# Access Control in IoT using Hyperledger Fabrics Blockchain for Temperature, Humidity, and Pressure

Mohamad Nur Hidayat Zarkia @ Zakaria[1], Sahnius Usman[2]

[1]*Faculty of Artificial Intelligence*

[2]*Malaysia-Japan International Institute of Technology*

[1]*mohamadnurhidayat@graduate.utm.my,* [2]*sahnius.kl@utm.my*

**Article history**

Received:
15 October 2025

Received in revised form:
28 October 2025

Accepted:
15 November 2025

Published online:
26 December 2025

*Corresponding author
mohamadnurhidayat
@graduate.utm.my

***Abstract***

*IoT system is widely used in industry and gives many benefits to the user. It helps a lot with monitoring and provides real-time information from sensors to the main node. While the IoT brings benefit, it also has its risks, vulnerabilities, and weaknesses. Based on these flaws, it can potentially be manipulated by the hackers to access and deny the services of the IoT system. Having access control through Hyperledger Fabrics Blockchain, it provides a permission blockchain framework that allows only registered devices or sensors to communicate and store the sensor data, which is temperature, humidity, and pressure. This paper will describe generally the integration of IoT using Sense Hat emulator and Hyperledger Fabrics Blockchain setup to show only the legitimate sensors are allowed to be stored in the ledger. In this study, it shows that access control can be managed using blockchain, especially for IoT, which have lacks resources to manage the traditional access control.*

***Keywords:*** *Access Control, IoT, Blockchain, IoT-Blockchain, Smart Contract, Hyperledger Fabrics*

## 1. Introduction

The advancement of technology has transformed our lifestyle, enabling us to communicate and interact with it more effectively. The Internet of Things (IoT) can provide information widely through sensors or actuators, enabling real-time data acquisition from various sensors deployed across multiple domains. This capability can monitor parameters such as temperature, humidity, and pressure etc., while enhancing operational efficiency, supporting decision-making processes, and ensuring environmental compliance in both industrial and urban settings. In Industrial Revolution 4.0, technology evolved into more sophisticated technology and a cyber-physical system. IoT has given benefits to humans in monitoring many aspects, such as health, security, etc. According to Kokila & Reddy K, (2025), IoT is a combination of a few technologies, such as Machine-to-Machine (M2M), Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), and Supervisory Control and Data Acquisition (SCADA), which consist of technology domains (big data analytics, cloud computing, and embedded devices) that enable the development of IoT applications.

* *Corresponding author. mohamadnurhidayat@graduate.utm.my*

Although IoT systems give many benefits, the system also faces several challenges to protect data security and integrity, where the increasing number of interconnected devices makes the threat harder to detect. As sensor-generated data are transmitted over networks to centralized or distributed databases, vulnerabilities may be exploited by malicious actors. This exposure required robust security mechanisms that guarantee the authenticity and immutability of recorded data. Riabi Imen et al. (2019) mentions the limitation of IoT in terms of CPU, memory, and battery lifetime, which require a lightweight access control solution with low latency. In another research, Bagga et. al., (2022) Dolev Yao's threat model recognized an adversary capable of modifying any messages that are communicated between the IoT environment. The attack can be potentially from a false data injection attack by injecting false data into the network, by compromising sensor nodes, or introducing malicious sensors (Ferrag et al., 2020). The intruder also potentially brings in fake devices to increase network load. Because of the scalability of IoT, it can be deployed with new malicious devices or sensors to harm the integrity of the network, then provide malicious activities such as accessing sensitive information without permission. This can lead to information being manipulated, resources being used more than it should be, and decisions being misleading, especially in the critical industries.

Access control can be defined as allowing activities of the registered users for every attempt by a user to access the system (Hu, 2022). The aim is to protect the system from unauthorized user access. Traditionally, access control that is being used, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), is inefficient when implemented in the IoT system due to security concerns and computational constraints; hence, it requires IoT to be complemented with other security features and blockchain technologies (Zhang et al., 2020).

In this context, blockchain technology focusing on Hyperledger Fabrics is a permissioned blockchain framework that offers a promising solution. Hyperledger Fabric's blockchain is a private permissioned blockchain, which is defined by Lee et al., (2023), as the network is controlled by a unique group of one or several owners who determine the participants in the consensus mechanism. Only selected can read or write to the blockchain. It is designed for enterprise use where the participants are trusted and can support various business applications. Hyperledger Fabrics provides a distributed ledger system where every transaction is cryptographically secured and recorded in an immutable format, thus ensuring transparency and traceability. It offers decentralized solutions that enhance auditability, privacy, scalability, and eliminate a single point of failure (SPOF). The advantages of employing blockchain for data security, traceability, and integrity are substantial. By using and implementing the Hyperledger Fabric blockchain, it is possible to integrate a system where every piece of sensor data is securely recorded, thereby minimizing the risk of tampering and providing an auditable history of all transactions. Blockchain can also strengthen the zero-trust security model by providing a decentralized network, immutable record, smart contracts, fine-grained access controls, self-sovereign identity management, reputation-based trust models, and micro-segmentation (Nie et al., 2025).

In recent decades, the rapid evolution of sensor technology and wireless communication has changed the way data is collected and processed. The IoT plays an integral role in this transformation, enabling devices to collect and transmit data automatically. In applications ranging from environmental monitoring and smart agriculture to industrial automation and urban planning, sensors are deployed to capture critical data parameters such as temperature, humidity, and pressure. However, as the volume of data grows and these systems become increasingly interconnected, the risks associated with data manipulation, unauthorized access, and cyberattacks are also threatening the user in terms of security and privacy issues.

Parallel to the evolution of IoT, blockchain technology has also emerged as an innovative solution for ensuring data integrity and security. Unlike traditional databases, blockchain operates as a decentralized ledger that stores transactions in a series of immutable blocks, ensuring that recorded information cannot be altered without detection. Hyperledger Fabrics is a notable blockchain framework that offers a permissioned environment where participants are authenticated, thereby providing enhanced security features such as confidential transactions, customizable consensus mechanisms, and detailed audit trails.

The significance of using Hyperledger Fabrics blockchain in this research, where it operates in a permissioned environment where participants are known and trusted. By having modular architecture, it allows for customizable consensus algorithms and supports plug-and-play components, making it adaptable to various use cases. It also provides high throughput and effective performance, which is designed to handle large numbers of transactions efficiently and concurrently. By having smart contracts, researchers can propose ABAC and a blockchain framework by filtering the devices, access, and policy contracts (Zhang et al., 2020). In this research, the ABAC was used to filter based on the registered and unregistered devices. According to Hu, 2022), Hyperledger Fabrics blockchain offers a flexible policy which enforces the smart contracts. The access control that is manageable by the blockchain-based access control model can be categorized into two types, which are Transaction Based Access Control (Transaction BAC) and Smart Contract Based Access Control (Smart Contract BAC). Transaction BAC used blockchain transaction to manage access token while Smart Contract BAC employs smart contract to evaluate access request and generate access token.

This background discussion focuses on the rationale for combining IoT with Hyperledger Fabrics blockchain. It provides complementary strengths of each technology, such as real-time data acquisition, while blockchain ensures the reliability and security of that data. Such an integrated system can significantly enhance the operational reliability of environmental monitoring applications and serve as a blueprint for future implementations in areas requiring high levels of data integrity and cybersecurity.

The objective of this research is to develop an IoT prototype using Sense Hat emulator capable of generating traffic and sensor flow environmental parameters such as temperature, humidity, and pressure, with the access control using Hyperledger Fabrics Blockchain framework to verify only registered sensors are allowed using a smart contract.

This introduction section presents the context and motivations of this research. Then the explanation of the technical background of the technologies involved clearly states the significance of the project intends to solve, outline the methodology adopted, discuss the results and discussion encountered, and finally conclude with a summary of the findings of this research.

## 2. Methodology

The process of the IoT using Hyperledger Fabrics blockchain simulation can be shown in Figure 1. The figure describes the simulation of the sensor by having Hyperledger Fabrics blockchain as a framework to filter the legitimate user based on the access control. It is important to register the sensor first before allowing the information from the sensor to be stored in the blockchain.

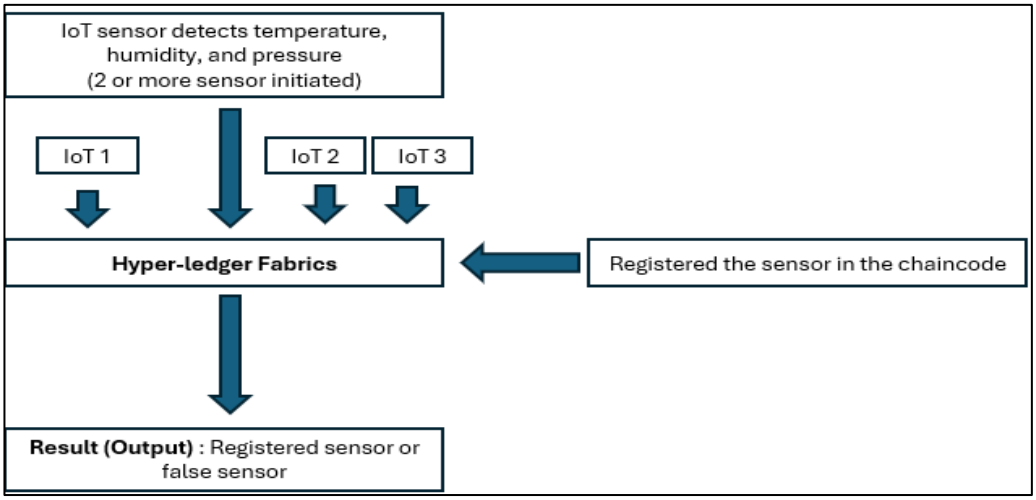


**Figure 1. IoT using Hyperledger Fabrics Blockchain Access Control Process**

## 2.1. Project Architecture Concept

The IoT will initially have its attribute ID by default in the respective embedded devices. To simulate it, the sensor ID can be inserted manually in the source code to give ID to the 2 or more devices in the sense_hat_data.py. The source code to initiate or declare the sensor can be shown in Figure 2. The registered process is done and stored inside the blockchain in an array, formed and can be verified before the process takes place. According to the (Wang, n.d.), many solutions implement access policies and ABAC through the smart contract and the blockchain itself. The Hyperledger Fabrics blockchain filtered the only registered ID to be stored in the log files, while unregistered IoT devices will not send the sensors output to the log files and will be determined as a false sensor.

```
# ✅ List of manually registered sensors (Only these will send data)
REGISTERED_SENSORS = ["Sensor01", "Sensor03", "Sensor02"]
```

**Figure 2. Code to initiate the Sensors**

The integration of IoT technology with blockchain security allows only registered sensors to write data, effectively blocking unauthorized sensors from storing information. This approach helps prevent any injection of fake or malicious data, providing access control to authorize the sensor. By having immutable data storage, the system keeps a record of sensor ID registrations; once this data is stored, it cannot be modified. Furthermore, it ensures tamper-proof records of sensor activities. Additionally, blockchain provides decentralized verification by having multiple nodes that confirm sensor transactions, thereby eliminating SPOF. The blockchain also maintains an audit trail and ensures compliance by keeping a transparent history of all sensor transactions. This setup is particularly useful for industries that require compliance, such as food storage and supply chain monitoring. Figure 3 shows the real process flow of the IoT system using Hyperledger Fabrics Blockchain which shows only the real concept for overall flow of the data. However, in this research is covered only for simulation of the sensor using Sense Hat emulator to be integrate with the Hyperledger Fabrics Blockchain.

In a real case, the sensor will be located at a suitable location to collect the required data using a protocol to communicate with the cloud server or IoT devices. Then, the access control will be managed by the Hyperledger Fabrics blockchain framework through the smart contract, which means that the researcher implementing the chaincode using the Java language. The transaction will be endorsed by the smart contract through the endorser, and it will be stored in a digital ledger to both Org 1 Peer and Org 2 Peer. Orderer then arranges the ordering of sequences, then creates a new block to be delivered.

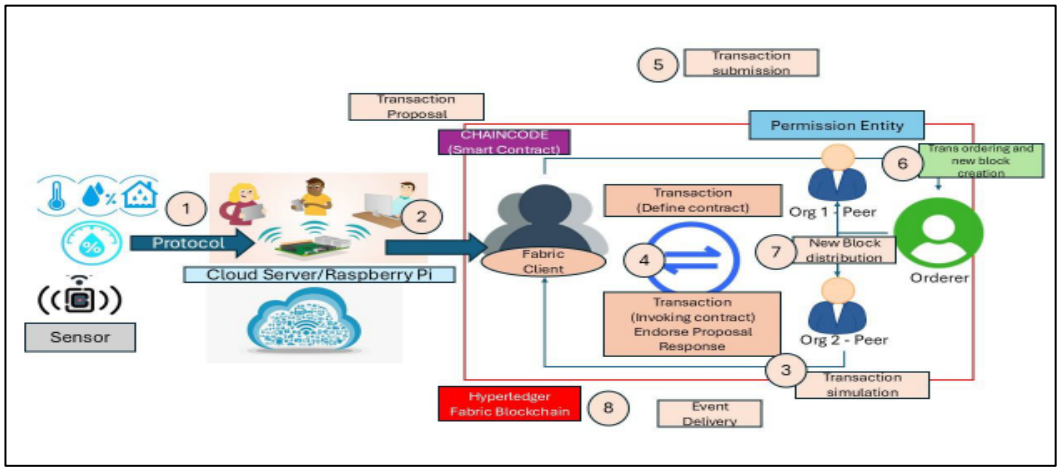


**Figure 3. Process Flow of IoT system using Hyperledger Fabrics Blockchain**

## 2.2. Setup Consideration

The IoT setup inside the Ubuntu 22.04.5 LTS environment required the proper setup of the environment itself. The project uses the virtual environment to simulate the IoT devices using the Sense Hat emulator. The setup requires Hyperledger Fabrics blockchain to be set up inside the environment. It simulates IoT data collection processes which generate temperature, humidity, and pressure. The sensor needs to be registered through the smart contract first to allow the data to be stored in an array and produce the output into the log files.

The setup of the Hyperledger Fabrics Blockchain framework environment can be configured generally using the steps below:

Set up the repositories: Update the apt package index and install packages to allow apt to use a repository over HTTPS.

a. Add Dockers official GPG key: The repository is created using the Docker pane.
b. Install Docker: Update the apt package index. Install Docker Engine, container, and Docker Compose. To identify what packages you have installed.
c. Verify installation: The verification is done for the Docker installation.
d. Install Fabric Sample and verify installation.
e. Copy the fabrics samples into the respective FOLDER. Give fabrics samples FOLDER root access.
f. Up Network, create channels and Certificate Authorities (CA). Start at this step when the initial step has been done previously.
g. Deploy chaincode. The language that the researcher uses is Java language.
h. Invoke chaincode.
i. Set the network down when the blockchain is not in use or terminates.

## 2.3 Implementation

In this prototype data is collected using the Sense HAT emulator sensor every 5 second interval. The sensor is registered first in the blockchain to ensure the endorser can acknowledge, thus sending the related data to the orderer and peer FOLDER. Figure 4 shows the IoT ID is registered in the blockchain ledger in the peer and the orderer.

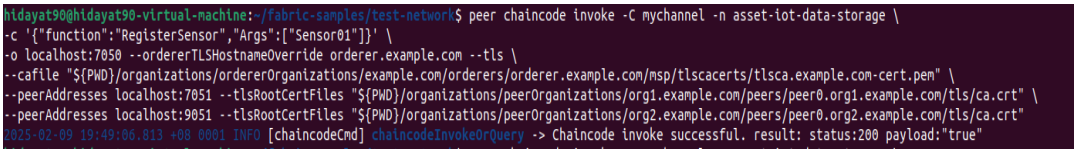


**Figure 4. IoT ID is registered in the blockchain ledger in the peer and the orderer**

Then the temperature, humidity, and pressure data are inserted inside the same folder. Figure 5 shows the IoT data is inserted in the blockchain ledger in the peer and the orderer.

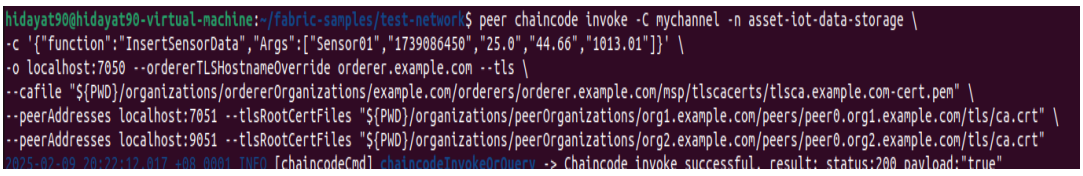


**Figure 5. IoT data is inserted in the blockchain ledger in the peer and the orderer**

After that, invoke the registered sensors, which sensor 1 has already registered in the CA.CERT files. It will show all the sensors that have been registered. Figure 6 shows the sensors that are successfully registered inside the blockchain.

```
hidayat90@hidayat90-virtual-machine:~/fabric-samples/test-network$ peer chaincode query -C mychannel -n asset-iot-data-storage \
-c '{"function":"GetRegisteredSensors","Args":[]}' \
--tls \
--cafile "${PWD}/organizations/ordererOrganizations/example.com/orderers/orderer.example.com/msp/tlscacerts/tlsca.example.com-cert.pem" \
--peerAddresses localhost:9051 \
--tlsRootCertFiles "${PWD}/organizations/peerOrganizations/org2.example.com/peers/peer0.org2.example.com/tls/ca.crt"
["Sensor01"]
```

**Figure 6. Invoke registered sensors**

## 3. Result and Discussion

The integration of the IoT prototype with Hyperledger Fabrics blockchain has demonstrated promising results in terms of data integrity, security, and real-time performance. The system was deployed in a simulated environment where it continuously transmitted data on temperature, humidity, and pressure to the blockchain network. Preliminary tests indicate that the blockchain component effectively secured each transaction, and only the trusted sensor is allowed to store the data in the blockchain network. In addition, the modular architecture of the system facilitates scalability, enabling future expansions where larger sensor networks and higher data volumes can be accommodated without compromising system performance. Figure 7 shows the sense hat emulator that is used in this experiment as IoT sensor. Figure 8 shows the integration of how the sensor and the Hyperledger Fabrics blockchain flow. The data collection below shows the Sensor01 is only verified and stored in the array, which is shown in Figure 9. The other sensors like Sensor03 and Sensor02 are rejected by the smart contract because the sensors are not registered yet inside the digital ledger through Hyperledger Fabrics blockchain. This sensor is known as a fake sensor that tries to access the network by injecting false data.

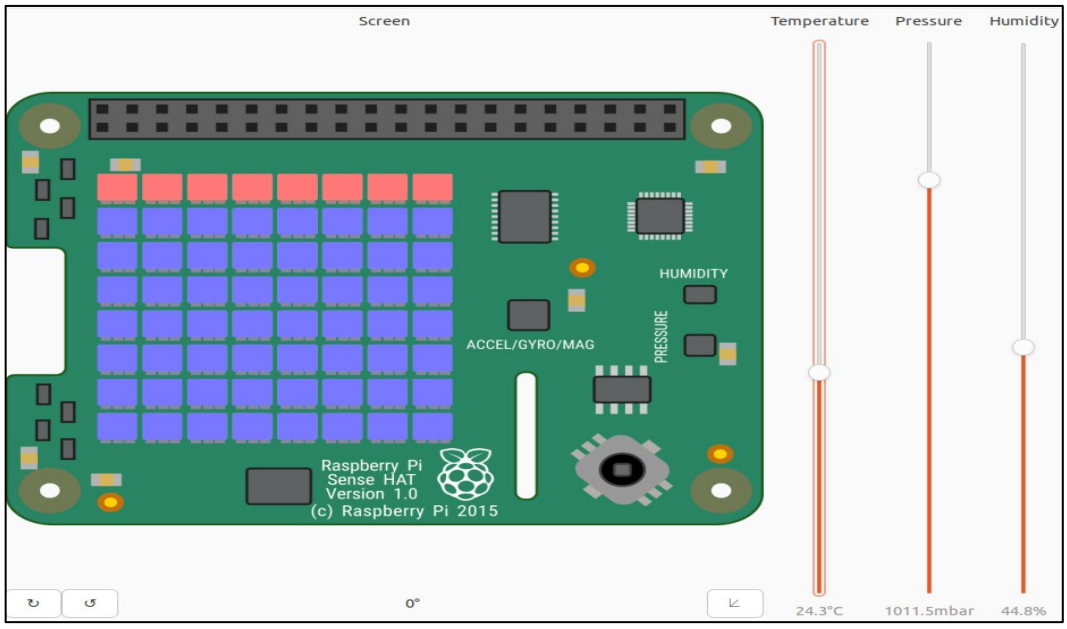


**Figure 7. IoT Sense Hat Emulator**

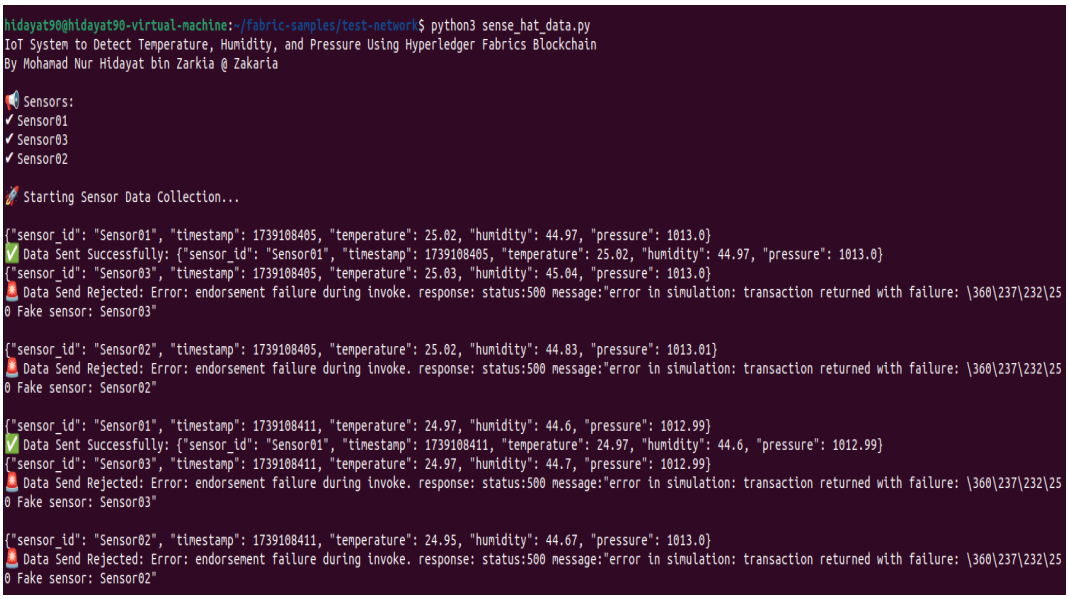


**Figure 8. IoT Code execution**

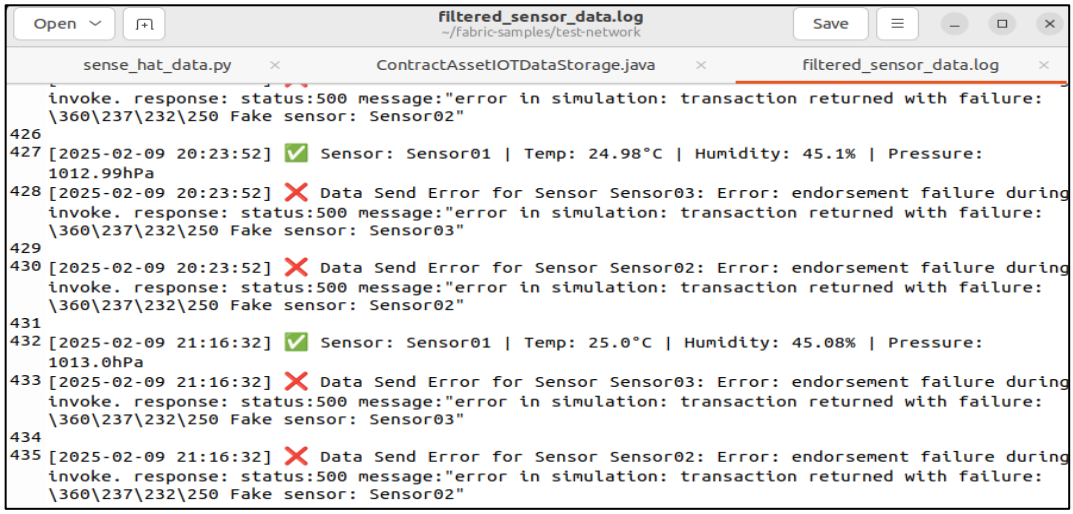


**Figure 9. IoT Detection Access Control Using Hyperledger Fabrics blockchain log files**

## 4. Conclusion

In conclusion, this project has successfully developed and demonstrated the feasibility of integrating by simulating an IoT system using Sense Hat emulator with Hyperledger Fabrics to detect and record environmental parameters such as temperature, humidity, and pressure. The integration provides a secure, immutable, and transparent data management system that addresses the critical issues of data integrity and cybersecurity inherent in traditional IoT deployments. By combining simulation from sensor data acquisition with the blockchain, the project lays a solid foundation for future applications in various sectors where data security and accuracy are important. The experimental and the result can be extended and adapted to other domains, thereby contributing to secure, decentralized data management in the era of digital transformation.

## Acknowledgement

The authors acknowledge Universiti Teknologi Malaysia (UTM), Kuala Lumpur campus, for providing guidance, support, and facilities to enable the completion of this paper.

## Conflicts of Interest

The author declares that there is no conflict of interest regarding the publication of this paper.

## References

[1] Bagga, P., Das, A. K., Chamola, V., & Guizani, M. (2022). Blockchain-envisioned access control for internet of things applications: a comprehensive survey and future directions. In *Telecommunication Systems* (Vol. 81, Issue 1, pp. 125–173). Springer. https://doi.org/10.1007/s11235-022-00938-7

[2] Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and Privacy for Green IoT-Based Agriculture: Review, Blockchain Solutions, and Challenges. In *IEEE Access* (Vol. 8, pp. 32031–32053). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2020.2973178

[3] Hu, V. C. (2022). *NIST IR 8403 - Blockchain for access control systems*. https://doi.org/10.6028/NIST.IR.8403

[4] Kokila, M., & Reddy K, S. (2025). Authentication, access control and scalability models in Internet of Things Security–A review. In *Cyber Security and Applications* (Vol. 3). KeAi Communications Co. https://doi.org/10.1016/j.csa.2024.100057

[5] Lee, J. Y., Kim, M. H., Park, K. S., Noh, S. K., Bisht, A., Das, A. K., & Park, Y. (2023). Blockchain-Based Data Access Control and Key Agreement System in IoT Environment. *Sensors*, *23*(11). https://doi.org/10.3390/s23115173

[6] Nie, S., Ren, J., Wu, R., Han, P., Han, Z., & Wan, W. (2025). Zero-Trust Access Control Mechanism Based on Blockchain and Inner-Product Encryption in the Internet of Things in a 6G Environment. *Sensors*, *25*(2). https://doi.org/10.3390/s25020550

[7] Riabi Imen, H. K. B. A. L. A. S. (2019). *A survey on Blockchain based access control for Internet of Things*. IEEE.

[8] Wang, G. (n.d.). *SoK: Applying Blockchain Technology in Industrial Internet of Things*.

[9] Zhang, Y., Memariani, A., & Bidikar, N. (2020). A Review on Blockchain-based Access Control Models in IoT Applications. *IEEE International Conference on Control and Automation, ICCA*, *2020-October*, 671–676. https://doi.org/10.1109/ICCA51439.2020.9264499