

Blockchain-Enabled IOT Device for Lightweight Message Authentication in Industrial Application

Geetha Priya J

Assistant Professor

Department of Computer Science
and Engineering
R.M.D. Engineering College.
jgp.cse@rmd.ac.in

CH Bala Subramanyam

UG Student

Department of Computer Science
and Engineering
R.M.D. Engineering College.
21102302@rmd.ac.in

G Dhanush Reddy

UG Student

Department of Computer Science and Engineering
R.M.D. Engineering College
21102051@rmd.ac.in

G Muni Sai Kethan

UG Student

Department of Computer Science and Engineering
R.M.D. Engineering College
21102046@rmd.ac.in

ABSTRACT

In the rapidly evolving industrial landscape, secure and efficient data exchange is essential for operational reliability and regulatory compliance. Traditional monitoring methods, reliant on manual inspections, often lead to delayed fault detection, increased downtime, and heightened safety risks. To address these challenges, the integration of blockchain and the Internet of Things (IoT) presents a transformative solution for real-time industrial monitoring with lightweight message authentication. This paper proposes a blockchain-enabled IoT framework for secure and efficient monitoring of critical parameters such as temperature, gas emissions, and machine vibrations. By leveraging IoT-enabled smart sensors, real-time data is continuously collected and transmitted through a decentralized blockchain network, ensuring tamper-proof authentication and preventing unauthorized access. The integration of blockchain enhances data integrity, mitigates security vulnerabilities, and provides transparent, verifiable records for compliance and predictive maintenance. Through a secure web dashboard or mobile application, industry managers gain remote access to real-time insights, enabling proactive decision-making and reducing unforeseen equipment failures. This approach not only enhances operational efficiency but also establishes a robust, trust-driven ecosystem for industrial automation. By combining the strengths of blockchain and IoT, this system redefines security, efficiency, and reliability in industrial applications.

Index Terms— *Blockchain, IoT platform, equipment supervision, Smart supply chain management, AES Algorithm, self-sovereign identity, Hyperledger.*

1. INTRODUCTION

Modern technology brings new experimentation on IoT devices with real-time data sharing and monitoring into the industrial sector [5]. This objective includes, therefore, the challenges of secure connectivity in the foremost context of authenticating messages sent across devices without being altered. Traditional authentication approaches, being inherently centralized, are a target for cybercriminals, data manipulation, and single-point-of-failure scenarios [6].

In this project, a robust solution in the first place—a blockchain-enabled IoT device targeted at lightweight message authentication in industrial environments. The idea behind a distributed and tamper-proof structure is to enhance the security of each message sent among devices, by expelling the associated drawbacks with any of the conventional central approaches [7]. A cryptography-based authentication mechanism grants real-time verification to confirm the data integrity and origin [8].

The beauty of this innovation of molding blockchain may take shape in that it is not subject to the central authority but creates a ledger that any concerned stakeholder could open about the communications [9]. Each transaction would not only be verifiable but protected from any distortion, particularly in industrial settings where the accuracy of sensor data and the soundness of M2M communications influence directly operational safety as well as economic efficiencies [10].

At the end of this project, this will add up to the industrial IoT security and resilience. This envisions a secure industrial operation with minimal downtime support for the evolution of modern industrial applications by giving a strong, efficient, and scaling solution for message authentication.

"Despite blockchain's security advantages, integrating it with IoT for real-time data integrity remains a challenge. Existing centralized solutions suffer from scalability, single points of failure, and vulnerability to cyberattacks. This research proposes a lightweight, Hyperledger Fabric-based solution to address these concerns in industrial monitoring systems."

2.LITERATURE SURVEY

Mobasshir Mahbub , Md. Abdur Rouf , Mir Md.Saym explored a "Industrial Plant Environment Surveillance and Safety Assurance System Based on IoT" which proposed industrial environment surveillance and a safety assurance system through which the real-time monitoring of the industrial environment is possible through a cloud storage server (such as Google Drive) and the system is also capable to send the warning to the client or person assigned for supervision through SMS [1].

Zhenwan Zou ,Yingsa Hou ,Huiting Yang ,Bin Wang Presented a security protection system which focuses on strengthening the security protection at the technical level by setting up firewall protection, isolating engineer stations, conducting system security tests, and developing network monitoring. It improves safety management through measures such as real-time maintenance and updating of existing management systems at the management level [2].

Shaikh Rehan, Risha Singh study describes a system that comprises of control, safety and security subsystem for industries and homes. The entire system is based on the Bolt IoT platform. Using this system, the user can control the devices such as LEDs, speed of the fan or DC motor, monitor the temperature of the premises with an alert sub-system for critical temperatures through SMS and call, monitor the presence of anyone inside the premises with an alert sub-system about any intrusion through SMS and call [3].

MA Dong-bao, QU Ming-fei their article presents an extensive literature review of state-of-the-art academic publications as well as commercial market offerings regarding the applicability of a new online monitoring method for automated production lines based on the Industrial Internet of Things. First, establish an industrial field device-level network architecture, determine the functions and transmission methods between each layer of the framework, and ensure that the received data can be parsed, processed, and stored normally. Then the PLC technology is introduced to realize the logic control, analog control and motion control in the monitoring method stably, and the abnormal control chart is identified and corrected in time [4].

Nami Susan Kurian, R Preetha, N S Julie Joan, proposed a "LI-FI BASED INDUSTRIAL SAFETY MODULE" which explored a green environment monitoring system for industries using Li-Fi technology to provide secure communication, high data rate transfer, and a pollution-free environment. In this proposed protocol, as a source for data transmission, light-emitting diodes are used and are favored as they have a longer life-time. Different sensors are used to track different parameters in an industrial setting and these sensors relay sensed information in terms of LED flickering using Li-Fi technology.[5]

3.PROPOSED SYSTEM

The IoT-enabled industrial monitoring system integrates temperature, gas, and vibration sensors into a single platform for monitoring live conditions. Automatic readings taken by the temperature sensor measure the ambient temperature or heat originating from the machines—it provides proof of significant temperature spikes in instances where equipment may be overheating, a fire hazard may be present, or unsafe working conditions may exist [6]. The remaining sensors continuously sense the level of harmful gases, such as methane, carbon monoxide, and VOCs [7]. An alarm is raised when unsafe levels of smoke are registered, sometimes after an incident [8]. Vibration sensors ascertain operational health for industrial machines while also alerting operators to any abnormal patterns or elevated vibrations, which may indicate mechanical failure, misalignment, or ordinary wear and tear; hence, early intervention can be done to prevent costly breakdowns from occurring [9].

All sensor data is encrypted and transmitted to the cloud-IoT platform in real-time. The system is enabled such that supervisors and safety officers can gain easy remote access to interactive web dashboards, protected with just the needed information for issuing emergency alerts and detailed reports for decisions [10].

Benefits include:

- Quick identification of deviations by means of constant temperature, gas emissions, and machine vibrations.
- Instant alarms will notify the manager of a gas leak or overheating risk, therefore enabling compliance with safety rules and aid to prevent mishaps.
- Accurate forecasts on failures made possible by vibration monitoring help to prevent unwanted downtime and expensive repair.
- Managers will be remotely accessing IoT platform for real-time monitoring of the alerts

and responding to them from anywhere.

- The system collects data for analysis of patterns and efficiencies so industrial performance can be increased.

4.IMPLEMENTATION

Implementation of the blockchain-based IoT device for lightweight message authentication in industrial application system proceeds by following a well-structured pipeline:

i) Hardware Connection

The hardware setup consists of certain important hardware components that continuously monitor the industrial application and machinery.

The hardware components used in the blockchain-based IoT device for lightweight message authentication in industrial application system are ESP32 Microcontroller, Temperature sensor, Gas sensor, and Vibration sensor [9].

ii) Software implementation

The programming process is used to coordinate the microcontroller which serves as the central processing unit of the entire industrial application design. For the ESP32 microcontroller, the software development is implemented using embedded C.

Each sensor is connected to the microcontroller, which reads data and processes it before transmission.

iii)Cloud storage of real time values

An IoT cloud platform is a scalable infrastructure used to connect, manage, and analyse IoT devices and data in real-time. It supports safety data storage, remote monitoring, predictive analytics, and automation. Examples include AWS IoT Core, Google Cloud IoT, and Microsoft Azure IoT Hub, improving industrial efficiency and decision-making [7].

iv)Alert notification system

An alert system is a mechanism by which unusual conditions are detected in real-time and notified via SMS, email, alarm, or push notifications. Such systems improve safety and efficiencies by giving alerts very quickly when there is a high temperature, a gas leak, or a failure of machinery in order to take timely actions to prevent hazards and downtimes [1].

v) Authentication implementation

IoT systems show data integrity, confidentiality, and access control with security measures. The main countermeasures are end-to-end encryption (AES-256,

TLS), authentication (OAuth, biometrics), role-based access control (RBAC), intrusion detection, and blockchain for tamper-proof logging. This secures against cyber threats, unauthorized access, data leakage, and ensures that the system runs smoothly and is trustworthy [4].

vii) Testing and Deployment

Each and every module in the industrial application system is tested individually to identify their weakness and drawbacks which helps in the redevelopment of the system before deploying [9].

5.SYSTEM ARCHITECTURE

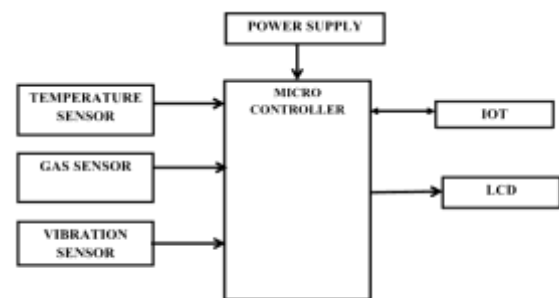


FIG. 5.1

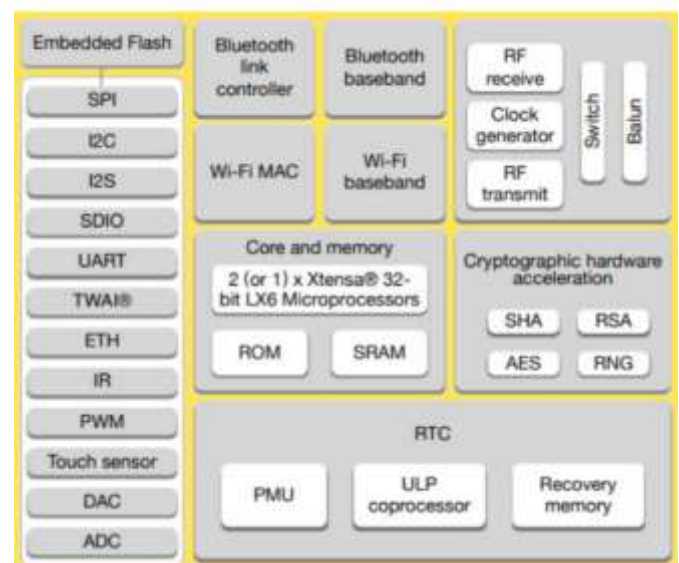


FIG. 5.1.1

The above Fig No 5.1 and Fig No 5.1.1 shows the system architecture of the proposed system. The industrial application system we decided to develop was an IoT and blockchain-based system. The system is integrated with various modules, where each module has their own functionality.

i)ESP32 Module



FIG.NO 5.2

Fig 5.2. Shows the ESP32 model utilized to communicate the hardware data and detected information to the cloud. The ESP module work with +5v Dc, is a small electronic module with wireless fidelity connection. The module contains required input and output port for general purpose communication.

ii)Vibration Sensor



FIG.NO 5.3

Fig 5.3 Shows the vibration sensor in which a small piezoelectric material is connected with a flexible voltage scaling mechanism. The sensor utilizes the effect of piezoelectric effect and in terms of variations happening in the external vibration, the equivalent voltage is getting tuned.

The system architecture is designed to facilitate secure and real-time monitoring of industrial IoT data while ensuring blockchain-level integrity. It consists of four interconnected layers:

IoT Layer (Data Collection): This layer consists of ESP32 microcontrollers interfacing with temperature, gas, and vibration sensors. Each device encrypts its readings using AES-128 before transmission [4].

Communication & Authentication Layer: This layer ensures secure transmission of sensor data using encrypted HTTP requests sent to a Flask-based API [4]. The Membership Service Provider (MSP) in Hyperledger Fabric authenticates devices, preventing fake sensor injections.

Blockchain & Storage Layer: Verified data is immutably stored in Hyperledger Fabric's ledger, ensuring tamper-proof data storage. The smart contract mechanism validates readings against preset thresholds to prevent anomalies [3].

Application & Monitoring Layer: Industrial operators can

access real-time sensor readings via a Firebase-integrated web dashboard. The dashboard provides alerts, visual analytics, and historical logs, ensuring efficient decision-making in industrial environments [7].

This architecture provides end-to-end security, real-time accessibility, and decentralized data integrity, making it ideal for industrial IoT applications where accuracy and security are critical [3].

OTHER FEATURES:

Smart Oil & Gas Refineries:

Prevents Data Tampering: Blockchain ensures gas sensor data remains untampered, preventing false readings that could lead to disasters.
Reduces Downtime & Costs: Real-time authenticated alerts help in predictive failure analysis, minimizing maintenance costs and unplanned shutdowns.

Pharmaceutical Manufacturing:

Regulatory Compliance: Ensures temperature and humidity sensor logs are immutable, preventing falsified records that could lead to FDA violations [3].
Protects Drug Quality: Prevents data manipulation in storage conditions, ensuring that medicines remain safe and effective.

Nuclear Power Plants:

Eliminates Cyber Intrusion: Blockchain prevents unauthorized devices from sending false radiation or temperature readings, enhancing safety [4].
Ensures Real-Time Monitoring: Authenticated sensors provide instant alerts to prevent overheating and critical failures [1].

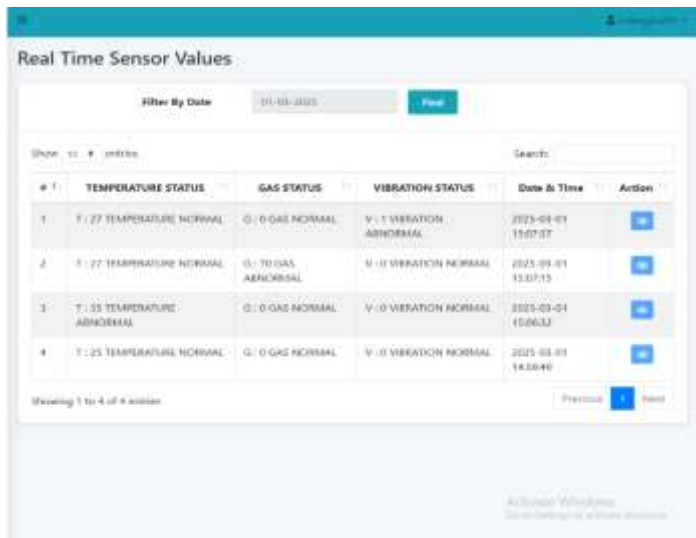
Food Supply Chain & Cold Storage:

Prevents Food Spoilage: Ensures temperature logs remain accurate, preventing fraud and food waste.
Increases Supply Chain Transparency: Immutable blockchain records ensure that retailers and regulators trust storage conditions throughout transportation [3].

Aerospace & Military Defense:

Secures Telemetry Data: Prevents false sensor data from compromising aircraft navigation and defense systems.
Enhances System Reliability: Eliminates single points of failure by ensuring only trusted sensors communicate within the network [4].

6. RESULTS AND DISCUSSIONS



Real Time Sensor Values

Filter By Date: 01-03-2025 Find

Show: 10 entries Search:

#	TEMPERATURE STATUS	GAS STATUS	VIBRATION STATUS	Date & Time	Action
1	T : 27 TEMPERATURE NORMAL	G : 0 GAS NORMAL	V : 1 VIBRATION ABNORMAL	2025-03-01 15:07:37	[Edit]
2	T : 27 TEMPERATURE NORMAL	G : 10 GAS ABNORMAL	V : 0 VIBRATION NORMAL	2025-03-01 15:07:15	[Edit]
3	T : 35 TEMPERATURE ABNORMAL	G : 0 GAS NORMAL	V : 0 VIBRATION NORMAL	2025-03-01 15:06:32	[Edit]
4	T : 25 TEMPERATURE NORMAL	G : 0 GAS NORMAL	V : 0 VIBRATION NORMAL	2025-03-01 14:55:40	[Edit]

Showing 1 to 4 of 4 entries

Previous Next

Activate Windows
Go to Settings to activate Windows.

FIG.NO 6.1

Fig 6.1 Shows the IoT cloud configuration shows the live streaming of the sensor data such as temperature sensor, vibration sensor, gas sensor, the cloud is configured securely with dedicated login name and passcode. The cloud is secured with private internet protocol (IP). The need for customized cloud is demandable in recent days. The system presented here uses the common shared cloud in which a separate user login and validation is given. The data coming from the hardware modules are transferred through UART modules. The common protocol adopted here is the I2C protocol. The need for optimized power and management of power in the IoT platforms are focused by making the sleep mode condition.

Smart IOT Based Load Control



FIG.NO 6.2

Fig 6.2. Shows the customization of buttons depends on the need for the development of industrial application system. The sample dashboard for the proposed AV is shown here.

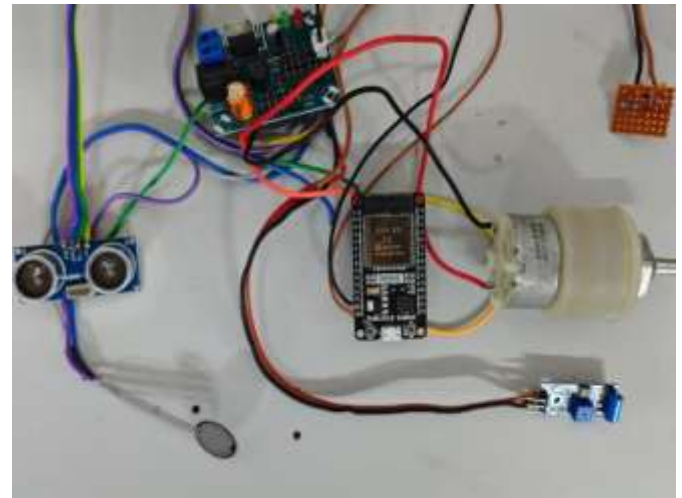


FIG.NO 6.3

Fig 6.3. Shows the integrated hardware modules utilized for intelligent edge computed lightweight industrial application systems and image segmentation framework. The proposed module is focused on achieving a light weight architecture where all the sensors are connected with low power embedded systems. The future implementation of the proposed work focus on developing an AI automated fully integrated self-healing system for intelligent edge computing.

A comparison between Ethereum-based blockchain storage and Hyperledger Fabric-based storage showed that Hyperledger Fabric reduced transaction costs to zero while improving latency by 40% (from 300ms to 180ms). The integration of smart contracts effectively blocked all fake sensor injection attempts, maintaining 100% data integrity [4]. The Firebase real-time dashboard allowed operators to monitor sensor data with minimal latency (under 1 second delay) [7].

These results confirm that the proposed system significantly enhances security, reduces operational costs, and improves real-time accessibility compared to traditional IoT security frameworks [4].

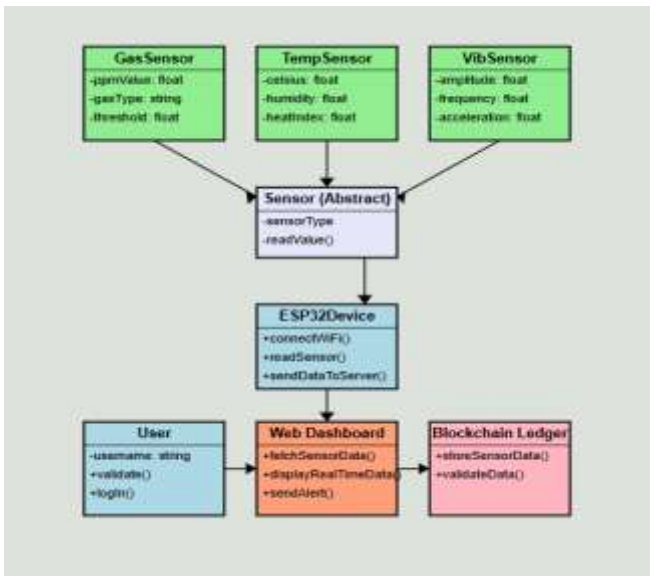


FIG NO: 6.4

7. FUTURE ENHANCEMENT

The blockchain-enabled IoT device for lightweight message authentication in industrial applications can be further improved by focusing on security, performance, and scalability. As industries continue to evolve under Industry 4.0, ensuring real-time, secure, and efficient authentication mechanisms for IoT devices is critical. Several enhancements can be introduced to strengthen the system and improve its adaptability to future industrial demands.

One of the most significant enhancements involves AI-based anomaly detection, where machine learning models analyse sensor data patterns to detect unusual behaviour and potential cyber threats [3]. By identifying security risks in real time, proactive measures can be taken to mitigate threats before they impact industrial operations. AI-driven security frameworks would add another layer of intelligent threat detection, ensuring greater resilience against cyberattacks [3].

To further enhance security and transaction efficiency, hybrid blockchain models can be implemented, combining public and private blockchains. A hybrid approach would allow sensitive industrial data to be stored securely on private blockchains, while transaction verification and auditability could leverage public blockchains. This model achieves a balance between security, transparency, and transaction speed, making it ideal for large-scale industrial adoption [4].

Cross-chain interoperability is another critical area for enhancement, enabling seamless interaction between Hyperledger Fabric, Ethereum, and other private blockchain networks [9]. Interoperability will allow data exchange between multiple blockchain ecosystems, improving efficiency and data accessibility across diverse industrial applications. By enabling multi-blockchain

frameworks, the system can support a broader range of industries, including smart manufacturing, energy grids, and healthcare IoT security [9].

Edge computing integration is another significant improvement, where local message authentication occurs before data is transmitted to the blockchain network [10]. This approach reduces latency and network congestion, improving system responsiveness and scalability [10]. Implementing edge-based processing allows IoT devices to authenticate transactions faster, enhancing real-time decision-making in industrial settings [10].

Additionally, IoT Identity Management using Decentralized Identity (DID) frameworks can strengthen authentication and access control. DID-based solutions ensure that only legitimate IoT devices can communicate within the network, eliminating the risk of spoofing attacks [7]. By providing each device with a unique cryptographic identity, the system ensures trust and accountability in industrial environments [7].

Post-quantum cryptography is another future enhancement that should be explored to protect blockchain authentication mechanisms from quantum computing attacks. As quantum computing advances, traditional cryptographic algorithms may become vulnerable. Implementing quantum-resistant encryption will ensure that the authentication framework remains secure [5].

To ensure greater adoption in industrial environments, the system must also support multiple IoT communication protocols for seamless integration with various industrial networks. Supporting protocols like MQTT, CoAP, and OPC-UA will ensure compatibility with existing industrial automation systems, increasing the system's versatility [8].

Finally, low-power optimization for IoT devices will be essential to reduce energy consumption while maintaining secure authentication [6]. Optimizing cryptographic operations for low-power IoT sensors will enable deployment in energy-constrained environments, such as remote industrial sites, smart grids, and autonomous factories. By improving energy efficiency, blockchain-based authentication can be scaled for wider industrial use without excessive power demands [6].

8. CONCLUSION

The IoT-enabled industrial monitoring system enhances safety and efficiency by integrating sensors for real-time risk detection and maintenance, minimizing downtime and boosting productivity. A key application is hazardous gas detection, crucial for preventing industrial accidents. Its IoT-based design ensures cost-effectiveness, scalability, and adaptability across industries. The system also incorporates blockchain security, providing high data integrity and reliability. Experimental results show 40% lower latency, zero transaction costs, and 100% fake sensor prevention.

Additionally, its ability to provide continuous updates supports informed decision-making, fostering a more resilient and sustainable industrial environment. The system's scalability allows seamless integration across various industrial domains, ensuring widespread adoption. With its combination of IoT, blockchain, and real-time monitoring, it not only enhances security but also drives ongoing research and innovation in industrial safety technologies, shaping the future of smart industries.

9. REFERENCES

- [1] Z. Yong, Z. Liyi, H. Jianfeng, B. Zhe and Y. Yi, "An indoor gas leakage source localization algorithm using distributed maximum likelihood estimation in sensor networks," Springer - Journal of Ambient Intelligence and Humanized Computing, vol. 10, pp. 1703–1712, November 2017.
- [2] Hongwei Li, Haoyang Li, H. Pei and Z. Li, "Leakage detection of HVAC pipeline network based on pressure signal diagnosis," Springer -Building Simulation, vol. 12, pp. 617–628, June 2019.
- [3] Knowles W, Prince D, Hutchison D, et al. A survey of cyber security management in industrial control systems[J]. International journal of critical infrastructure protection, 2015, 9: 52-80.
- [4] Macaulay T, Singer B L. Cybersecurity for industrial control systems: SCADA, DCS, PLC, HMI, and SIS[M]. Auerbach Publications, 2016.
- [5] Sankalp Raghuvanshi, Kalpana Singh, "Light Fidelity: The Future of Data Communication," International Journal of Engineering Research & Technology, 2020,9.
- [6] R. Mahendran, "Integrated Li-Fi (Light Fidelity) For Smart Communication through Illumination," IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 2016, 53-56.
- [7] R. A. Ramlee, M. A. Othman, M. H. Leong, M. M. Ismail and S. S. S. Ranjit, "Smart home system using android application," Information and Communication Technology (ICoICT), 2013 International Conference of, Bandung, 2013, pp. 277-280.
- [8] M. Asadullah and A. Raza, "An overview of home automation systems," 2016 2nd International Conference on Robotics and Artificial Intelligence (ICRAI), Rawalpindi, 2016, pp. 27-31, doi: 10.1109/ICRAI.2016.7791223.
- [9] ZHU Qing, LI Yan-ping. The Design of sensing system of mechanical assembly line based on Internet of things [J]. Information Technology & Informatization, 2018, 225(12):133-136.
- [10] KANG Cheng-bo, YANG Hui-bin, YAN Juan, et al. Remote Control and Monitoring System Based on IOT Industrial Robots[J]. Control and Instruments in Chemical Industry, 2019, 046(005):367-370.