IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 04, April https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1304.13

Secure Data Exchange Techniques for Industrial Environments: A New Approach

SK.Pujitha
Assistant Professor, Department of CSE,
Guru Nanak Institute of Technology, Hyderabad, India
pujithask.csegnit@gniindia.org
https://orcid.org/0000-0002-7740-0593
P.Neha,O.Abhlash,R.Vaishnavi
Student, Department of CSE,
Guru Nanak Institute of Technology, Hyderabad, India
np2301069@gmail.com, odetiabhilashreddy@gmail.com , vaishnaviramathirtham2029@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10092
Research Article | Open Access | Double-Blind Peer-Reviewed| Article ID: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10092
Received:02,March 2026, Revised: 29, March 2026, Accepted: 10,April 2026,Published Online: 22, April 2026.
https://www.ijirae.com/volumes/Vol13/iss-04/13.AEAP26.APAE10092.pdf
ArticleCitation:Pujitha,Neha,Abhlash,Vaishnavi(2026),Secure Data Exchange Techniques for Industrial Environments: A New Approach, IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 13, Issue 04 of 2026 pages 813-817 **Doi:>** https://doi.org/10.26562/ijirae.2026.v1304.13 **BibTeX Key:Pujitha@2026Secure**
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2025, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2026.v1304.13 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: This project introduces a web-based secure data management system for IoT sensor datasets. It is built using Java EE (JSP and Servlets), MySQL, and Apache Tomcat. In contrast to the original draft that discusses an Industrial Control System AES framework, the source code and database provided implement a practical application. In this application, a client uploads tab-separated IoT sensor data files. The system parses the values, and each token is encrypted with AES before being stored in the database. This solution improves the confidentiality of sensor readings, supports controlled access, and provides a simple and affordable model for secure data exchange in academic IoT projects. It uses existing web technologies effectively.

Keywords: Secure Data Exchange, Industrial Environments, Internet of Things (IoT), Industrial Control Systems (ICS), AES Encryption, Data Security, Role-Based Access Control, Key Management, Secure Data Storage, Cybersecurity, Authentication and Authorization, IoT Sensor Data, Data Confidentiality, Secure Data Sharing, Web-Based Application

I. INTRODUCTION

The Internet of Things (IoT) has emerged due to the increasing number of connected devices, significantly improving healthcare through the Internet of Medical Things (IoMT). IoMT systems consist of wearable sensing devices connected via a wireless body area network (WBAN), an internet gateway, and a cloud-based data center, generating personal health data such as heart rate, and blood sugar levels for local or cloud-based analysis. The digitization of patient records supports remote monitoring, timely decision-making, and advanced medical research, enhancing overall healthcare efficiency and patient outcomes; however, fragmented data storage, unstable network infrastructure, and the massive volume of generated data hinder efficient data exchange and accessibility, while critical concerns such as data privacy regulations, increased risk of security breaches, and communication disruptions under abnormal conditions further complicate IoMT implementation. The proposed framework integrates IoMT and blockchain for the secure recording, processing, and storage of health metrics is preprocessed and securely stored in the blockchain to ensure tamper-proof records and transparency, while also enabling real-time access, visualization, and continuous monitoring of patient health, supporting proactive healthcare management, early diagnosis, and delivering a robust, decentralized, and scalable solution for secure, reliable, and efficient healthcare data management.

A. Objective

The main goal of this project is to ensure that IoT sensor data is securely stored and accessed only by authorized users. To achieve this, the system uses AES encryption to protect all uploaded sensor values before saving them in the database. It is designed in a way that clients can easily upload structured sensor data files, and for each upload, a unique batch ID is generated to keep the data organized. Every sensor value(token) is encrypted individually, a unique 16-digit secret key is created for each one to enhance security. The System also follows role-based access control, meaning users can only access the type of sensor data they registered for, such as temperature, humidity, or light. Additionally, users can view the original data only when they provide the correct batch details along with the valid secret key, ensuring controlled and secure data access at all times.

B. Problem Statement

Industrial environments increasingly rely on Internet of Things (IoT) and Industrial Control Systems (ICS) for real-time monitoring and automation.

However, most existing systems use legacy communication protocols that lack proper security mechanisms such as encryption, authentication, and secure key management. This makes sensitive industrial data vulnerable to cyber threats, including unauthorized access, data breaches, and manipulation. Additionally, current systems often transmit data in plaintext and depend heavily on perimeter-based security, which is insufficient against advanced attacks like man-in-the-middle and advanced persistent threats. There is also a lack of fine-grained access control, resulting in improper data sharing and increased risk of information exposure.

C. Scope of the Project

The scope of this project focuses on designing and developing a secure web-based system for managing and protecting IoT sensor data in industrial environments. The system ensures that sensitive data is encrypted, stored securely, and accessed only by authorized users. The project includes the implementation of AES encryption to protect sensor data before storage, along with role-based access control to restrict data access based on user roles such as Admin, Client, and User. It also provides a mechanism for secure data retrieval using unique batch IDs and secret keys, ensuring controlled and authenticated access.

II. LITERATURE SURVEY

M.Slunjski and D.Sumina[1](2025) presented an approach for enhancing Industrial Control System (ICS) security using next-generation Programmable Logic Controllers (PLCs). Their system integrates Linux-based environments to enable intrusion detection, threat monitoring, and secure communication, while maintaining compatibility with existing industrial infrastructures.

G.Yu and T.Shon[2](2024) analyzed security and forensic challenges in industrial Ethernet protocols. They highlighted vulnerabilities due to weak authentication and mis configurations and proposed solutions such as intrusion detection systems, network segmentation, and zero-trust architecture to improve industrial network security.

M.Slunjski et al.[3] (2022) investigated how off-the-shelf hardware and software tools can act as cyber threats in industrial environments. The study demonstrated attacks like Man-in-the-Middle (MITM) and Legal Client-to-Server attacks and proposed a cost-effective hardening methodology to enhance system protection.

M.Wan et al.[4](2021) provided insights into industrial cybersecurity challenges and defence mechanisms. Their work analyzed vulnerabilities in networked control systems and suggested improvements by adapting traditional IT security techniques for industrial applications.

R.Trifonov et al.[5](2021) discussed emerging cyber trends in industrial systems, including risks from cloud computing, remote access, and insider threats. They emphasized the importance of continuous monitoring, security audits, and employee awareness to strengthen system security.

W.Deng et al.[6](2024) proposed a self-sovereign identity (SSI)-based access control system using Ciphertext Policy Attribute-Based Encryption (CP-ABE) for IoT environments. Their approach eliminates centralized identity management and enhances privacy, security, and efficiency in resource-constrained IoT systems.

III. SYSTEM DESIGN

A. System Architecture

The system architecture for Secure Data Exchange in Industrial Environments using IoT and AES Encryption integrates IoT sensor data sources, a web-based application, encryption mechanisms, and a database to ensure data security, confidentiality, and controlled access. IoT sensor data is collected and uploaded by clients through the web interface, where it is processed and divided into individual data tokens. Each data value is encrypted using the AES algorithm before being securely stored in the database.

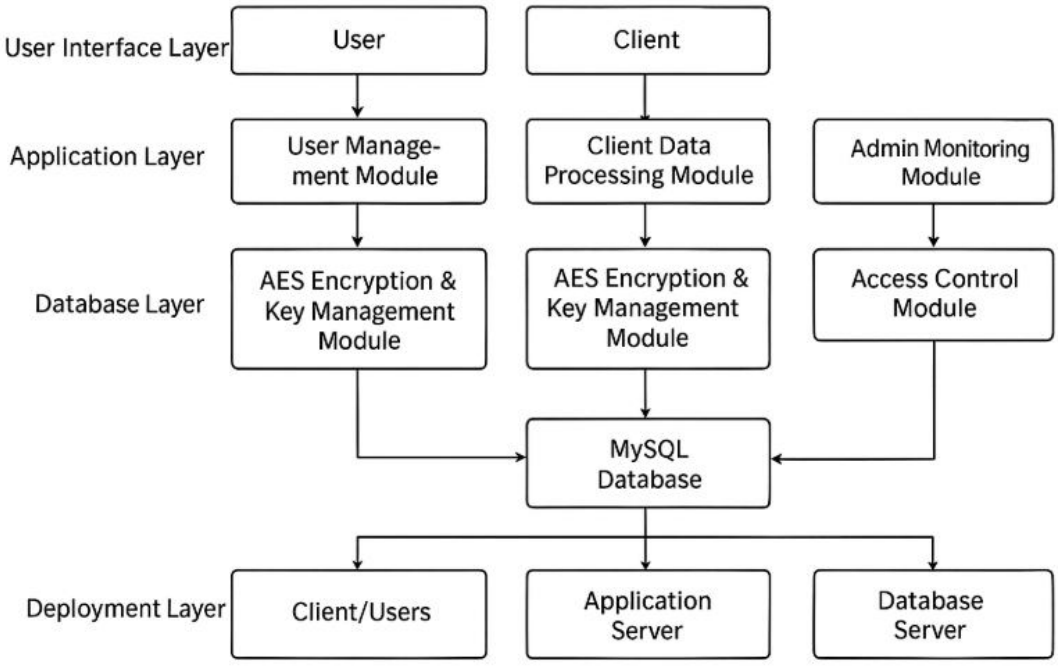

Fig: System Architecture Diagram

B. Methodology

The proposed system follows a structured methodology to ensure secure data handling, efficient processing, and controlled access in industrial IoT environments. Initially, users and clients interact with the system through a web-based interface where users register and log in securely. Clients upload IoT sensor data files, which are then processed by the system to extract and categorize sensor values. Each uploaded dataset is assigned a unique batch ID to maintain proper organization and traceability. Additionally, the system incorporates monitoring and logging mechanisms to track user activities, data access, and system performance. This methodology ensures data confidentiality, integrity, and secure data exchange while maintaining system efficiency and scalability.

C. Modules

1) AES Encryption Module: The AES module is the core security component of the system. It encrypts each IoT sensor data value before storing it in the database. AES, a symmetric key encryption algorithm, ensures that all data is converted into secure ciphertext. Only users with the correct secret key can decrypt and access the original data, thereby maintaining confidentiality and protection against unauthorized access.

2) Data Processing Module: The Data Processing module handles the uploaded IoT sensor data files. It parses the input file, extracts individual sensor values, and categorizes them based on sensor types such as temperature, humidity, or light. Each dataset is assigned a unique batch ID to maintain proper organization and traceability of data.

3) Role-Based Access Control (RBAC) Module: This module ensures controlled access to data based on user roles such as Admin, Client, and User. It restricts users to access only authorized sensor data. Users must request access to encrypted data, and only after admin approval can they retrieve and decrypt the data, ensuring secure and regulated data sharing.

4) Key Management Module: The Key Management module is responsible for generating and managing unique secret keys for each encrypted data token. It securely stores and maps keys with corresponding batch IDs. The module ensures that keys are distributed only to authorized users after verification, preventing misuse and enhancing system security.

5) Web Application (JSP/Servlet) Module: This module provides the user interface for the system. It includes functionalities such as user registration, login, file upload, data viewing, and key requests. The dashboard displays encrypted data, user activities, request status, and system details, enabling smooth interaction between users and the system.

6) MySQL Database: The MySQL database stores all system data, including user details, uploaded sensor data, encrypted values, batch IDs, secret keys, and access request logs.

7) Admin Monitoring Module: The Admin module oversees the entire system. It manages user registrations, monitors uploaded data, reviews key requests, and approves or rejects access requests.

IV. EXISTING SYSTEM VS PROPOSED SYSTEM

A. Existing System

The existing system in industrial environments uses Industrial Control Systems (ICS) that were originally designed for performance and reliability rather than security. Many of these systems rely on legacy communication protocols that do not support encryption or secure key exchange mechanisms. Data is often transmitted in plaintext, making it vulnerable to cyber threats such as unauthorized access, interception, and manipulation. Security mainly depends on firewalls and network isolation, which are not sufficient against advanced attacks like man-in-the-middle and advanced persistent threats. Additionally, integrating modern security solutions is difficult due to high cost, system complexity, and compatibility issues with existing infrastructure. As a result, current systems lack proper data protection and remain highly vulnerable to cyber attacks.

B. Proposed System.

The proposed system provides a secure web-based solution for managing IoT sensor data in industrial environments. It uses AES encryption to protect all sensor data before storing it in the database, ensuring data confidentiality and security. Each uploaded file is assigned a unique batch ID, and every data value is encrypted with a unique secret key for enhanced protection. The system implements Role-Based Access Control (RBAC), allowing users to access only authorized data based on their roles. Users must request access to encrypted data, and only after admin approval can they retrieve and decrypt it using valid keys. This ensures controlled data access and prevents unauthorized usage.

V. IMPLEMENTATION

A. Environment Initialization

The system is developed using Java EE technologies with JSP and Servlets for backend processing. The development environment includes JDK, Eclipse IDE, and Apache Tomcat Server for deployment. A MySQL database is configured to store user details, encrypted sensor data, keys, and logs, using JDBC connectivity for database interaction. Required drivers such as MySQL Connector are added to the project.

B. System Workflow Execution

The system workflow begins with user registration and secure login. The client uploads IoT sensor data files through the web interface. The system processes the file, extracts sensor values, and assigns a unique batch ID. Each data value is then encrypted using AES and stored in the database along with its secret key. When a user needs access, they send a request for the required data. The admin reviews the request and approves or rejects it. Upon approval, the user receives the corresponding key and can decrypt and view the data.

VI. RESULTS AND DISCUSSION

This section features screenshots that provide visual documentation of the system development, functionality and user interface evidence. The snapshots provide a clear representation of how the application works in real-time, and illustrates main functionality during release.

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 04, April https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1304.13

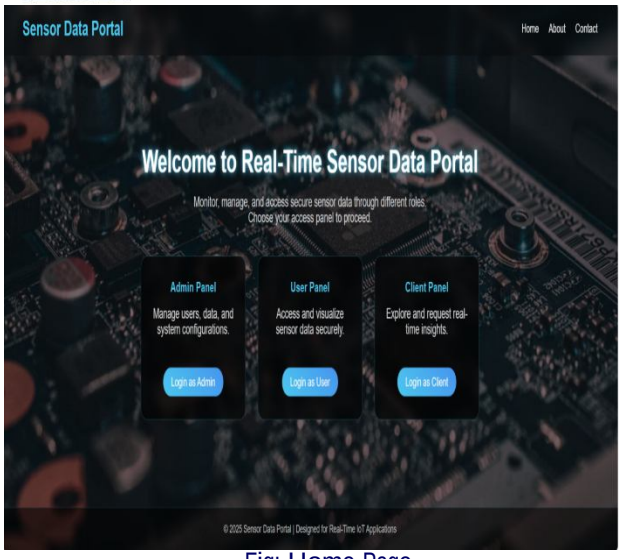

Fig: Home Page

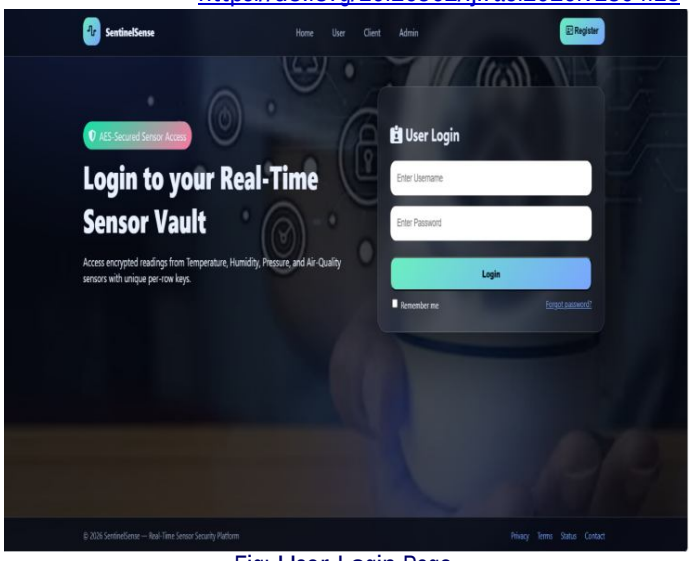

Fig: User Login Page

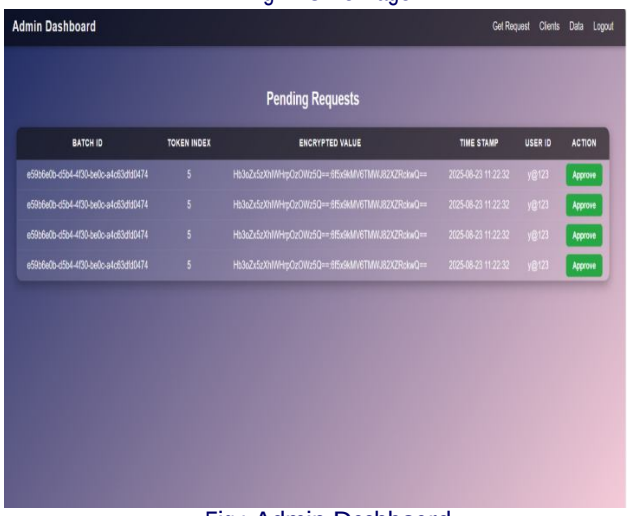

Fig.: Admin Dashboard

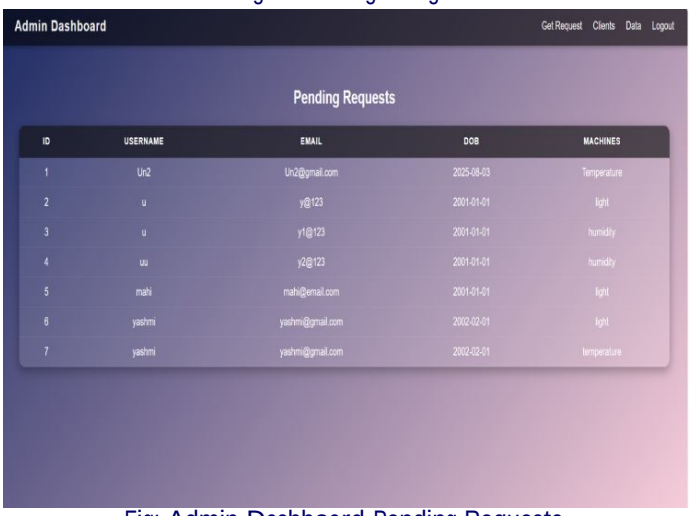

Fig: Admin Dashboard-Pending Requests

Fig: Admin Dashboard-User Details

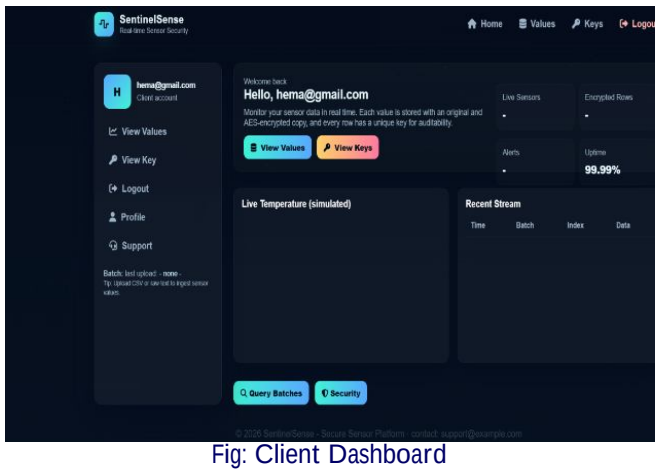

Fig: Client Dashboard

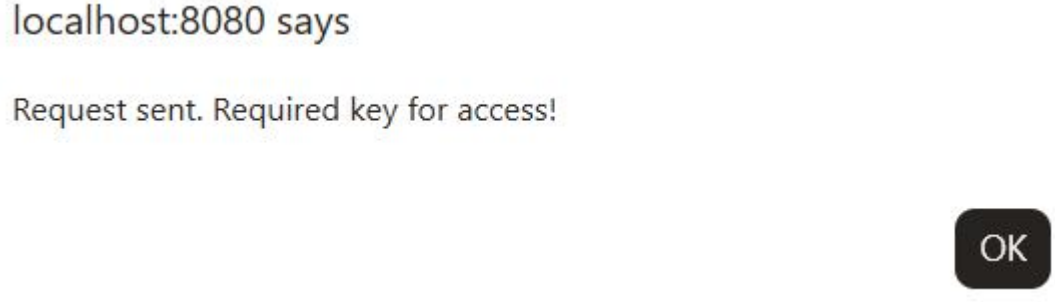

Fig: Ket Request Notification Alert

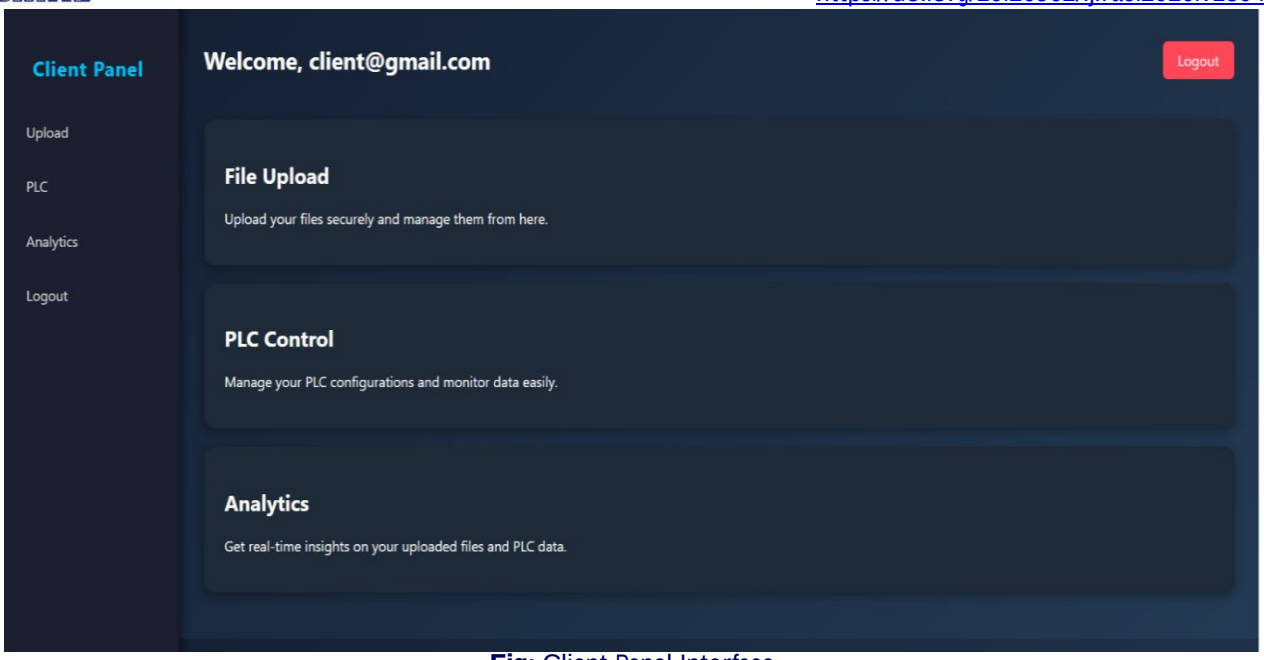

Fig: Client Panel Interface

The client panel provides options for uploading files, controlling PLC data, and viewing analytics. It is designed for ease of navigation and efficient workflow.

VII. CONCLUSION

In conclusion, the project successfully presents a secure and efficient system for managing IoT sensor data in industrial environments. By using AES encryption, the system ensures that all data is protected from unauthorized access and remains confidential even if the database is compromised. The implementation of role-based access control and admin-approved key management provides controlled and secure data access. The system also supports efficient data processing, storage, and retrieval through a user-friendly web interface. Overall, the proposed solution enhances data security, integrity, and reliability, making it a practical approach for secure data exchange in IoT-based industrial systems.

ACKNOWLEDGMENT

The authors express sincere gratitude to Mrs.SK.Pujitha, Assistant Professor, CSE Department, for her valuable guidance and continuous support. They also thank Dr.B.Santhosh Kumar, Head of the Department, for expert supervision, and the faculty members and lab technicians of the CSE Department, Guru Nanak Institute of Technology, Hyderabad, for their assistance and cooperation throughout this project.

REFERENCES

1. M.Wan, J.Li, Y.Liu, J.Zhao, and J.Wang, “Characteristic insights on industrial cyber security and popular defense mechanisms,” China Communications, vol. 18, no. 1, pp. 130–150, 2021.
2. G.Yu and T.Shon, “Security and forensic analysis for industrial Ethernet protocols,” in Proc. Int. Conf. Platform Technology and Service, 2022.
3. M.Slunjski, D.Sumina, S.Groš, and I.Erceg, “Off-the-shelf solutions as potential cyber threats to industrial environments,” IEEE Access, vol. 10, 2022.
4. R.Trifonov, G.Tsochev, S.Manolov, R.Yoshinov, and G.Pavlova, “Cyber trends in industrial control systems,” in Proc. Int. Conf. Circuits, Systems, Communications and Computers, 2021.
5. W.Deng, J.Li, H.Yan, et al., “Self-sovereign identity management in ciphertext policy attribute-based encryption for IoT,” 2024.
6. M. Slunjski and D. Sumina, “Utilising next-generation PLC capabilities for ICS protection,” 2025.
7. M.Cheminod, L.Durante, and A. Valenzano, “Review of security issues in industrial networks,” IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 277–293, 2013.
8. B.Galloway and G.P.Hancke, “Introduction to industrial control networks,” IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 860–880, 2013.
9. J.-Q.Li,F.R.Yu,G.Deng, C.Luo, Z.Ming, and Q. Yan, “Industrial internet: A survey on enabling technologies, applications, and challenges,” IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 1504–1526, 2017.
10. F.Khorrami, P.Krishnamurthy, and R. Karri, “Cybersecurity for control systems: A process-aware perspective,” IEEE Design & Test, vol. 33, no. 5, pp. 75–83, 2016.
11. K.E.Hemsley and R.E. Fisher, “History of industrial control system cyber incidents,” Idaho National Laboratory Report, 2018.