International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 10 | Oct - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

# Cyber Secure IOT Gateway for Secure Industrial/Defence IOT

**Ms.Waghmare.S.M** E&TC Dept. ( JSPM's BSP )
**Mr.Surwase.S.S** E&TC Dept. ( JSPM's BSP )
**Ms.Thombre.S.S** E&TC Dept. ( JSPM's BSP )
**Ms.Khurange.R.M** E&TC Dept. ( JSPM's BSP )
**Mr.Waghmode.M.N** E&TC Dept. ( JSPM's BSP )

---

**Abstract -** The rapid adoption of Internet of Things (IoT) technologies in industrial automation, critical infrastructure, and defence environments has increased the need for secure and reliable communication between sensors, controllers, edge devices, and cloud or command systems. Industrial and defence IoT networks face threats such as unauthorized access, malware, spoofing, denial of-service attacks, data interception, and compromised field devices. This review paper studies the role of a Cyber Secure IoT Gateway as a security boundary between field devices and higher-level networks. The paper reviews gateway architecture, device authentication, encrypted communication, access control, network segmentation, intrusion detection, secure firmware, logging, and edge based threat monitoring. It also discusses suitable hardware and software technologies for developing a practical gateway using microcontrollers or embedded Linux platforms. The reviewed approach shows that a layered gateway can reduce the attack surface, isolate vulnerable IoT nodes, and provide centralized monitoring while maintaining low-latency communication required by industrial and defence applications. The paper concludes with implementation considerations, limitations, applications, and future research directions.

**Key Words:** Cyber Security, Internet of Things, IoT Gateway, Industrial IoT, Defence IoT, Edge Security.

## 1. INTRODUCTION

The Internet of Things (IoT) connects physical devices, sensors, controllers, machines and information systems through wired and wireless networks. Industrial IoT (IIoT) extends this concept to manufacturing plants, energy systems, transportation, process control and other operational technology (OT) environments. Defence IoT

introduces additional requirements because connected assets may operate in mission-critical and hostile environments. A security failure in such systems can affect safety, availability, confidentiality and operational continuity.

An IoT gateway is an important intermediate node that connects field devices with enterprise, cloud or command networks. Besides protocol translation and data forwarding, a modern gateway can enforce authentication, encryption, access control, traffic filtering, device isolation and security monitoring. Therefore, a Cyber Secure IoT Gateway can be designed as a security boundary rather than only as a communication bridge.

This review focuses on the architecture and security mechanisms required for an IoT gateway intended for secure industrial and defence environments. It considers practical components, communication protocols, threat controls, deployment challenges and future improvements.

## 2. CYBER SECURITY REQUIREMENTS FOR INDUSTRIAL/DEFENCE IoT

Industrial and defence IoT systems require a

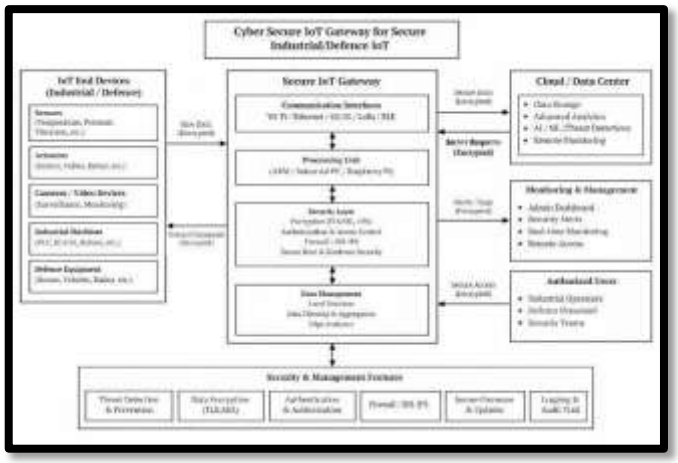
combination of information security and operational reliability. The main requirements are:

• Confidentiality: Sensitive telemetry, control commands and operational information should be protected from unauthorized disclosure.
• Integrity: Sensor readings and control messages must not be modified without authorization.
• Availability: Gateway and connected services should continue operating during faults and cyber attacks.
• Authentication: Only trusted devices, users and services should be allowed to communicate.
•Authorization: Access should be limited according to device identity, role and required function. • Secure management: Configuration, firmware updates, keys and credentials should be protected.

• Monitoring and logging: Security events should be recorded for detection, investigation and maintenance.

• Network isolation: Critical OT or defence devices should be separated from less-trusted networks.

## 3. CYBER SECURE IoT GATEWAY ARCHITECTURE




This diagram shown how the Cyber Secure IoT Gateway Protects Industrial/Defence IoT devices. Sensors, actuators, cameras, machine, and defence equipment send their data to the Secure IoT Gateway receives this data through Wi-Fi, Ethernet, 4G/5G, LoRa and processes it using a Raspberry Pi or Industrial computer, Before sending the data to the Cloud or monitoring System, the gateway provides Authentication, encryption, Firewall/IDS, threat detection, and secure data management.

The protected data is then send to the Cloud/Data Center, where it can be stored and analyzed, and to the Monitoring & Management System for real-time monitoring and alerts. Only authorized users such as industrial operators, defence personnel, and alerts. Only authorized users such as industrial operators, defence personnel, and security teams can access the system. Thus, the gateway acts as a secure middle layer between IoT devices and the cloud, preventing unauthorized access and protecting sensitive IoT data,

## 4. KEY SECURITY MECHANISMS

4.1 Device Authentication Each field device should have a unique identity. Certificates, pre-shared keys or secure tokens can be used depending on the device capability.
Mutual authentication is preferred for critical connections.

4.2 Encryption Transport Layer Security (TLS) can protect IP-based communication. For constrained or application specific systems, security mechanisms appropriate to the protocol should be used. Encryption protects telemetry and commands against interception.

4.3 Access Control Role-based or policy-based access control can restrict who or what can read data, change configuration, or issue control commands. Least privilege reduces the impact of a compromised account.

4.4 Intrusion Detection and Anomaly Detection The gateway can monitor connection rates, unexpected protocols, repeated authentication failures, unusual packet patterns and abnormal device behaviour. Rulebased detection is lightweight, while machine-learning methods may identify more complex anomalies.

4.5 Secure Firmware and Updates Firmware should be signed and verified before installation. Secure boot, protected credentials and controlled update mechanisms can reduce the risk of persistent malware.

4.6 Logging and Incident Response Authentication attempts, configuration changes, blocked traffic, firmware events and important system errors should be logged. Time synchronization and protected log storage improve forensic analysis.

## 5. COMMUNICATION PROTOCOLS AND TECHNOLOGIES

A gateway can support multiple protocols because industrial and defence deployments often contain heterogeneous equipment. MQTT is useful for lightweight publish/subscribe telemetry. HTTP/HTTPS is common for web-based services and APIs. CoAP can be considered for constrained devices. Modbus and Modbus TCP remain

common in industrial environments, while OPC UA provides richer industrial interoperability and security features. CAN/CAN-FD may be relevant to vehicles and embedded control networks. Ethernet, Wi-Fi and cellular links can provide network connectivity.

The gateway should not simply pass every protocol through. It should validate messages, restrict commands according to policy, and expose only the services required by the application.

## 6. COMPONENTS

### 6.1 HARDWARE COMPONENTS

#### i. ESP32



Fig.ESP32 DevKit V1 (ESP32-WROOM-32)

The ESP32 WROOM-32 is a low-cost microcontroller used for IoT applications. It can built-in Wi-fi and Bluetooth for wireless Communication. It can connect sensors like DHT22, PIR, MQ-2, and vibration sensors. It provides multiple GPIO pins for Connecting LEDs, buzzers, and relays. In this project, it collects sensor data and sends it securely to the Raspberry Pi Gateway. It supports MQTT and TLS encryption for secure Industrial/Defence IoT communication.

#### ii. Raspberry Pi 4/5



Fig.Raspberry Pi 4/5

The Raspberry Pi 4 Model B Is a small single- board computer used as the main controller in the project. It has GPIO pins, USB ports, Ethernet, Wi-Fi/Bluetooth, and communicate with other systems. In a Cyber Secure IoT Gateway, it can work as the central gateway for monitoring, data processing, and security.

#### iii. Temperature Sensor DHT11

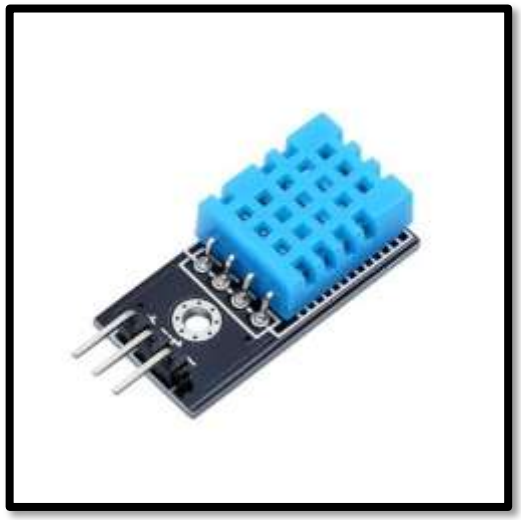


Fig.DHT11 Sensor

The DHT11 Temperature Humidity Sensor Is used to Measure the Temperature and humidity of the surrounding environments. It provides digital output that can be easily read by a Raspberry Pi or Microcontroller. In a Cyber

secure IoT Gateway, It can collect environmental data and send it is to the Gateway for monitoring and analysis.

**iv. Gas/Smoke Sensor (MQ-2)**




Fig.Gas/Smoke Sensor (MQ-2)

The MQ-2 Gas Sensor is used to detect gases such as smoke, LPG, Methane, and other combustible gases. It Provides a signal when the gas concentration increases. In a Cyber Secure IoT Gateway, It can monitor the Environment and send alerts to the Raspberry Pi when dangerous gas or smoke is detected.

**v. PIR Sensor**



Fig.PIR Sensor

This is a PIR(Passive Infrared) Motion Sensor. It detects the movements of people or object by Sensing changes in infrared radiation.

**vi. Vibration Sensor**



Fig.Vibration Sensor

This is a Vibration Sensor Module(SW-420 Type). It detects vibration or shaking and gives a digital output signal through the DO pin. The onboard potentiometer is used to adjust sensitivity. It can be connected to ESP32, Arduino, or Raspberry Pi for detecting machine vibration, Movement, tampering, or shocks.

**vii. Buzzer**



Fig.Buzzer

This is a Buzzer. It is an output device that produces a beeping Sound when electrical voltage is applied. In a Project, It can be used as an alarm or waiting indicator, such as when vibration, instrusion, or an abnormal condition is detected.

**viii. MicroSD Card**




Fig.MicroSD Card

This is a 32 GB microSD Card. It is used for storing data, Program, sensor readings, logs, and system files. In an IoT project, it can be connected to an ESP32 or Raspberry pi to save collected sensor data locally for later analysis or monitoring.

### 6.2 SOFTWARE/TECHNOLOGY USED

**i. Raspberry Pi OS / Linux**

Raspberry Pi OS /Linux is the operating system used to run and control the Raspberry Pi. It provides the required environment for programming, sensor communication, Networking, data processing, and security operations. In the project, It manages the IoT gateway, connected sensors, and data communication.

**ii. Arduino IDE**

Arduino IDE is a software tool used write, compile, and upload programs, to Arduino and ither microcontroller boards.. In this project, it can be used to Program the ESP32 for collecting sensor data and communicating with the Raspberry Pi gateway.

**iii. MQTT and Mosquitto MQTT Broker**

MQTT(Message Queuing Telementry Transport) is a lightweight communication protocol used to exchange data between IoT devices. Mosquitto MQTT Broker is a other devices. In this project, MQTT enables fast and reliable Sensor Data communication through the IoT gateway.

**iv. SQLLite/MySQL**

SQLite/MySQL are database system used to store and manage sensor data, Device Information, alerts, and Security logs. In this project, They can store data received from IoT Devices through the Raspberry Pi gateway, allowing the data to be retrieved, Monitored, and analyzed when required.

## 7. REVIEW OF SECURITY APPROACHES

Research and industry practice generally show that security is stronger when implemented as defence in depth. Encryption alone does not prevent an authenticated but compromised device from sending malicious commands. Similarly, authentication without segmentation can allow a compromised endpoint to reach sensitive systems.

Gateway-centric security is useful because it provides a common enforcement point for heterogeneous devices. However, the gateway itself becomes a critical asset and must be hardened, monitored and redundantly designed. Edge analytics can reduce response time, but resource constrained gateways may limit complex machine learning models. Lightweight rules and carefully selected anomaly features can provide a practical balance between security and performance.

For industrial systems, security controls must also consider deterministic communication and safety requirements. Security mechanisms should be tested so that they do not introduce unacceptable latency or interfere with legitimate control operations.

## 8. PROPOSED SECURE GATEWAY WORKING

The proposed concept starts with registration of trusted field devices. Each device receives an identity and security credential. During communication, the gateway verifies the device and applies an access policy. Valid telemetry is inspected and forwarded to an authorized application or cloud service through an encrypted channel. Control commands arriving from an authorized application are verified before being passed to the relevant field device.

If suspicious behaviour is detected, the gateway can block the connection, place the device in an isolated security

zone, generate an alert, and record the event. A local dashboard can display connected devices, network status, blocked events and alerts. This workflow allows the gateway to combine communication, policy enforcement and monitoring in one edge platform.

## 09: APPLICATIONS

The Cyber Secure IoT Gateway concept can be applied in smart manufacturing, industrial automation, power and energy monitoring, water treatment, transportation systems, secure surveillance, defence laboratories, military vehicle telemetry, perimeter monitoring, remote equipment monitoring and critical infrastructure. In defence-oriented systems, the gateway can provide an additional security boundary between field equipment and higher-level command or monitoring networks.

## 10. ADVANTAGES

•Centralized security enforcement for multiple IoT devices. Authentication and encryption reduce unauthorized access and data interception.
•Network segmentation can limit lateral movement after device compromise.
•Local edge processing can reduce dependence on cloud connectivity.
•Security logging supports monitoring and incident investigation.
•Multi-protocol support allows integration of legacy and modern equipment.
•Policy-based control can protect critical commands. • The architecture can be scaled from a student prototype to industrial edge deployment.

## 11. LIMITATIONS

A gateway cannot eliminate every endpoint vulnerability. If a field device is physically compromised or its credentials are stolen, additional controls may be required. Gateway failure can affect many connected devices, so redundancy and recovery mechanisms are important in high-availability environments. Advanced intrusion detection may also require additional CPU, memory and storage. Industrial protocol compatibility and legacy equipment can create implementation challenges.

## 12. FUTURE SCOPE

Future work can integrate hardware-backed key storage, secure boot, zero-trust access policies, software-defined network segmentation and lightweight artificial intelligence for anomaly detection. Federated or distributed learning can be investigated where data cannot be centrally collected. Digital twins and cyber range simulation can help evaluate attacks before deployment. Redundant gateways, trusted execution environments and post-quantum cryptographic migration are also promising research areas for long-life industrial and defence systems.

## 13. CONCLUSION

A Cyber Secure IoT Gateway can provide an effective security boundary for industrial and defence IoT environments. The gateway can combine device authentication, encrypted communication, access control, firewalling, segmentation, intrusion detection, secure updates and event logging. The review indicates that a layered security architecture is more suitable than relying on a single mechanism. A practical prototype using an embedded computer, industrial interfaces and opensource security software can demonstrate these principles at relatively low cost.

## 14. REFERENCES

1. Alwarafy, A., AI-Thelaya, K.A., Abdallah, M., Schneider, J., & Hamdi, M.(2022). A Survey on security and privacy Issues In Edge Computing-Assisted Internet of Things. *IEEE Internet of Things Journal, 9(6), 4003-4023*

2. NIST. (2022). Cybersecurity Framework 2.0: Internet of Things and Operational Technology Security Considerations. National Institute of Standards and Technology

3. ENISA. (2022). ENISA Threat Landscape for Supply Chain Attacks. European Union Agency for Cybersecurity

4. ENISA. (2022). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity

5. ENISA. (2022). ENISA Threat Landscape for Supply Chain Attacks. European Union Agency for Cybersecurity

6. AI-Hawawreh, M., Sitnikova, E., & McAndrew(2023). Industrial IoT cybersecurity: Challenges and Solutions for Critical Infrastructure. *IEEE Access.*

## 15. BIOGRAPHIES



Ms.Waghmare.S.M is a Diploma student in Electronics & Telecommunication Engineering. His academic interests include IoT, embedded systems, networking, cybers



Mr.Suwase.S.S is a Diploma student in Electronics & Telecommunication Engineering. His academic interests include IoT, embedded systems, networking, cybers



Ms.Thombre.S.S is a Diploma student in Electronics & Telecommunication Engineering. His academic interests include IoT, embedded systems, networking, cybers



Ms.Khurange.R.M is a Diploma student in Electronics & Telecommunication Engineering. His academic interests include IoT, embedded systems, networking, cybers



Mr.Waghmode.M.N is Diploma lecturer in Electronic and Telecommunications Engineering Department at JSPM's Bhivrabai Sawant Polytechnic, Wagholi