IPFS (InterPlanetary File System) A new Frontier for Next-Gen IoT Communication

PROJECT BY:

MANOJ KUMAR T

211121101603

DEPARTMENT OF IT

GUIDED BY:

Mr.N.JEYSANKAR

DEPARTMENT OF IT

CO-ORDINATED BY:

Dr.M.KIRUTHIGA DEVI

DEPARTMENT OF IT

ABSTRACT

The Internet of Things (IoT) has witnessed an exponential growth in recent years, with billions of interconnected devices generating massive amounts of data. Traditional centralized approaches to IoT communication, relying on cloud-based platforms and centralized servers, have faced challenges in terms of scalability, security, and privacy. To address these limitations, this paper explores the potential of the InterPlanetary File System (IPFS) as a decentralized and secure solution for IoT communication. IPFS is a distributed file system that utilizes content-addressing and peer-to-peer networking to create a robust and resilient infrastructure for data storage and sharing. By leveraging IPFS, IoT devices can establish direct communication channels, eliminating the need for intermediaries and reducing the risk of single points of failure. Moreover, IPFS provides a decentralized storage mechanism that ensures data integrity and prevents tampering. This paper presents a comprehensive overview of IPFS and its key features, highlighting its suitability for IoT communication. By leveraging IPFS, IoT systems can become more resilient, secure, and scalable, paving the way for a more decentralized and interconnected future.

Introduction of the project

- It's an open source project on a mission to develop a distributed IOT system. It feels like BitTorrent + Git smashed together to allow anyone running the IPFS daemon to access each other's files in a peer-to-peer (P2P) fashion.
- Pubsub basically lets you "subscribe" to a channel or topic allowing you to receive messages from other devices that "publish" messages to that same channel or topic.
- Just as easily automate the toggling of this LED to fully complete automated decentralised manufacturing factory

Scope of the Project

- Develop a scalable and efficient IoT data management system using IPFS.
- Ensure secure and reliable storage of IoT data.
- Enable seamless data sharing and analysis between IoT devices.
- Provide a decentralized and privacy-preserving solution for IoT applications.

SDG GOALS

The Sustainable Development Goals (SDGs) that support this project based on the circular provided are:

Goal 9: Industry, Innovation, and Infrastructure
The project aligns with this goal by incorporating IoT and blockchain technologies, which promote technological innovation in data management for home automation and industry systems.

Goal 11: Sustainable Cities and Communities
By using IoT and blockchain, the project supports the development of sustainable urban solutions, improving home automation and resource management, contributing to smarter, more efficient cities.

Goal 12: Responsible Consumption and Production
The system allows for better data tracking and efficient use of resources, contributing to responsible consumption patterns by optimizing home automation through decentralized systems.

These goals highlight the project's contribution to sustainable development by focusing on innovation, resource efficiency, and technological advancements to create more sustainable and smarter systems.

TABLE RELATED TO CORE SUBJECTS

SUBJECTS	DESCRIPTION
INTERNET OF THINGS (7TH SEM / IV YEAR)	This subject covers the vision of IoT from a global context, the use of devices and gateways in IoT, and real-world design constraints. It provides foundational knowledge on IoT architecture and application, critical for understanding how IoT devices interact in a smart home automation system.
DATA MINING AND DATA WAREHOUSING (6TH SEM / III YEAR)	This subject explores data management techniques, including data mining solutions that are important for processing large data streams generated by IoT devices. It includes techniques for handling and analyzing sensor data efficiently.
CLOUD TECHNOLOGY (7th SEM / IV YEAR)	Cloud computing fundamentals, typically covered in courses like Cloud Computing Architecture, help in understanding centralized storage models, which IPFS seeks to replace with decentralized alternatives.
WEB TECHNOLOGY (6TH SEM / III YEAR)	This is relevant for developing the web interface for your home automation system, allowing users to control and monitor IoT devices remotely.
MICROPROCESSOR AND MICROCONTROLLER (4TH SEM / II YEAR)	It's crucial for the hardware and signal processing aspects of your IoT system, helping you understand how the devices work at a low level, which is foundational for home automation projects.

Literature Survey

S.NO	AUTHOR	TITLE	DESCRIPTION	ADVANTAGES	YEAR
1	Xiaochen Zheng, Jinzhi Lu, Shengjing Sun, Dimitris Kiritsis	Decentralized Industrial IoT Data Management Based on Blockchain and IPFS	This paper discusses a decentralized system designed for managing industrial IoT data using a combination of Blockchain and IPFS technologies. It focuses on data integration and secure sharing in industrial environments, addressing issues like scalability, privacy, and storage of large datasets.	The integration of Blockchain and IPFS ensures data security, immutability, and efficient storage. It provides a decentralized system with enhanced privacy controls and removes single-point failures, making it highly tamper-resistant. The system also supports different privacy modes, which is beneficial in securing sensitive industrial data	Jun-23
2	HAYA R. HASAN,RAJA JAYARAMAN,KHALED SALAH, IBRAR YAQOOB,SASA PESIC,ANDMOHAMMED OMAR	Trustworthy IoT Data Streaming Using Blockchain and IPFS	This study explores the implementation of Blockchain and IPFS for trustworthy IoT data streaming. It highlights how Blockchain's immutable ledger can ensure the integrity and authenticity of IoT data streams, while IPFS provides a decentralized method for handling large volumes of data efficiently.	By using Blockchain, the system ensures data integrity and trustworthiness. IPFS adds the advantage of decentralized storage, avoiding reliance on a single server, thus enhancing scalability and reducing the risk of data tampering	Feb-22
3	Waseem Khan,Gargi Kum	Integrating IoT with Health Record Management System using IPFS and Blockchain	This paper focuses on leveraging Blockchain and IPFS to secure health record management systems (HRMS). By integrating these technologies, the paper addresses challenges related to privacy, data sharing, and management within the healthcare industry.	The combination of Blockchain and IPFS offers improved privacy and security for patient data. It ensures secure sharing of health records between healthcare providers while maintaining a decentralized and tamper-resistant system.	Mar-22

Existing Work

- Centralized Data Storage:
- Security and Privacy Concerns:
- Inefficient Data Management:

Proposed Work

- Decentralized Data Storage
- Secure and Immutable Data
- Efficient Data Management

Problem Statement

Current Challenges in Traditional IoT Systems:

- Single Points of Failure
- Data Privacy Concerns
- Scalability Limitations

Requirement Analysis

SOFTWARE REQUIRMENT:

- WINDOWS/LINUX
- IDE EDITOR
- IPFS DESKTOP
- COMMAND SHELL

HARDWARE REQUIRMENT:

- MICROPROCESSOR (Rpi,ESP32,Arduino UNO)
- SENSORS
- ACTUATORS
- POWER PACK

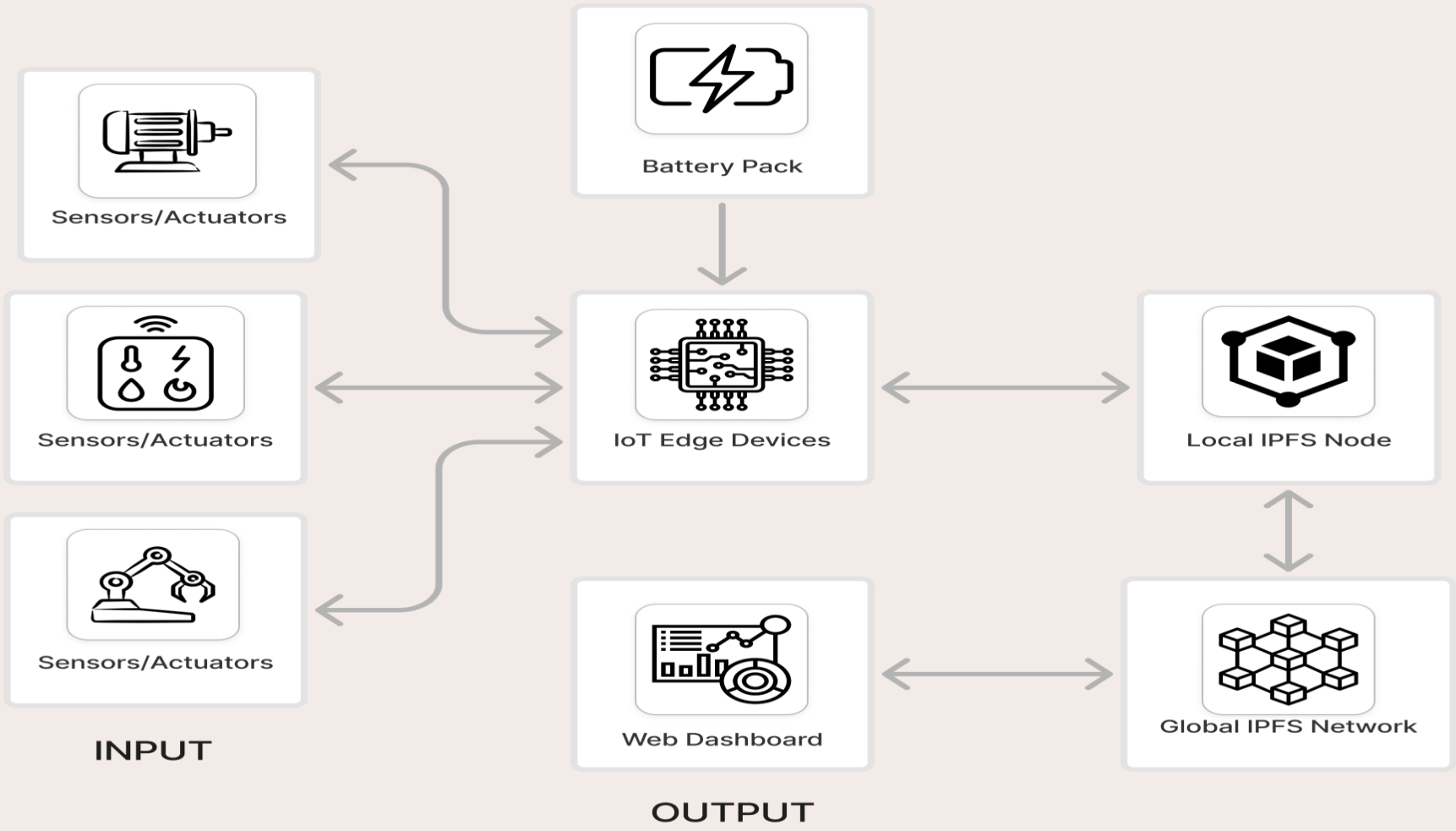
Feasibility Study

- Technical Feasibility: Most microcontrollers (e.g., Arduino, Raspberry Pi, ESP8266/ESP32) can be easily programmed to interface with serial communication for receiving commands. Local IPFS Node: Running a local IPFS node on a computer is technically feasible with minimal resource requirements. IPFS has mature libraries for Python, making it easy to interact with the network.

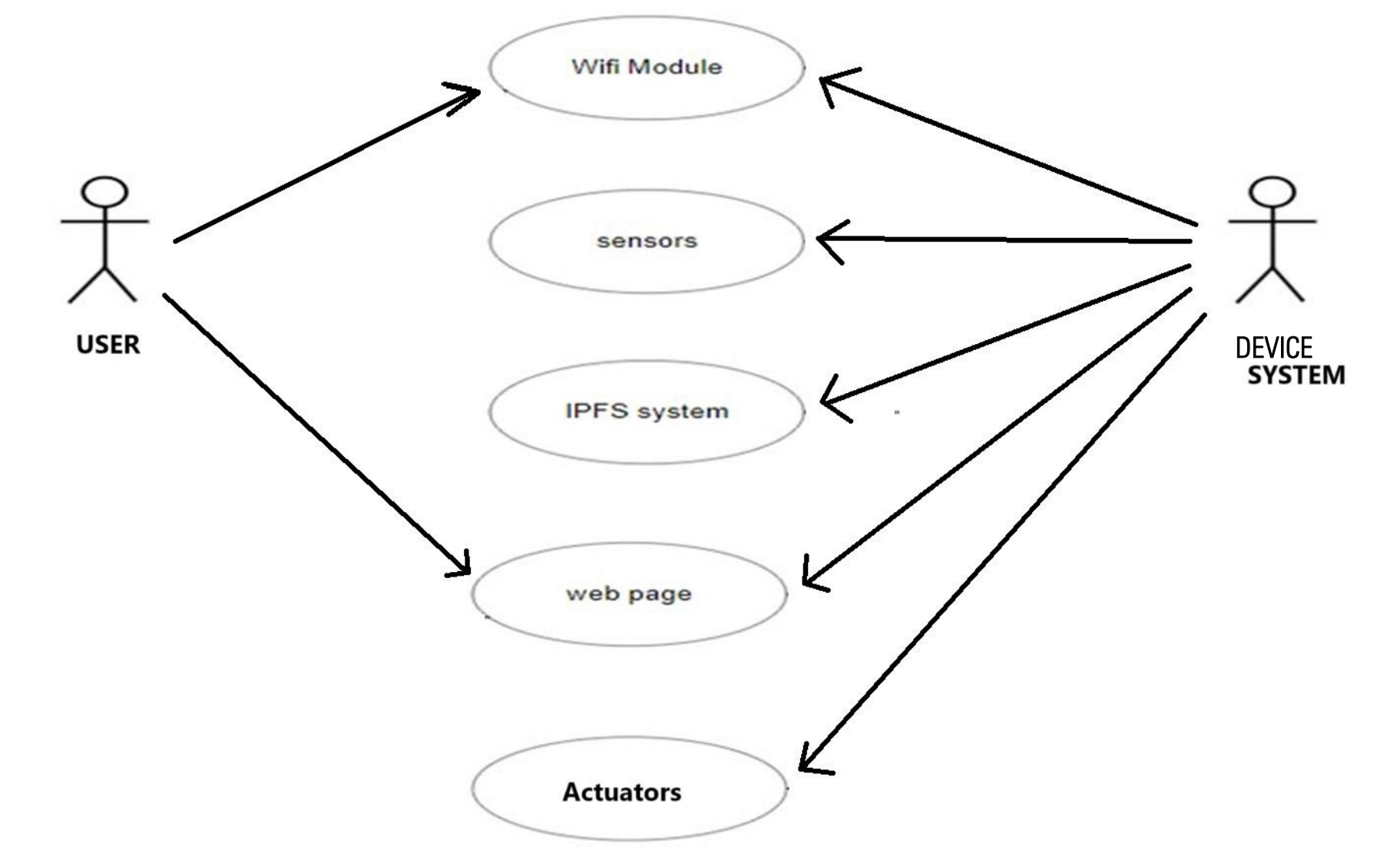
- Operational Feasibility: The system requires regular monitoring to ensure the IPFS node is running and the microcontroller is functioning correctly. The project can be implemented with minimal setup. The most time-consuming part may be setting up the IPFS node and ensuring it communicates effectively with the microcontroller.

- Economic Feasibility: The project is technically and economically feasible with minimal costs and development time. It provides a valuable learning experience in combining IoT with decentralized technologies like IPFS.

Architecture Diagram

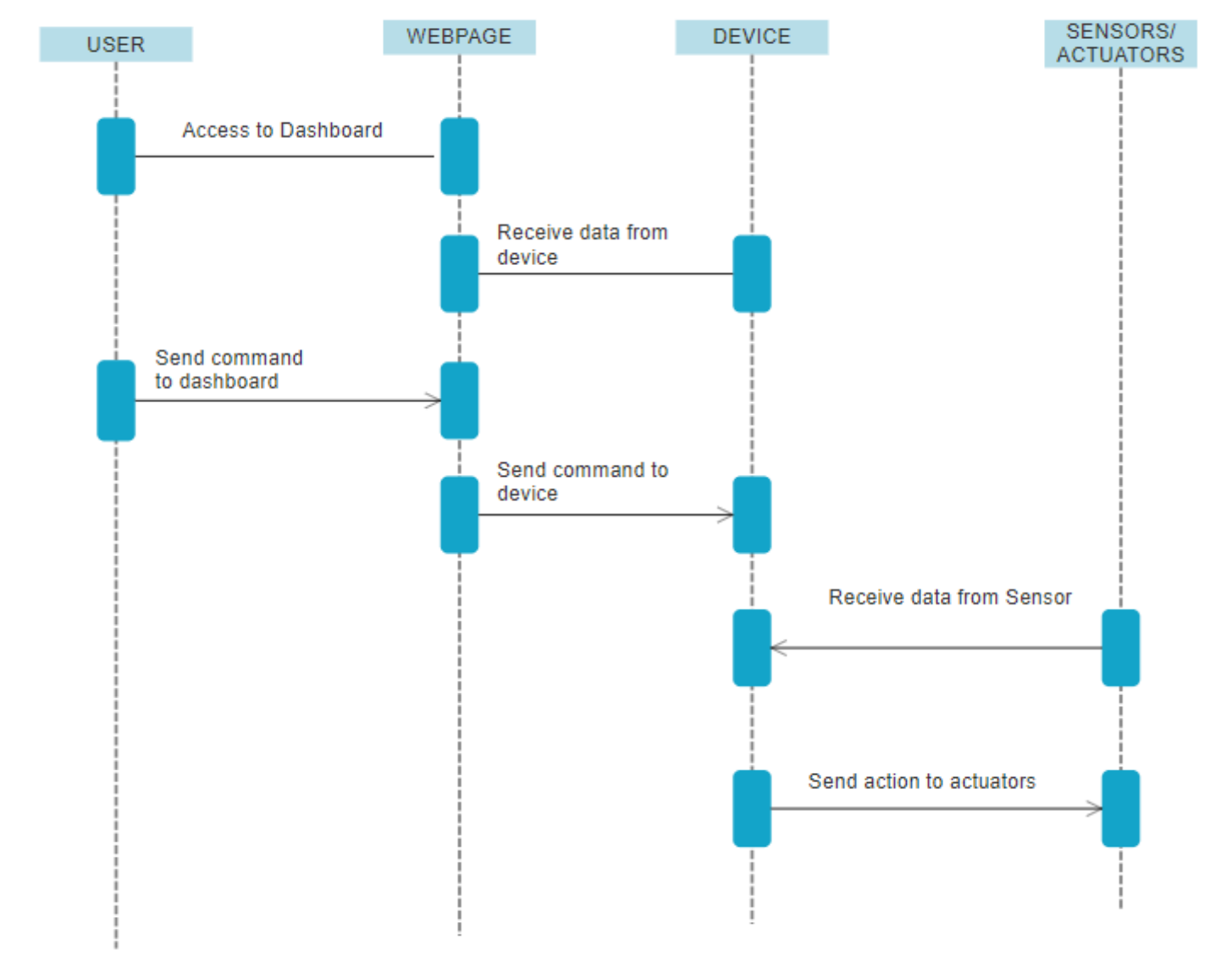


Use Case Diagram



ACTIVITY DIAGRAM

SEQUENCE DIAGRAM



MODULES/METHODOLOGY

- IOT DEVICE MANAGEMENT MODULE
- BLOCKCHAIN INTEGRATION MODULE
- IPFS DATA STORAGE MODULE
- DEVICE AUTHENTICATION AND SECURITY MODULE
- USER INTERFACE AND DASHBOARD MODULE

Conclusion

In conclusion, this project demonstrates the transformative potential of integrating the Interplanetary File System (IPFS) with the Internet of Things (IoT) for home automation. By addressing some of the critical limitations present in traditional, centralized IoT architectures, such as privacy concerns, scalability issues, and vulnerability to single points of failure, IPFS offers a decentralized and more secure framework for IoT communication. In the context of home automation, where the interconnectedness of devices plays a crucial role in enhancing the efficiency, security, and functionality of smart homes, the decentralized model proves particularly advantageous.

References

1.Benet, J. (2014). "IPFS - Content Addressed, Versioned, P2P File System." Protocol Labs. Retrieved from https://ipfs.io/ipfs/QmR7GSQM93Cx5eAg6a6dCENJGZ5g6VFJ6KuWxz8bWwv2P

2.Parker, L. (2021). "IPFS and IoT: Solving data decentralization challenges in smart homes." IoT For All. Retrieved from https://www.iotforall.com/ipfs-iot-data-decentralization

3.Mylonas, G., Markakis, E., & Sakkopoulos, E. (2022). "The role of decentralized storage in IoT." IEEE Internet of Things Magazine. DOI: 10.1109/IOTM.2022.3172649

4.Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). "Security, privacy and trust in Internet of Things: The road ahead." Computer Networks, 76, 146-164. DOI: 10.1016/j.comnet.2014.11.008

5.Ray, P. P. (2018). "A survey on Internet of Things architectures." Journal of King Saud University - Computer and Information Sciences, 30(3), 291-319. DOI: 10.1016/j.jksuci.2016.10.003

Thank you