiple hardware nodes are placed throughout the network. Each node is equipped with sensors, a microcontroller (such as NodeMCU or ESP32), and an OLED display.

2. Continuous Monitoring

Each node continuously monitors the surrounding network activity, collecting data such as access attempts, signal strength, and communication patterns.

3. Data Analysis Using AI

The nodes use embedded AI algorithms to analyze the collected data in real-time. This analysis helps detect unusual behavior like repeated login failures or irregular signal patterns that may indicate a cyber threat.

4. Threat Detection

When the AI identifies suspicious activity, it flags it as a potential security threat.

5. Alert Activation

The affected node immediately activates visual alerts on the OLED display and audio alarms to notify users about the detected threat.

6. Isolation of the Threatened Node

To contain the threat, the system isolates the compromised node from the rest of the network, preventing further access or damage.

#### 7. Real-Time Communication

All nodes continuously communicate with each other, sharing information about detected threats and their status.

#### 8. Coordinated Response

Using the shared information, nodes coordinate their responses, enhancing the overall security by collaboratively defending the network against intrusions.

#### **V RESULT**

The image showcases a prototype of an AI-based cybersecurity system designed to secure industrial machines or IoT-based smart factory environments. The setup includes multiple modular units, some labeled as CNC machines or heaters, each equipped with microcontrollers, sensors, OLED displays, and connection interfaces. These components work together to simulate a secure industrial ecosystem where data is constantly monitored in real time. AI algorithms analyze this data to detect anomalies or potential cyber threats such as unauthorized access, unusual behavior patterns, or device malfunctions. The OLED displays can show system status or alerts, and buttons may allow manual control or simulate user interactions. By employing machine learning at the edge, the system can rapidly respond to threats without needing constant cloud connectivity. This kind of setup demonstrates how artificial intelligence can be embedded into physical systems to enhance their resilience against cyber-attacks in Industry 4.0 scenarios.



This AI-based cybersecurity system uses sensor-equipped nodes with microcontrollers and AI to monitor network activity, detect threats, and isolate compromised nodes. Real-time communication between nodes enables coordinated alerts and responses, simulating an intelligent intrusion detection network.



This AI-based cybersecurity system uses sensor-equipped nodes and a central unit to simulate and monitor network activity. It detects threats with AI, triggers alerts, and coordinates responses to protect the network.

#### VI CONCLUSION

This project successfully demonstrates a secure and insecure communication infrastructure between industrial IoT machines using ESP8266 microcontrollers and the ESP-NOW protocol. Through the simulation of real-world cyber-attacks such as data sniffing, replay attacks, and fake injection, the project highlights the vulnerabilities of unprotected IoT networks and the importance of incorporating security mechanisms. The system's modular design—featuring machine nodes, a secure hub, and a hacker hub—allowed for flexible testing, demonstration, and education about cybersecurity in embedded systems. With OLED and TFT displays, real-time feedback is provided to both operators and attackers, enhancing system transparency and usability. By introducing a network protection mechanism,

the system emphasizes how proactive security policies can mitigate potential threats, ensuring safe and continuous machine operations. This project lays a strong foundation for future expansions, including integration with cloud services, machine learning-based threat detection, and comprehensive industrial automation systems.

## **VII REFERENCES**

- [1] Bhardwaj, M.D. Alshehri, K. Kaushik, H.J. Alyamani, M. Kumar, Secure framework against cyber-attacks on cyberphysical robotic systems, J. Electron. Imaging 31 (6) 2022.
- [2] P. Chithaluru, A.T. Fadi, M. Kumar, T. Stephan, Computational intelligence inspired adaptive opportunistic clustering approach for industrial IoT networks, IEEE Internet Things J 2023.
- [3] M. Barrett, Technical Report, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2018.
- [4] I. Wiafe, F.N. Koranteng, E.N. Obeng, N. Assyne, A. Wiafe, S.R. Gulliver, Artificial intelligence for cybersecurity: a systematic mapping of literature, 2020.
- [5] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, K.K.R. Choo, Artificial intelligence in cyber security: research advances, challenges, and opportunities, Artif. Intell. Rev. 55 2022.
- [6] J. Martínez Torres, C. Iglesias Comesana, ~ P.J. García-Nieto, Machine learning techniques applied to cybersecurity, Int. J. Mach. Learn. Cybern. (10) 2019.
- [7] Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions IEEE Internet of Things Journal.
- [8] OWASP IoT Security Guidelines.
- [9] IEEE Research Papers on IoT Security and ESP-NOW
- [10] Practical IoT Hacking Book by Fotios Chantzis et al.