International Journal of Electrical and Electronics Engineers
Volume 18, Issue No. 01, Jan-June 2026
ISSN (0) 2321-2055 ISSN (P) 2321-2045

SECURE IOT PLATFORM FOR INDUSTRIAL CONTROL SYSTEMS

Mrs. B. Thriveni
Department of ECE
Tirumala Engineering College
Narasaraopet, India
bollavaraputhriveni1@gmail.com

Shaik Reshma
Department of ECE
Tirumala Engineering College
Narasaraopet, India
shailkreshuuu@gmail.com

NethuluriVijayKrishna
Department of ECE
Tirumala Engineering College
Narasaraopet, India
vijaynethuluri@gmail.com

Srinivasulu muthukuri
Department of ECE
Tirumala Engineering College
Narasaraopet, India
srinivasulumuthukuri2@gmail.com

***Abstract*— Secure IoT platforms play a crucial role in modern industrial environments where continuous monitoring, safety, and efficient control of industrial processes are essential. Traditional industrial control systems often face challenges related to limited remote accessibility, delayed fault detection, and potential security vulnerabilities. To address these issues, this project presents a secure Internet of Things (IoT) based platform for industrial control systems that enables reliable monitoring and management of industrial operations. The proposed system integrates sensors, actuators, and controllers to continuously collect real-time data from industrial equipment and transmit it to a centralized IoT platform using secure communication protocols. Advanced security mechanisms such as device authentication, role-based access control, secure data storage, and encrypted communication are incorporated to protect critical industrial infrastructure from unauthorized access and cyber threats.**

***Index Terms*—Automatic Question Generation (AQG), Natural Language Processing (NLP), Transformer Models, T5 Architecture, Flask API, Deep Learning, BLEU-4, ROUGE-L, METEOR, SQuAD v1.1.**

I. INTRODUCTION

Industrial Control Systems (ICS) are widely used in industries such as factories and power plants to monitor and control machines and processes [13]. In recent years, the rapid growth of the Internet of Things (IoT) has changed the way devices are connected and operated. IoT allows devices to communicate through the internet using wireless technologies like Wi-Fi, enabling real-time monitoring and control[8]. This development has improved efficiency and flexibility in industrial systems[7]. Traditionally, industrial systems operated in isolated environments with limited connectivity. However, with the integration of IoT, these systems are now connected to networks for better monitoring and automation[9]. IoT based sensors can continuously track parameters such as temperature, gas levels, and voltage[15]. While this improves system performance, it also introduces security challenges, as connected devices may be vulnerable to cyber-attacks, unauthorized access, and data breaches[2][16]. The availability of smart sensors and microcontrollers like ESP32 has made it easier to implement IoT-based monitoring systems. These technologies allow real-time data collection, processing, and transmission to cloud platforms[8]. Cloud services provide storage, analysis, and remote access to system data, helping users monitor industrial conditions from anywhere and make better decisions[10]. The motivation of this project is to develop a system. The system is designed to continuously monitor important parameters and detect abnormal conditions at an early stage. By providing timely alerts and enabling quick response, it helps in reducing production loss, preventing system failures, and improving worker safety. Security features are also included to ensure that only authorized users can access and control the system[14].

The Secure IoT-Based Industrial Control and Monitoring System is designed to improve safety, automation, and reliability in industrial environments[9]. Industries often deal with hazardous materials, heavy machinery, electrical systems, and environmental variations. Any small fault such as gas leakage, fire, voltage instability, or abnormal vibration can lead to serious accidents and financial loss[15]. This system provides a smart solution by continuously monitoring multiple parameters and responding automatically when dangerous conditions are detected. The integration of sensors with the ESP32 microcontroller and cloud platform makes the system suitable for various real-world applications in industries, warehouses, and research environments.

Gas leakage is one of the most dangerous problems in industrial areas[15], especially where LPG, methane, or other combustible gases are used. If gas accumulates in a closed environment, it can cause explosions or fire accidents. The MQ-2 gas sensor continuously monitors the gas concentration in the surrounding area. When the gas level crosses a safe limit, the system automatically activates an exhaust fan and buzzer through a relay module. This immediate response helps in reducing the risk and alerting workers in time. The gas data is also uploaded to the cloud for remote monitoring and analysis.

II. LITERATURE SURVEY

Industrial IoT Monitoring Systems play a vital role in modern industries by enabling real-time data collection, analysis, and control of industrial processes. These systems use smart sensors, embedded devices, and cloud platforms to monitor critical parameters such as temperature, gas leakage, voltage, and vibration. The primary objective is to ensure safety, improve efficiency, and reduce system failures by detecting abnormal conditions at an early stage. With the integration of IoT, industrial systems can be monitored remotely, allowing better decision-making and faster response to emergencies [10].

Traditionally, industrial monitoring was performed manually, where workers periodically checked machine conditions and environmental parameters. This method often resulted in delayed fault detection and increased chances of human error. In the proposed system, automation is achieved using an ESP32 microcontroller integrated with multiple sensors such as the MQ-2 gas sensor, flame sensor, DHT11 temperature and humidity sensor, ultrasonic sensor, and voltage sensor. These sensors continuously monitor real-time conditions and send data to the ESP32 for processing. When abnormal conditions such as gas leakage, fire, or temperature rise are detected, the system automatically activates output devices like a buzzer, exhaust fan, or water pump through a relay module. This automated approach improves accuracy, reduces response time, and ensures reliable industrial monitoring without continuous human intervention [1][2]..

To ensure effective industrial monitoring, various parameters are continuously observed using the implemented hardware setup. In this project, the important parameters include: Environmental Parameters: Temperature and humidity are measured using the DHT11 sensor to maintain safe working conditions. Safety Parameters: Gas leakage is detected using the MQ-2 sensor, and fire is detected using the flame sensor to prevent hazardous situations.

A. Treytl et al. (2005) in their work titled "Security Measures in Automation Systems" studied different security methods used in industrial automation systems. They explained how to protect automation networks from cyber attacks and unauthorized access. Their study shows that using secure communication and proper monitoring helps industries run systems safely and reliably [1].

B. A. R. Sadeghi et al. (2015) in the paper "Security and Privacy Challenges in Industrial IoT" explained the main security and privacy problems in Industrial IoT systems. They showed how connected devices can be attacked by hackers and suggested using strong authentication and encryption methods to protect important data [2].

III. METHODOLOGY

The proposed methodology focuses on developing a Secure IoT-Based Industrial Control and Monitoring System that can monitor industrial environmental parameters and automatically respond to abnormal conditions. The system is designed using an embedded controller and multiple sensors to detect hazards such as gas leakage, fire, abnormal voltage, vibration, temperature rise, and proximity issues. The system continuously collects real-time data from different sensors and processes it using a microcontroller. Based on the analyzed data, the system determines whether the operating conditions are normal or abnormal. If any abnormal condition is detected, alert mechanisms and automatic control actions are triggered to ensure industrial safety. *The entire system follows a structured process that includes sensor monitoring, data processing, abnormal condition detection, actuator control, and secure IoT monitoring. This approach enables industries to improve safety, reduce manual monitoring, and provide real-time remote monitoring through IoT technology.*

turned ON . Once the system receives power, all hardware components such as sensors, relays, display modules, and actuators are energized and prepared for operation. During this stage, the controller initializes all required modules, sets up communication interfaces, and configures input and output pins, ensuring that every hardware component connected to the system is ready to perform its designated function

Question Generation: A pre-trained T5 (Text-to-Text Transfer Transformer) or similar model takes the context and the selected keyword to synthesize a grammatically correct question.

Distractor Generation: For MCQs, the system uses Word-Net or sense-based embeddings to create plausible but incorrect options (distractors).

IV. EXECUTED RESULT

This chapter presents the experimental results and performance analysis of the proposed Secure IoT Platform for Industrial Control Systems. The system was implemented using a prototype hardware kit consisting of multiple sensors, controllers, and actuators integrated with an IoT platform . The objective of the system is to monitor industrial conditions in real time and ensure safe and reliable operation of industrial equipment. Various sensors such as temperature and humidity sensors, gas sensors, flame sensors, ultrasonic sensors, and vibration detection modules were connected to the microcontroller to collect environmental and machine-related data.

- The developed system continuously gathers data from the connected sensors and processes it through the microcontroller. The processed data is then transmitted securely to the IoT monitoring platform, where it can be observed remotely by authorized users. The platform displays the sensor readings in graphical form, allowing users to easily understand system behaviour and track changes in environmental and operational conditions over time.
-
- The obtained results show that the proposed system can effectively monitor important industrial parameters such as gas leakage, fire detection, vibration levels, and object distance. Whenever abnormal conditions are detected, the system provides alerts and activates necessary control actions through actuators. These results demonstrate that the proposed IoT-based industrial monitoring system is efficient, reliable, and capable of improving safety and monitoring in industrial environments.
- The developed kit consists of an ESP32 microcontroller, which acts as the central controller for the entire system. Several sensors are connected to the controller to monitor different industrial parameters. These include a DHT11 temperature and humidity sensor to measure environmental conditions, an MQ gas sensor to detect harmful gases or smoke, a flame sensor to identify fire

– the hardware implementation of the proposed secure IoT platform for industrial monitoring. The system is built around the ESP32 microcontroller, which acts as the central control unit, interfacing with multiple sensors such as the DHT11 temperature and humidity sensor, flame sensor, MQ gas sensor, ultrasonic sensor, and vibration detection module. These sensors continuously collect real-time data from the surrounding environment and industrial equipment, enabling the system to monitor critical parameters like temperature changes, gas leakage, fire presence, object distance, and abnormal vibrations.

The collected sensor data is processed by the microcontroller and transmitted to the IoT monitoring platform through Wi-Fi for remote visualization and analysis, allowing operators to monitor the system from any location and receive instant updates. The system also includes actuators such as a relay module, DC fan, water pump, buzzer, and LED indicator to perform automatic control actions during abnormal conditions, where the fan can be activated to reduce gas concentration, the water pump can be triggered to control fire hazards, and the buzzer and LED provide immediate local alerts. Additionally, the LCD display presents real-time sensor values

ment, specifically in the BLEU-4 score (0.58), indicating better grammatical fluency. However, it remains limited in capturing long-range de-pendencies within large instructional documents. Proposed Framework Excellence: The *Proposed T5 Transformer* architecture achieves the highest evaluation scores, with a **BLEU-4 of 0.76** and a **ROUGE-L of 0.79**. This significant margin is attributed to the self-attention mechanism, which allows the model to maintain context-awareness across the entire input text, resulting in questions that are more accurate, relevant, and indistinguish-able from human-generated assessments.

The distance graph in fig 6.2 represents the readings obtained from the ultrasonic sensor used for obstacle or object detection. From the graph, the distance value remains close to 200 cm for most of the time, which indicates that no object was present within the detection range during normal operation. At a few time instances, the graph shows a sudden drop in the distance value, reaching around 16 cm, which indicates that an object came closer to the sensor during that moment. The system successfully detected this change in distance and updated the values in the IoT monitoring platform in real time, ensuring continuous monitoring and accurate data transmission. The last recorded value is 57 cm, while the minimum value is 16 cm and the maximum value is 200 cm, which confirms that the sensor is capable of detecting objects at different distances with good accuracy. The quick

V. DISCUSSION

The Discussion section evaluates the humidity sensor used in the Secure IoT Industrial Monitoring System. The sensor continuously measures the moisture level present in the surrounding environment and transmits the collected data to the IoT monitoring platform for real-time observation. Monitoring humidity is important in industrial environments because excessive moisture can affect equipment performance and product quality. In the graph, the humidity value is recorded as 55.0%, which indicates a moderate and normal moisture level in the environment during the monitoring period, and the last recorded value shows that the humidity remained stable without major fluctuations. This result confirms that the humidity sensor is functioning properly and providing accurate real time data to the IoT platform. Continuous monitoring of humidity helps maintain suitable environmental conditions.

the Secure IoT Industrial Monitoring system, where a value of 1.00 indicates an abnormal condition based on sensor readings such as gas, temperature, or vibration, triggering alerts like buzzer, LED, or IoT notifications to reduce response time. This representation helps operators quickly identify unsafe situations and analyze trends. It also allows continuous monitoring of system performance over time, making it easier to detect recurring issues or patterns. Additionally, the graphical visualization improves decision-making by providing a clear and immediate understanding of system behaviour during critical conditions..

VI. CONCLUSION

The proposed project successfully develops a Secure IoT-Based Industrial Control and Monitoring System that enhances safety and reliability in industrial environments by employing an ESP32 microcontroller integrated with multiple sensors for continuous monitoring. The system uses gas, flame, vibration, ultrasonic distance, voltage, and temperature-humidity sensors to collect diverse environmental and operational data in real time [9], and compares these readings against predefined thresholds to detect hazardous situations such as gas leakage, fire, excessive vibration, voltage fluctuations, or unsafe distance conditions, thereby preventing potential equipment damage and industrial accidents . Upon detecting any abnormal condition, automatic control actions are executed through actuators including exhaust fans, water pumps, buzzers, motors, and LEDs operated via relay modules[15], reducing human intervention and improving response times. Real-time status and sensor readings are displayed locally on a 16×2 LCD and through audible alerts, while integration with the ThingSpeak cloud platform allows remote monitoring, historical data storage, trend analysis, and alert notifications, supporting better decision-making, predictive maintenance, and operational efficiency. Despite its effectiveness, limitations such as sensor accuracy, environmental interference, dependence on Wi-Fi, and IoT security concerns exist [2][16], which can be addressed in future work by deploying high precision sensors, secure and resilient communication protocols, robust encryption, and optimized system design, making the system more scalable, secure, and suitable for evolving industrial automation and IIoT applications[14].

The Secure IoT-Based Industrial Control and Monitoring

System developed in this project provides a strong foundation for multi-hazard industrial safety monitoring using the ESP32 microcontroller and ThingSpeak cloud platform, but there are several opportunities to enhance its performance, reliability, and intelligence in real industrial environments. Future improvements could include integrating GSM or cellular communication modules like SIM800L or SIM7600 to enable SMS or call alerts even when Wi-Fi is unavailable, and using the MQTT protocol instead of HTTP to reduce delay, minimize data usage, and support two-way communication for remote control and configuration . Upgrading the firmware to an RTOS such as FreeRTOS can further improve real-time performance by efficiently managing tasks and prioritizing critical operations, making the system more responsive and robust[3]. Additional developments could involve applying machine learning methods to detect unusual patterns and predict failures, adding sensors for current monitoring, air quality, and toxic gases to extend monitoring capabilities, and incorporating microSD-based local data storage to ensure continued operation during internet unavailability [21]. These enhancements would make the system more intelligent, reliable, and scalable, helping it better address the challenges of advanced industrial environments while supporting long-term monitoring, predictive maintenance, and improved safety for indu strialappli

REFERENCES

[1] A. Treytl, T. Sauter, and C. Schweiger, "Security measures in automation systems: Practice-oriented approach," in 2005 IEEE 10th International Conference on Emerging Technologies and Factory Automation (ETFA), 2005.

[2] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in Industrial Internet of Things," in 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015, pp. 1–6.

[3] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, "Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation," in IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 28–33, Mar. 2017.

[4] M. Antonakakis et al., "Understanding the Mirai botnet," in 2017 26th USENIX Security Symposium, 2017, pp. 1093–1110.

[5] M. Radovan and B. Golub, "Trends in IoT security," in 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017, pp. 1302–1308.

[6] H. Thapliyal, "Internet of Things-based consumer electronics: Reviewing existing consumer electronic devices, systems, and platforms and exploring new research paradigms," in IEEE Consumer Electronics Magazine, vol. 7, no. 1, pp. 66–67, Jan. 2018.

[7] B. Cheng, J. Zhang, G. P. Hancke, S. Karnouskos, and A. W. Colombo, "Industrial cyberphysical systems: Realizing cloud-based big data infrastructures," in IEEE Industrial Electronics Magazine, vol. 12, no. 1, pp. 25–35, Mar. 2018.

[8] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An analysis framework," in Computers in Industry, vol. 101, pp. 1–12, Oct. 2018.

[9] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," in IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[10] A. Griffiths, "Trends and innovations in the Industrial IoT," in Embedded Computing, Jun. 2018.

[11] L. Joris, F. Dupont, P. Laurent, P. Bellier, S. Stoukatch, and J.-M. Redouté, "An autonomous Sigfox wireless sensor node for environmental monitoring," in IEEE Sensors Letters, vol. 3, no. 7, Jul. 2019.

[12] S. Dey and A. Hossain, "Session-key establishment and authentication in a smart home network using public key cryptography," in IEEE Sensors Letters, vol. 3, no. 4. [13] J. Jasperneite, T. Sauter, and M. Wollschlaeger, "Why we need automation models: Handling complexity in Industry 4.0 and the Internet of Things," in IEEE Industrial Electronics Magazine, vol. 14, no. 1, pp. 29–40, Mar. 2020.

[14] IEC, Security for Industrial Automation and Control Systems, IEC Standard 62443, 2020.

[15] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K. K. R. Choo, "Consumer, commercial, and Industrial IoT security: Attack taxonomy and case studies," in IEEE Internet of Things Journal, vol. 9, no. 1, pp. 199–221, Jan. 2022.

[16] B. Pospisil, T. Sauter, A. Treytl, E. Huber, and W. Seböck, "Cyber security at home—What really matters to people," in 2022 IEEE 31st International Symposium on Industrial Electronics (ISIE), 2022, pp. 1208–1213.

[17] A. Treytl, A. R. Kondapuram, T. Sauter, and H. Ruotsalainen, "Comprehensive analysis of supply voltage watermarking for protection of sensor systems," in 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA), 2022, pp. 1–8.

[18] L. Vogl, T. Sauter, A. Treytl, and T. Bigler, "Side-channel watermarking for LoRaWAN using robust inter-packet timing: An experimental approach," in 2022 IEEE 18th International Conference on Factory Communication Systems (WFCS), 2022.

[19] S. Colley, "Key IoT security trends for 2023," in IoT Business News, Dec. 2022.

[20] S. Misra, C. Roy, T. Sauter, A. Mukherjee, and J. Maiti, "Industrial Internet of Things for safety management applications: A survey," in IEEE Access, vol. 10, pp. 83415–83439, 2022.

[21] E. Ragusa, F. Zonzini, L. De Marchi, and P. Gastaldo, "Vibration monitoring in the compressed domain with energy-efficient sensor networks," in IEEE Sensors Letters, vol. 7, no. 8, Aug. 2023.