CHAPTER 1

INTRODUCATION

The rapid advancement of the Internet of Things (IoT) has significantly impacted various sectors, with home automation emerging as one of the most popular applications. In modern homes, IoT devices are integrated to automate everyday tasks such as lighting, security, climate control, and energy management. These interconnected devices enable users to monitor and control various functions in their homes remotely via smartphones or other digital interfaces. This transformation towards smart homes promises greater convenience, energy efficiency, and enhanced security. However, as the number of devices grows, traditional centralized architectures for IoT communication face several challenges, especially in terms of scalability, security, and reliability. Centralized IoT systems in home automation often depend on cloud-based platforms, where data from IoT sensors and devices is sent to centralized servers for processing and storage. While this model works well for small-scale implementations, it becomes problematic as the number of IoT devices in the home increases. With each device generating a continuous stream of data, centralized systems can struggle to handle the rising volume, leading to delays, bottlenecks, and potential system failures. Additionally, reliance on third-party cloud providers raises concerns about data privacy and security, as sensitive information such as user habits and security logs are stored on external servers. The risk of a single point of failure is also an issue: if the cloud service goes down, the entire home automation system can become inoperative. To address these limitations, decentralized solutions are gaining attention, with the Interplanetary File System (IPFS) being a promising alternative for IoT communication in home automation. IPFS is a peer-to-peer distributed file system that enables devices to store and share data across a decentralized network. Instead of relying on a single server, data in IPFS is stored across multiple nodes in the network, making it highly resilient and eliminating central points of failure. IPFS uses content-addressing, where each piece of data is identified by a unique cryptographic hash, ensuring that the data cannot be tampered with or duplicated without detection. Home automation systems using IPFS can significantly improve security and privacy by allowing IoT devices to communicate directly with each other through a peer-to-peer network. This decentralized approach reduces dependency on external cloud services, ensuring that sensitive data remains within the local network and is only shared with

trusted peers. Furthermore, IPFS enhances scalability by distributing data across a wider network, thus mitigating the challenges posed by the increasing number of IoT devices. This paper explores the potential of integrating IPFS with IoT-based home automation systems. By decentralizing communication, IPFS offers a secure and scalable solution that addresses the limitations of traditional centralized architectures. The paper will provide a detailed analysis of the benefits of using IPFS in home automation, focusing on improving system resilience, privacy, and efficiency.

1.1 OBJECTIVES

The primary objective of this project is to seamlessly integrate home automation systems with decentralized technologies, specifically focusing on the Internet of Things (IoT) and the InterPlanetary File System (IPFS). By utilizing IPFS, the project aims to overcome the inherent limitations of traditional centralized systems, thereby providing enhanced security, improved data privacy, and effective real-time monitoring for smart home applications. The initiative is designed to establish a robust and efficient method for securely storing and sharing sensor data, while allowing users to monitor and control devices—such as sensors and actuators—from any location in real time. Additionally, the project seeks to facilitate faster communication between devices, ensuring timely responses to user commands and system events. This will significantly enhance the overall efficiency of home automation processes, creating a more responsive and user-centric environment. Ultimately, the project aspires to build a comprehensive smart home ecosystem that not only ensures data integrity and security but also minimizes reliance on centralized servers. By promoting decentralized architecture, this project aims to provide users with greater control over their home automation systems while supporting the evolution of smart technologies in the modern household.

1.2 AIM OF THE PROJECT

Traditional home automation systems predominantly rely on centralized cloud servers for the storage and processing of data generated by various IoT devices, such as sensors and actuators. This centralization poses significant risks, including data breaches, as sensitive personal information is housed on third-party servers that users cannot control. Moreover, the immense volume of data produced by these devices can create scalability challenges, as centralized systems often struggle to

efficiently manage the growing data load. This project aims to address these issues by implementing IPFS (InterPlanetary File System), a decentralized file-sharing protocol, for the secure storage and retrieval of sensor data. By utilizing IPFS, the system ensures that data is distributed across multiple nodes, significantly reducing the risk of data loss or unauthorized access. Furthermore, the project intends to establish a real-time communication framework between users and their home devices, enhancing the responsiveness and functionality of the home automation setup. This approach not only improves security and scalability but also empowers users with greater control over their data. Ultimately, the project aspires to create a more resilient, efficient, and user-friendly smart home environment, paving the way for the future of home automation technologies.

1.3 SCOPE OF THE PROJECT

The scope of this project is to develop a scalable and efficient IoT data management system utilizing IPFS (InterPlanetary File System). The primary objective is to ensure the secure and reliable storage of vast amounts of data generated by IoT devices. By leveraging IPFS, the system aims to decentralize data storage, eliminating traditional centralized vulnerabilities while enhancing privacy and security. Additionally, the project seeks to enable seamless data sharing and analysis between interconnected IoT devices. This will facilitate more efficient communication and collaboration across a variety of IoT applications. A key focus is on providing a decentralized solution that not only preserves the privacy of users and their data but also enhances the system's robustness by mitigating the risks associated with single points of failure. This project is intended to contribute to the growing need for scalable IoT systems capable of handling ever-increasing volumes of data, while maintaining high levels of data integrity and accessibility. By integrating blockchain technology alongside IPFS, the system ensures that the data is tamper-proof and traceable, making it an ideal solution for modern IoT environments that prioritize security, privacy, and scalability.

1.3.1 SDG GOALS

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

GOAL 9: INDUSTRY, INNOVATION, AND INFRASTRUCTURE

This project aligns with Goal 9 by integrating cutting-edge IoT and blockchain technologies, which foster technological innovation in data management systems for both home automation and industrial applications. The use of IPFS and blockchain ensures secure, efficient, and decentralized data handling, making it a crucial step toward enhancing industrial infrastructure. The project improves operational efficiency, minimize downtime, and enhance data integrity, ultimately supporting technological growth and innovation within industries and home automation ecosystems.

GOAL 11: SUSTAINABLE CITIES AND COMMUNITIES

The project supports Goal 11 by promoting the development of sustainable urban solutions through the use of IoT and blockchain technologies. By enhancing home automation and resource management, it aids in creating smarter, more efficient cities. The project's innovations not only optimize resource distribution but also reduce waste, making urban living more efficient, sustainable, and environmentally friendly, thus aligning with the vision of sustainable cities.

GOAL 12: RESPONSIBLE CONSUMPTION AND PRODUCTION

This project contributes to Goal 12 by promoting responsible consumption and production practices through improved data tracking and resource management. By leveraging IoT and blockchain technologies, the system optimizes home automation to ensure efficient use of energy, water, and other resources. The decentralized nature of the system further supports sustainable production by minimizing reliance on central authorities, enhancing transparency, and encouraging more responsible use of resources.

GOAL 13: CLIMATE ACTION

This project contributes by leveraging IPFS and blockchain technologies to reduce energy consumption and minimize the carbon footprint in data storage and management. By utilizing decentralized systems, it eliminates the need for energy-intensive centralized servers, promoting more energy-efficient operations. Additionally, the optimized resource management enabled by IoT technology helps reduce waste and unnecessary energy use in home automation systems. This directly supports climate action efforts by promoting sustainable energy practices.

1.4 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, which is critical for understanding how IoT devices interact in a smart home automation system.
DATA MINING AND DATA WAREHOUSING (6^{th} 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 analysing 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 (6^{TH} 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.

CHAPTER 2

LITERATURE SURVEY

1. Bobde Y, Narayanan G, Jati M, Raj RSP, Cvitić I, Peraković D. Enhancing Industrial IoT Network Security through Blockchain Integration. Electronics. 2024; 13(4):687. https://doi.org/10.3390/electronics13040687

This paper explores the integration of blockchain technology and decentralized systems, such as IPFS (InterPlanetary File System), to improve the security of IoT infrastructures. The research emphasizes the significance of decentralized storage and peer-to-peer networks in mitigating key security issues that IoT systems encounter, particularly in critical applications like home automation. By utilizing blockchain's immutable ledger alongside IPFS's distributed storage capabilities, the proposed approach aims to enhance data integrity and prevent unauthorized access. This paper underlines the critical need for decentralized solutions in securing IoT applications, reinforcing the notion that adopting such technologies is vital for creating safer and more reliable home automation systems. Ultimately, the findings contribute to a better understanding of how decentralized networks can effectively address security vulnerabilities within the rapidly evolving IoT landscape.

2. Xiaochen Zheng, Jinzhi Lu, Shengjing Sun, Dimitris Kiritsis. Decentralized Industrial IoT Data Management Based on Blockchain and IPFS. IFIP International Conference on Advances in Production Management Systems (APMS), Aug 2020, Novi Sad, Serbia. pp.222-229, ⟨10.1007/978-3-030-57997-5_26⟩. ⟨hal-03635622⟩

This paper presents an innovative approach to managing industrial IoT (IIoT) data by leveraging Blockchain and IPFS (InterPlanetary File System). The study emphasizes the importance of decentralization for achieving a secure and scalable system for handling large volumes of IIoT data. Traditional centralized systems often face challenges like data tampering, loss, and a lack of traceability. By utilizing Blockchain’s immutable ledger and IPFS’s distributed storage capabilities, the proposed framework enhances data integrity, ensures traceability, and resists tampering, which are essential requirements in IIoT environments. The decentralized approach also addresses concerns around data ownership and privacy, offering a more resilient solution to securely manage industrial data. This

system is highly relevant in sectors where data authenticity and security are crucial, such as manufacturing, logistics, and automation.

3. H.R.Hasan, K.Salah, I.Yaqoob, R.Jayaraman, S.Pesic and M.Omar, "Trustworthy IoT Data Streaming Using Blockchain and IPFS," in IEEE Access, vol. 10, pp. 17707-17721, 2022, doi: 10.1109/ACCESS.2022.3149312. (2022)

This research paper investigates the potential of combining Blockchain technology with IPFS (InterPlanetary File System) to improve the reliability of IoT data streams. Written by a team of researchers, the study addresses the critical issue of ensuring data integrity in real-time streaming applications. The authors propose a decentralized framework that leverages the unique features of both technologies to counteract the risks associated with data tampering. By implementing this solution, the paper aims to establish a more secure and trustworthy environment for streaming IoT data, ultimately enhancing the overall effectiveness of IoT applications. This method enhances data security while enabling smooth communication across different IoT ecosystems, representing a valuable advancement in the field. By leveraging decentralized technologies, it addresses critical vulnerabilities associated with centralized systems, thus reducing the risk of data breaches. Furthermore, it fosters interoperability among diverse IoT devices, ensuring that they can communicate effectively and efficiently.

4. Khan, Waseem, Gargi Kumbhare, and Pradnya Pugaonkar. "Integrating IoT with Health Record Management System using IPFS and Blockchain." International Journal of Computer Applications 975: 8887. (2022)

This paper focuses on the convergence of IoT technology with health record management systems, leveraging the strengths of blockchain and IPFS for enhanced security in data storage and sharing. It emphasizes the importance of blockchain in maintaining data immutability, ensuring that health records remain unchanged and secure from tampering. Additionally, the paper discusses how IPFS facilitates decentralized storage solutions, which is essential for managing sensitive health information efficiently. This integration of technologies aims to address the critical need for secure health management systems within smart healthcare applications. By combining the real-time capabilities of IoT devices with the robust security features of blockchain and IPFS, the study paves the way for innovative

approaches to safeguard patient data, ultimately enhancing the quality of healthcare services and patient privacy in a rapidly evolving digital landscape.

5. Bugeja, Joseph, Andreas Jacobsson, and Paul Davidsson. "On privacy and security challenges in smart connected homes." 2016 European Intelligence and Security Informatics Conference (EISIC). IEEE, 2016.

This paper addresses significant privacy and security issues prevalent in smart home systems, particularly concerning the transmission of sensitive data to centralized cloud servers. The study provides a comprehensive examination of the vulnerabilities associated with cloud-based architectures, highlighting risks such as data breaches and unauthorized access. These concerns pose considerable threats to user privacy and the integrity of personal information. The relevance of this research lies in its identification of the inherent weaknesses in traditional smart home infrastructures. It suggests that adopting decentralized models like IPFS (InterPlanetary File System) can effectively mitigate these issues by providing users with greater control over their data. By moving away from centralized storage, smart homes can enhance privacy and security, ensuring that sensitive information remains protected and accessible only to authorized users.

6. Kasmi, Mahdi, Faouzi Bahloul, and Haykel Tkitek. "Smart home based on Internet of Things and cloud computing." 2016 7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT). IEEE, 2016.

The paper discusses the architecture and implementation of a smart home system that integrates the Internet of Things (IoT) with cloud computing. The system allows users to control and monitor their home devices remotely, enhancing convenience, security, and energy efficiency. IoT-enabled sensors and devices are connected to a cloud platform, enabling real-time data collection, storage, and processing. This architecture allows users to access the system through mobile or web applications, giving them the flexibility to monitor and manage their home environment from anywhere. The system also incorporates automated features like turning off lights or adjusting thermostats based on predefined rules or real-time conditions. Security is addressed through authentication and secure data transfer protocols, ensuring user privacy and data protection.

CHAPTER 3

RESEARCH GAP

Despite significant advancements in home automation and IoT systems, most existing solutions continue to rely heavily on centralized cloud-based infrastructures. These centralized models introduce several limitations, such as data privacy concerns, security vulnerabilities, and scalability issues. With the exponential growth of connected devices, the volume of data generated by IoT systems is overwhelming, creating bottlenecks in data processing and storage. Additionally, centralized systems expose sensitive user data to third-party control, increasing the risk of data breaches and unauthorized access. Furthermore, while blockchain technology has been widely recognized for its potential to enhance data security, it has yet to be fully integrated into mainstream IoT and home automation systems. The use of IPFS as a decentralized storage solution is also underexplored in this context. Most studies focus on general applications of blockchain and IPFS but lack comprehensive frameworks tailored specifically for home automation environments. This research aims to fill this gap by integrating decentralized technologies such as IPFS and blockchain into IoT-based home automation systems. The goal is to enhance data security, privacy, and scalability while reducing the reliance on centralized cloud servers. This project will offer a more resilient, efficient, and secure solution for smart homes.

3.1 EXISTING SYSTEM

In the existing systems for home automation, IoT devices are typically managed through centralized architectures where cloud-based platforms or servers act as intermediaries between the user and the devices. These systems allow users to control smart home devices like lights, thermostats, and security cameras through cloud-hosted applications, which process data and relay commands back to the devices. However, the reliance on centralized servers introduces several issues, such as increased vulnerability to single points of failure, privacy concerns, and the potential for data breaches. If the server goes down or is compromised, the entire home automation system could fail or become exposed to cyber threats. Moreover, centralized systems often struggle with scalability as more IoT devices are added, causing latency issues and increasing costs associated with maintaining large-scale cloud infrastructure.

3.2 PROPOSED SYSTEM

To overcome the limitations of traditional centralized systems, the proposed solution introduces a decentralized architecture for home automation, powered by the InterPlanetary File System (IPFS). By employing IPFS, the system leverages a peer-to-peer network to store data generated by IoT devices in a distributed manner, eliminating the need for central control. This architecture ensures that data is no longer dependent on a single server, significantly reducing the risks associated with centralized management, such as single points of failure and data breaches. In this model, each piece of data is addressed by its content rather than its location, using cryptographic hashing to ensure data integrity and privacy. This content-addressed storage model not only guarantees that the data remains unaltered but also enables secure sharing between devices. By decentralizing the storage and management of data, the system enhances privacy, as sensitive information is distributed across multiple nodes within the network. Only authorized devices can access the data, providing an added layer of security. Furthermore, IPFS facilitates direct communication between IoT devices within the smart home, bypassing the need for a centralized cloud server. This direct, decentralized communication reduces latency and enhances the system's responsiveness, allowing devices to operate more efficiently in real-time. The decentralized nature of the system also improves scalability. Unlike centralized systems, where adding new devices can overburden a central server, the proposed system allows for seamless expansion. Additional devices can easily be integrated into the peer-to-peer network without compromising performance or security. Another key advantage of this decentralized approach is its resilience. The proposed home automation system powered by IPFS provides a more secure, scalable, and resilient solution for IoT ecosystems. By decentralizing data storage and device communication, it addresses the challenges of scalability, privacy, and system reliability. This innovative approach paves the way for the development of more decentralized IoT systems in the future, ensuring that smart homes can operate efficiently without reliance on vulnerable centralized servers. In the proposed system, data is spread across a distributed network of nodes, meaning there is no single repository for potential attacks. By distributing data storage, the system minimizes the risks associated with centralized data breaches and unauthorized access.

3.3 FEASABILITY STUDY

A feasibility study for the IoT-based home automation system, leveraging IPFS and Blockchain, assesses the project's technical, operational, and economic aspects. Technically, the system uses IoT devices to collect sensor data, which is stored in a decentralized manner using IPFS (InterPlanetary File System), ensuring data integrity, security, and availability. Blockchain enhances this by providing a tamper-proof ledger, ensuring transparency in how data and device commands are managed. Both technologies complement each other to provide a robust and secure infrastructure for the automation system, making it highly scalable and reliable.

Operationally, the system integrates with a user-friendly web-based dashboard, allowing users to monitor and control home devices from anywhere. The system processes user commands, collects data from sensors, and sends these through IPFS and Blockchain, maintaining seamless communication between the devices and the control interface. This streamlining of home automation tasks enhances user experience and improves system reliability. 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.

Economically, although the initial setup may involve costs for IoT devices, Blockchain nodes, and IPFS gateways, the long-term operational costs are reduced due to the decentralized nature of IPFS, which eliminates reliance on expensive centralized cloud services. This solution is cost-effective in the long run, offering secure, transparent, and efficient automation without ongoing cloud service fees. 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.

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.

CHAPTER 4

SYSTEM REQUIREMENTS

4.1 HARDWARE REQUIREENTS

For an IoT-based home automation system that leverages Blockchain and IPFS, the hardware requirements include:

- **ESP8266/ESP32 or Raspberry Pi**
  - ESP8266/ESP32: These microcontrollers are widely used in IoT projects due to their built-in Wi-Fi capability, low cost, and energy efficiency. They handle communication between sensors and the control dashboard, sending data to IPFS and receiving commands via Blockchain.
  - Raspberry Pi: An alternative to ESP devices, Raspberry Pi is a more powerful single-board computer that can run full operating systems and manage complex operations like running a Blockchain node or IPFS gateway. It offers greater versatility but consumes more power than ESP devices.

- **Storage Drive**
  - A storage medium (such as an SSD or HDD) is needed, particularly if you use Raspberry Pi or local nodes, to store data and logs. IPFS will ensure distributed storage and data integrity, but a local storage drive helps cache important information locally for quick access.

- **Wi-Fi Router**
  - A stable Wi-Fi connection is crucial for communication between IoT devices, the control interface (web dashboard), and the distributed network (Blockchain and IPFS). A router allows all devices to be connected within a local network and can also connect the system to the internet for remote access.

- **Optional: Ethernet**
  - While Wi-Fi is the primary method of communication, Ethernet is a wired alternative that provides more stability and higher security. For fixed

installations or industrial setups, Ethernet may be preferable for stable, real-time communication.

- **Power Supply**
  - Each IoT device, controller, and actuator will need an appropriate power supply. ESP8266/ESP32 devices typically operate at 3.3V to 5V, while Raspberry Pi requires 5V power, typically provided via micro-USB or USB-C. The power supply should be reliable, ensuring constant operation.

- **Various Sensors (temperature, motion, light, humidity), Actuators (drives, relays)**
  - Sensors: These are the key data collectors in an IoT system. For example, a temperature sensor monitors environmental heat, a motion sensor detects movement, and a humidity sensor tracks moisture levels. These sensors collect real-time data that is fed to the system and stored via IPFS.
  - Actuators: These are devices like motors, relays, or switches that act upon the data or commands received. For instance, if a sensor detects high temperature, an actuator might turn on a fan or cooling system. Actuators make the system interactive by carrying out tasks based on input commands.

4.2 SOFTARE REQUIRMENTS

For a home automation system based on Blockchain and IPFS, the software requirements include:

- **Operating System**
  - A stable operating system (OS) is needed to run the central control hub, especially when using devices like Raspberry Pi. Common OS choices include Linux distributions (such as Raspbian for Raspberry Pi) or Windows. Linux is often preferred due to its stability, flexibility, and compatibility with IoT and Blockchain platforms. It also supports open-source development environments.
- **IPFS Software**
  - IPFS (InterPlanetary File System) is a decentralized storage network that allows the system to store and retrieve data securely and efficiently. The IPFS software handles the storage of sensor data, making it accessible across a

distributed network. The installation of IPFS on a local node (e.g., Raspberry Pi) enables secure data sharing and backup without depending on a centralized server.

- **IoT Device Control Software**
  - This software is responsible for interacting with IoT devices (e.g., sensors and actuators). Software libraries like Arduino IDE, or custom IoT frameworks allow the programming of ESP8266/ESP32 devices, enabling data collection and the execution of commands. This software also facilitates device integration and management with protocols like MQTT (Message Queuing Telemetry Transport).

- **Mobile/Web Application**
  - A user-friendly mobile or web-based dashboard is necessary to control and monitor the IoT devices. This dashboard communicates with IPFS and Blockchain networks to provide real-time data to users. The app allows users to send commands (like turning on lights or adjusting the thermostat) and view collected data (e.g., temperature or motion detection). React, Angular, or Flutter can be used to develop web or mobile applications with seamless user interfaces.

- **Python IDE**
  - Python is widely used for scripting and programming IoT systems, handling sensor data processing, and interacting with Blockchain and IPFS. A Python IDE, such as PyCharm, Visual Studio Code, or Thonny, is used for developing, debugging, and running Python scripts. Python libraries like Flask (for backend API development) and paho-mqtt (for MQTT communication) allow for seamless device integration and control. Additionally, Python helps in automating tasks, managing IPFS nodes, and interfacing with Blockchain smart contracts.

CHAPTER 5

SYSTEM DESIGN

5.1 ARCHITETURE DIAGRAM

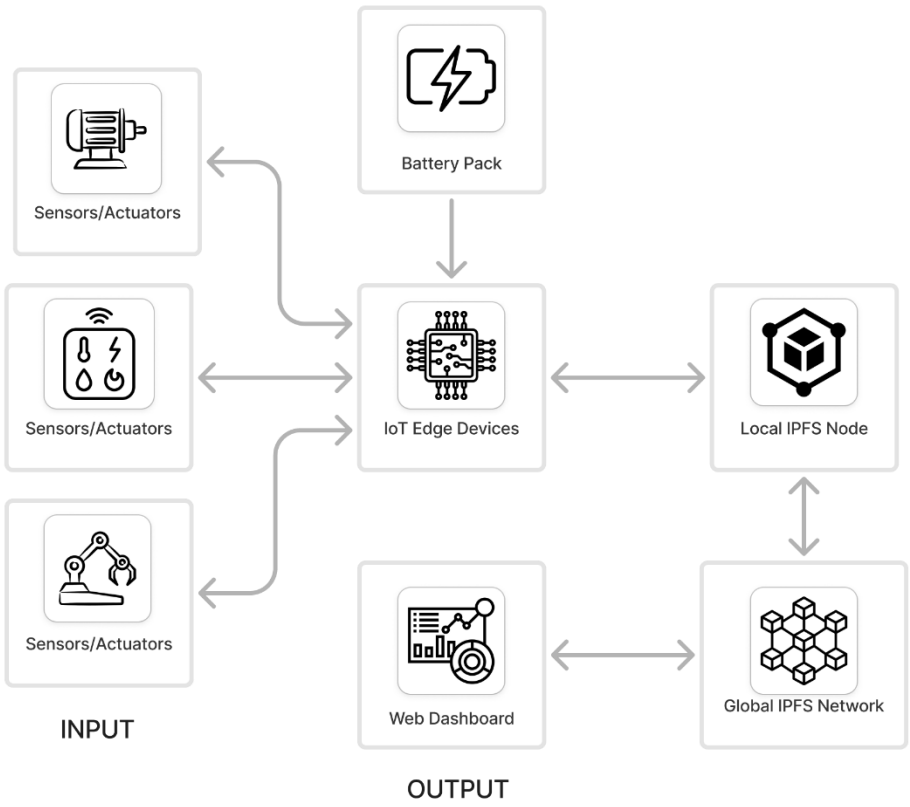

Fig 5.1 Architecture diagram

A decentralized home automation system leveraging IoT devices and the InterPlanetary File System (IPFS). Sensors and actuators provide input data, which is processed by IoT edge devices powered by a battery pack. These edge devices communicate with a local IPFS node, which stores and retrieves data in a decentralized manner. The local node is connected to the global IPFS network, allowing secure and distributed data sharing. Users interact with the system via a web dashboard, which visualizes real-time data and enables device control. This setup enhances scalability, security, and independence from centralized servers.

5.2 UML DIAGRAMS

UML stands for Unified Modeling Language. UML is a standardized general purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

5.2.1 USE-CASE DIAGRAM

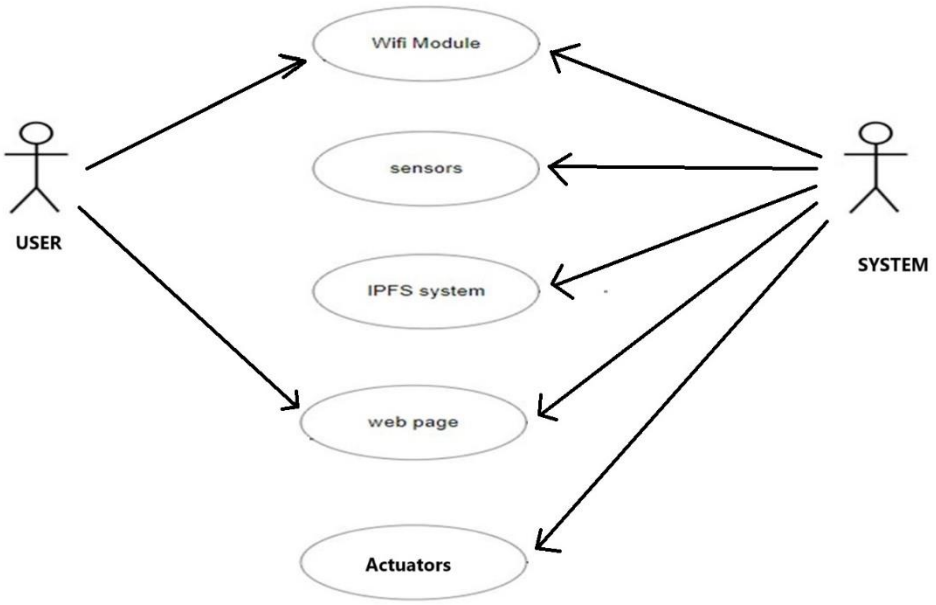

Fig 5.2 Use-case diagram

The diagram represents the interaction flow between a user and a system in a home automation environment, integrating Wi-Fi, sensors, IPFS, and actuators. The user communicates with the system through a Wi-Fi module, enabling remote control and monitoring of the devices in the home. The sensors in the system gather data from the environment (e.g., temperature, humidity, motion) and send this data to the system for further processing. The web page serves as the interface where the user can visualize the sensor data and interact with the system, issuing commands such as controlling the actuators. The actuators, in turn, execute the user's commands by performing actions such as turning on lights, adjusting thermostats, or operating other smart devices.

5.2.2 CLASS DIAGRAM

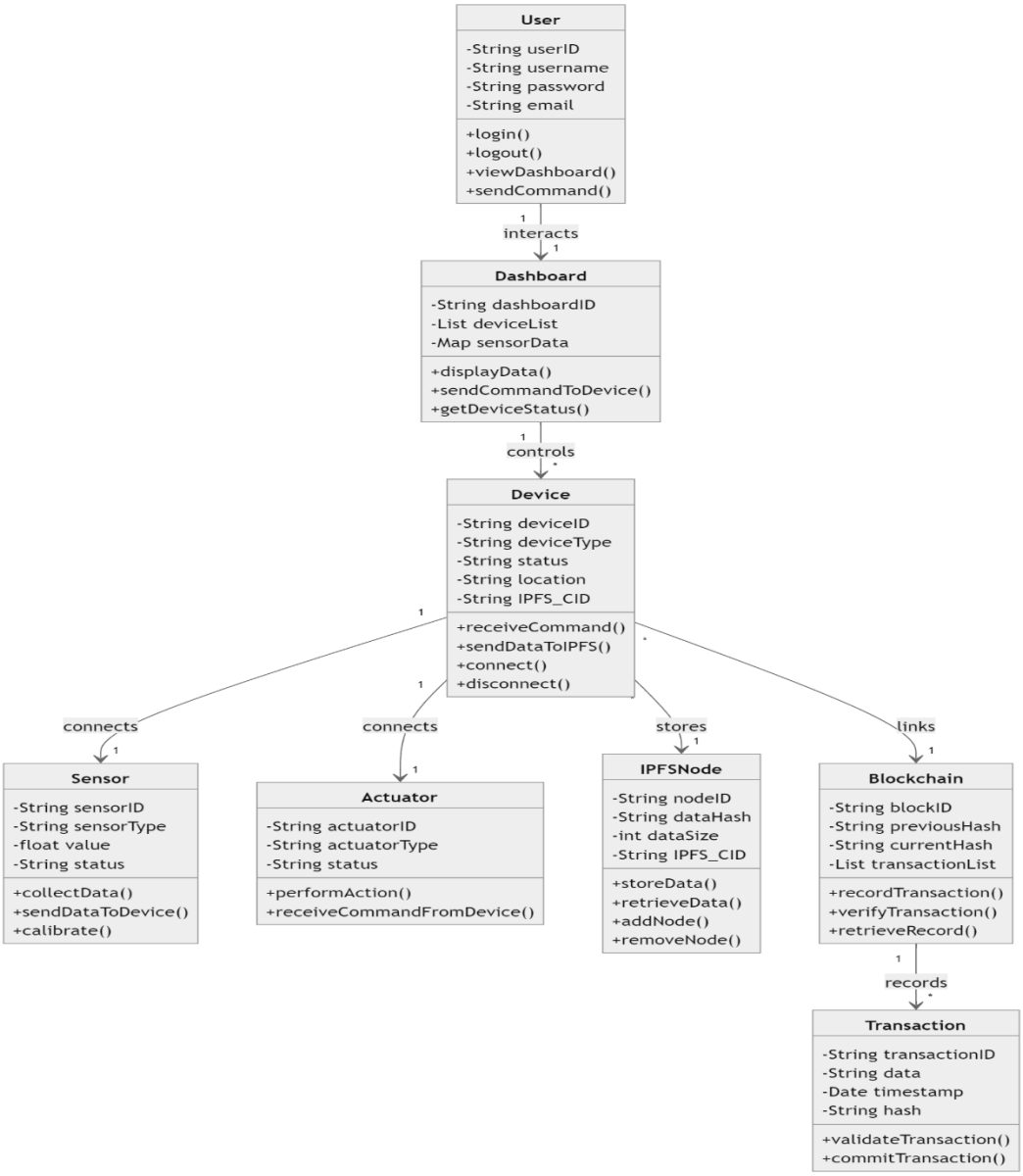

Fig 5.3 Class diagram

This class diagram represents an IoT-based home automation system using Blockchain and IPFS for secure data management. The User interacts with the system through a Dashboard, which displays device data and sends commands to various IoT devices. The Device class connects to Sensors to collect data and Actuators to perform actions, while storing data in IPFS via an IPFS Node. The Blockchain class ensures secure and immutable transaction recording, linking every action and data change. The Transaction class validates actions, maintaining data integrity and ensuring a tamper-proof system for secure, decentralized IoT management.

5.2.3 ACTIVITY DIAGRAM

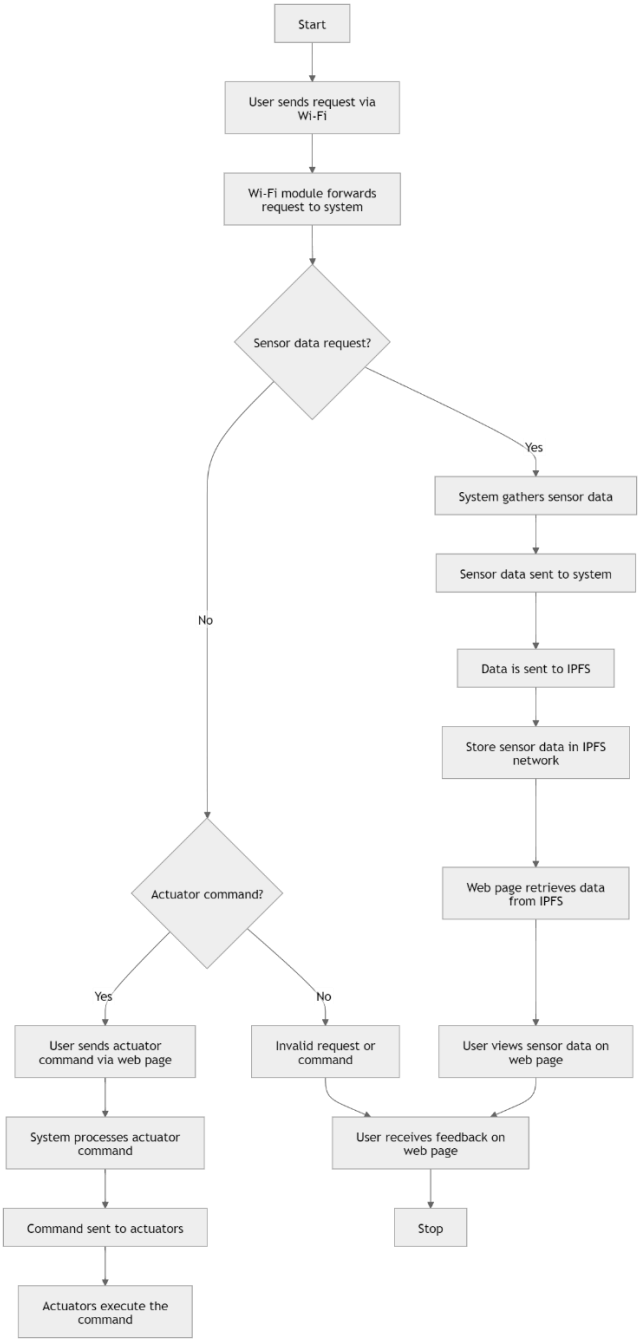

Fig 5.4 Activity diagram

The diagram represents the activity flow in a decentralized IoT system utilizing IPFS for communication. It begins with a user sending a request via Wi-Fi, where the system decides whether the request is for sensor data or actuator control. If sensor data is requested, it is gathered, sent to IPFS, and displayed on a web page. If the command is for actuators, the system processes the command and executes it through the actuators. The diagram ensures that the user receives feedback on the web page, closing the interaction loop.

5.2.4 SEQUENCE DIAGRAM

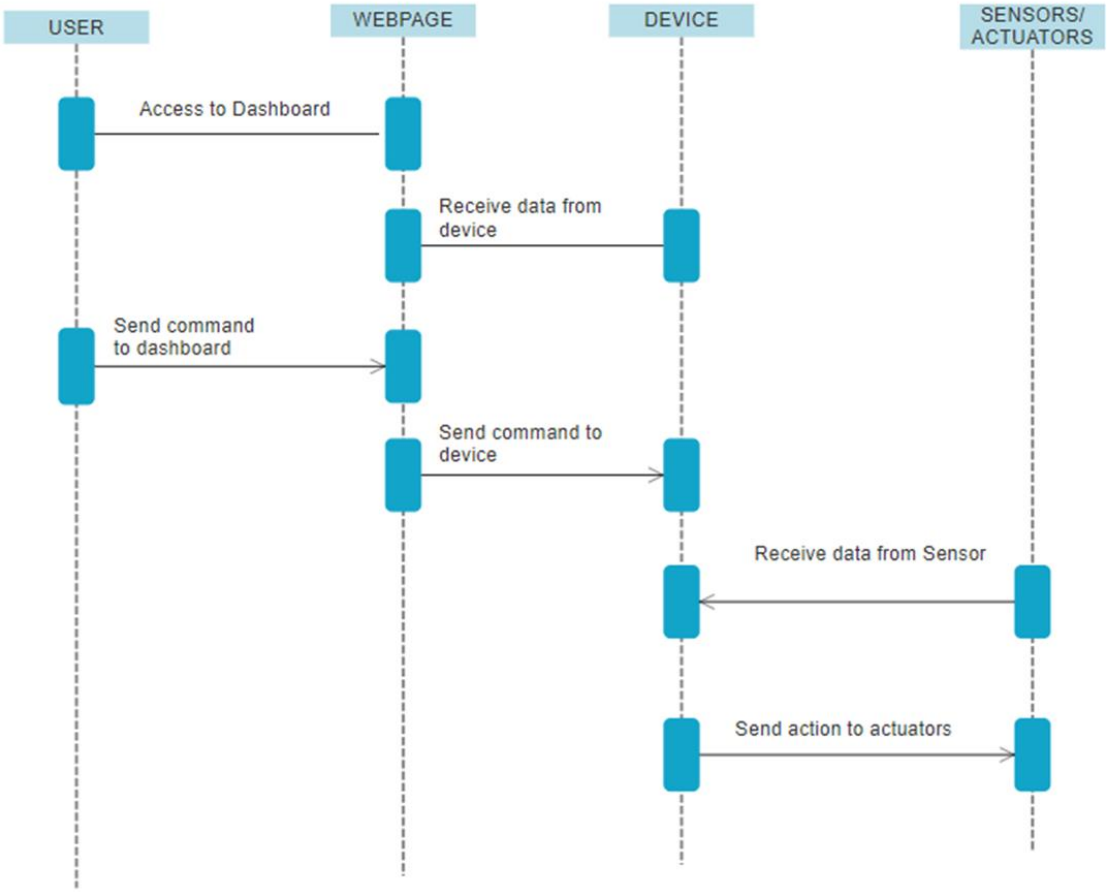

Fig 5.5 Sequence diagram

The diagram is a sequence diagram that illustrates the interaction between different components in an IoT system using a web-based dashboard for communication with sensors and actuators. It begins with the user accessing the dashboard on the webpage and sending a command. The webpage receives this command and forwards it to the IoT device. The device then communicates with the sensors/actuators to either retrieve data or execute an action. The sensor/actuator sends data back to the device, which is relayed to the webpage for the user to view. This interaction represents the continuous flow of commands and responses between the user, web interface, device, and physical sensors or actuators.

5.2.5 DEPLOYMENT DIAGRAM

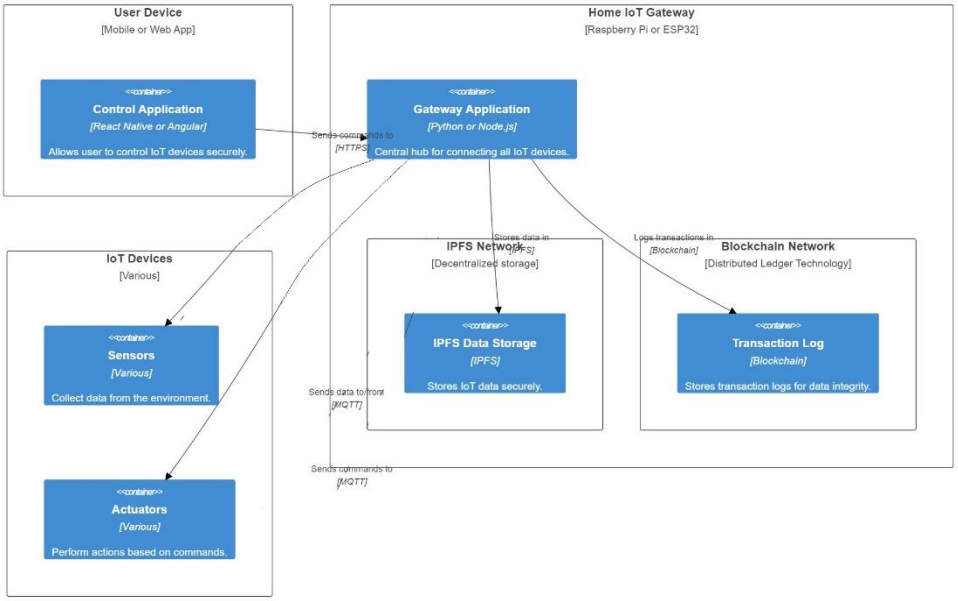

Fig 5.6 Deployment Diagram

The deployment diagram for an IoT-based home automation system illustrates the system's components and their interactions in a distributed environment using IPFS and blockchain technologies. At the user level, a User Device, such as a mobile or web application, allows users to control IoT devices in their homes. This application interfaces with the Gateway Application, hosted on a Home IoT Gateway device like a Raspberry Pi or ESP32, which acts as a central hub. The gateway handles communication between the user's app and the various IoT devices in the system, such as Sensors and Actuators. Sensors gather data from the environment (like temperature or motion), while actuators execute tasks (such as switching on lights) based on user commands. The gateway ensures seamless communication using the MQTT protocol, sending collected data to a decentralized storage system via the IPFS Network. This data is securely stored in the IPFS Data Storage, ensuring integrity and scalability by distributing the information across multiple nodes.

To maintain data integrity and transparency, every action or command is logged in a Blockchain Network, where a Transaction Log stores transaction records. This combination of IPFS and blockchain ensures decentralized, secure, and immutable data storage and communication, avoiding single points of failure and offering enhanced security for home automation systems.

5.3 FLOW CHART

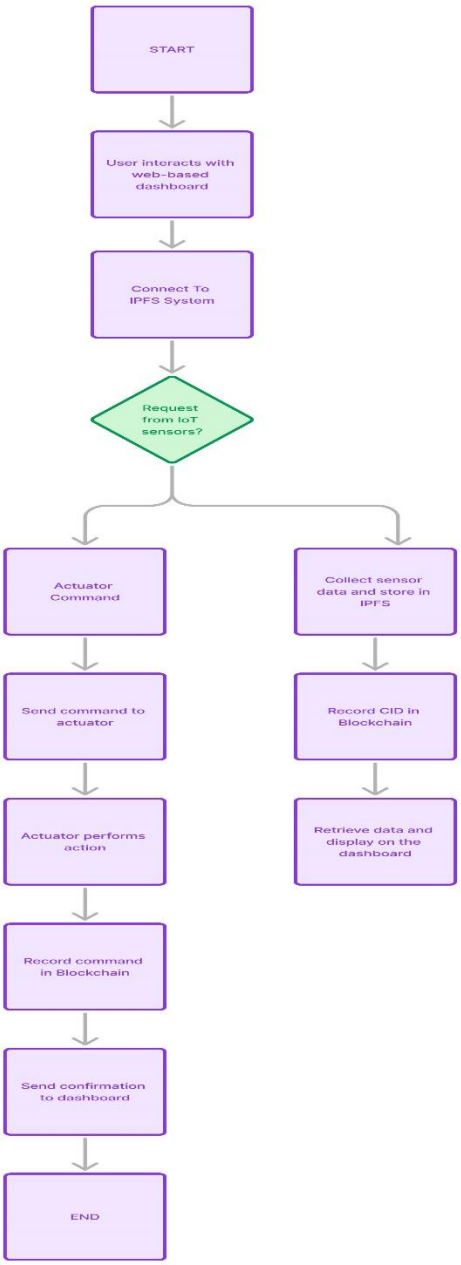

Fig 5.7 Flowchart

The flowchart illustrates the process of an IoT-based home automation system integrated with IPFS and Blockchain. It begins with the user interacting with a web-based dashboard, followed by two possible actions: requesting sensor data or sending commands to actuators. If a sensor data request is made, data is collected and stored in IPFS, with the Content Identifier (CID) recorded on the Blockchain for security. The data is then retrieved and displayed on the dashboard. For actuator commands, the system sends the command, performs the action, records the command in the Blockchain, and confirms execution back to the dashboard.

CHAPTER 6

METHODOLOGY

6.1 MODULES DESCRIPTION

6.1.1 IOT DEVICE MANAGEMENT MODULE

This module handles the real-time interaction between various IoT devices, such as sensors and actuators, and the control hub (e.g., Raspberry Pi, ESP8266, or ESP32). The devices are responsible for monitoring environmental conditions (e.g., temperature, humidity, light) or performing specific tasks (e.g., turning on lights or motors).

Functions:

- Data Collection: Sensors, such as temperature, humidity, and motion detectors, continuously collect data from the environment. These sensors are connected to the microcontroller (ESP8266, ESP32, or Raspberry Pi), which acts as the central hub.
- Actuation Control: Commands sent from the user via the web or mobile app are relayed to the actuators (e.g., motors, relays) to trigger actions like opening doors, turning on fans, or adjusting lighting.
- Protocols: The communication between IoT devices and the hub typically uses protocols like MQTT, HTTP, or WebSockets. MQTT is widely used for its lightweight nature and low power consumption.

6.1.2 BLOCKCHAIN INTEGRATION MODULE

The Blockchain module ensures the security, integrity, and transparency of data transactions and device interactions. Each action or piece of data collected from IoT devices is recorded as a transaction on the Blockchain, making the system tamper-proof and auditable.

Functions:

- Transaction Logging: Each command or action performed by the IoT devices is stored as a transaction on a Blockchain network. This provides a secure and immutable record of device interactions.
- Smart Contracts: Smart contracts may be used to automate specific processes, such as sending notifications when sensor readings reach a

critical level. The contracts are self-executing and run on the Blockchain, ensuring decentralized execution.

- Security and Trust: Blockchain provides a high level of security by using cryptographic methods to ensure that only authorized users can send commands or access data. It also guarantees data integrity since the ledger cannot be altered without consensus.

6.1.3 IPFS DATA STORAGE MODULE

The InterPlanetary File System (IPFS) module is responsible for decentralized data storage. Instead of storing data in centralized databases, sensor data and device records are stored across multiple nodes on the IPFS network, ensuring both security and redundancy.

Functions:

- Data Storage: Sensor readings, device states, and other important data are stored in the IPFS network. IPFS assigns a unique Content Identifier (CID) to each data file, allowing easy retrieval.
- Distributed Storage: Unlike traditional databases, IPFS splits data into smaller chunks and distributes them across multiple nodes. This decentralized approach reduces the risk of data loss or tampering.
- Data Retrieval: The IPFS system retrieves data based on its CID, rather than using traditional URLs or paths. Users or systems can query the IPFS network to get the required data efficiently, regardless of where it is stored.

6.1.4 DEVICE AUTHENTICATION AND SECURITY MODULE

This module ensures that only authorized devices and users can interact with the system. It protects the system from unauthorized access, data breaches, or device manipulation.

Functions:

- Encryption: Communications between IoT devices, the control hub, and the user interface are encrypted to ensure that sensitive data (e.g., user commands or sensor data) is secure and protected from eavesdropping.
- Authentication: Only authenticated users and devices are allowed to interact with the system. This ensures that only legitimate commands are executed

and that unauthorized entities are blocked from accessing or altering the system.

- Blockchain Security: The Blockchain further enhances security by maintaining a tamper-proof record of all transactions. If an unauthorized entity tries to alter data or send commands, the Blockchain's consensus mechanism will reject the transaction.

6.1.5 USER INTERFACE AND DASHBOARD MODULE

The user interface (UI) provides a centralized platform for users to interact with the system. This can be a mobile app or a web-based dashboard that allows users to monitor real-time data and control the IoT devices.

Functions:

- Monitoring: Users can view real-time data from the IoT devices (e.g., temperature, humidity, or light levels). The data is often visualized using graphs, charts, or widgets.
- Control: Users can send commands to actuators through the interface, such as turning on lights, adjusting thermostats, or triggering alarms. These commands are transmitted to the Blockchain and executed by the IoT devices.
- Logs and History: Users can also view historical data that is securely stored on the Blockchain and IPFS, giving them insight into past device actions and sensor readings.
- Notifications: Alerts or notifications can be sent to users when certain thresholds (e.g., temperature) are reached. This enhances the usability of the system by keeping users informed of critical changes.

6.2 ALGORITHM

The InterPlanetary File System (IPFS) uses several key algorithms and protocols to provide decentralized, distributed storage and content delivery. For sending data in IoT systems using IPFS, a combination of several components and algorithms is employed to handle communication, storage, and retrieval of data between IoT devices. The main algorithms and mechanisms used in IPFS for IoT devices include:

Distributed Hash Table (DHT) with Kademlia Algorithm

The DHT, using the Kademlia algorithm, is the primary mechanism for looking up where data is stored in the IPFS network. Here's how it works:

- **Data storage and retrieval:** When an IoT device sends or retrieves data, it uses the content hash (CID) to locate the relevant nodes that hold the data. Kademlia helps in routing the query across the network to find the nearest peer storing the required data.
- **Decentralization:** No central server is involved. Devices query the DHT to locate the peers storing the requested content.

Usage in IoT

- When an IoT device generates data (e.g., sensor readings), it is chunked and added to IPFS. The CID for that data is then stored in the DHT, allowing any authorized IoT device or user to retrieve the data by querying the DHT.

Merkle Directed Acyclic Graph (Merkle DAG)

The Merkle DAG is used to structure and address the data. It helps ensure data integrity and immutability in the IPFS network.

Usage in IoT

- Data produced by IoT devices (e.g., sensor readings) is split into smaller blocks, each of which is hashed to create a unique content identifier (CID). These blocks are linked in a DAG structure, allowing them to be addressed individually or as part of a larger file.

BitSwap Protocol (Block Exchange)

BitSwap is the protocol responsible for exchanging blocks of data between peers in the IPFS network. It's used for transferring and retrieving blocks of data efficiently between nodes.

Usage in IoT

- IoT devices act as peers in the IPFS network. When an IoT device requests a specific block of data, BitSwap helps to locate and download the block from nearby peers. Similarly, IoT devices can provide blocks they possess to other peers in exchange for blocks they need. BitSwap tracks debt and ensures peers are incentivized to share data by keeping a ledger of exchanged blocks, helping to maintain a balanced network.

libp2p (Peer-to-Peer Communication Framework)

libp2p handles the peer discovery, transport, and communication between devices in the IPFS network. It supports different transport protocols (e.g., TCP, WebRTC) for the communication between peers.

Usage in IoT

- libp2p enables IoT devices to discover other devices or gateways in the local or global network, set up connections, and manage data exchange securely. It also supports encryption, making the communication between devices secure and private.

PubSub (Publish-Subscribe Pattern)

While PubSub is not an algorithm, it plays a role in real-time communication between IoT devices. Devices can subscribe to topics (e.g., "temperature-updates") and get notified when relevant data is published to the topic.

Usage in IoT

- When an IoT sensor generates new data (e.g., temperature data), it can publish the data to a specific PubSub topic.Other IoT devices (e.g., a thermostat or data logger) that are subscribed to that topic will receive the data and act on it, such as adjusting the heating or logging the data.

CHAPTER 7

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. IPFS, through its content-addressed, peer-to-peer network, eliminates the need for cloud-based intermediaries, thereby ensuring that data shared between IoT devices is secure, private, and resilient to network failures or attacks. Moreover, the project underlines the importance of security and privacy in IoT systems, particularly in the home automation sector, where personal data, such as behavioural patterns or device usage, could be sensitive. IPFS offers inherent privacy benefits due to its distributed nature, as data is fragmented and stored across multiple nodes rather than in a single repository. This approach not only makes it difficult for unauthorized users to access the entire dataset but also minimizes the risk of data loss or breach. Additionally, by using cryptographic hash functions to reference data, IPFS ensures that data integrity is maintained, offering users confidence that the information transmitted between their devices is tamper-proof.The project also highlights the convenience brought by real-time data retrieval and command execution using IPFS. Through the integration of IoT edge devices and IPFS nodes, users can control and monitor their home automation systems with minimal latency. The system architecture, which involves gathering sensor data, storing it on a local IPFS node, and then distributing it across the global IPFS network, allows for seamless data retrieval through a web-based dashboard. Users can interact with their home automation devices in real-time, whether to control actuators or view sensor data, without experiencing delays typical of cloud-based systems.

REFERENCE

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

2. 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

3. 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

4. Li, H., & Palanisamy, B. (2018). "Decentralized data management framework for IoT using IPFS and blockchain." In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) (pp. 1321-1326). IEEE. DOI: 10.1109/Cybermatics_2018.2018.00231

5. Xu, R., Ceballos, G., & Lee, B. (2019). "Design of a secure home automation system using the IPFS-based decentralized storage framework." International Journal of Network Security & Its Applications (IJNSA), 11(5), 57-68. DOI: 10.5121/ijnsa.2019.11504

6. Zhang, L., Cui, L., Li, Q., & Xu, C. (2020). "Blockchain and IPFS-based data integrity verification in the Internet of Things." IEEE Access, 8, 195264-195272. DOI: 10.1109/ACCESS.2020.3032162

7. Sharma, V., Chen, M.-Y., Lin, W.-K., Liu, C.-T., & Lin, Y.-C. (2021). "Decentralized IoT Data Sharing Using IPFS and Smart Contracts." IEEE International Conference on Communications Workshops (ICC Workshops). DOI: 10.1109/ICCWorkshops50388.2021.9473746

8. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F.-Y. (2019). "Blockchain-enabled smart contracts: Architecture, applications, and future trends." IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266-2277. DOI: 10.1109/TSMC.2019.2895123

9. 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

10. 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

11. Atzori, L., Iera, A., & Morabito, G. (2010). "The Internet of Things: A survey." Computer Networks, 54(15), 2787-2805. DOI: 10.1016/j.comnet.2010.05.010

12. Zhao, K., & Ge, L. (2013). "A survey on the internet of things security." In 2013 Ninth International Conference on Computational Intelligence and Security (pp. 663-667). IEEE. DOI: 10.1109/CIS.2013.145

13. Bhushan, B., Sahoo, S., & Mishra, D. (2020). "Blockchain for Smart Homes: Challenges and Solutions." Computer Communications, 151, 76-94. DOI: 10.1016/j.comcom.2020.01.040

14. Banafa, A. (2016). "Blockchain technology in the Internet of Things." IEEE Internet of Things Journal, 3(6), 1573-1585. DOI: 10.1109/JIOT.2016.2618420

15. Sharma, P. K., Singh, S., Jeong, Y. S., & Park, J. H. (2017). "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks." IEEE Communications Magazine, 55(9), 78-85. DOI: 10.1109/MCOM.2017.1601043

16. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). "Blockchain for IoT security and privacy: Thecase study of a smart home." 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). DOI: 10.1109/PERCOMW.2017.7917634

17. Zhang, H., Li, Z., & Huang, Y. (2023). "A Blockchain-based Secure Data Sharing Framework for IoT Devices." IEEE Internet of Things Journal. DOI: 10.1109/JIOT.2023.3214567

18. Alfawaz, T., & Khattak, H. A. (2022). "Integrating IPFS and Blockchain for Secure IoT Data Management." Journal of Network and Computer Applications, 198, 103335. DOI: 10.1016/j.jnca.2022.103335

19. Mishra, S., & Naik, B. (2022). "Blockchain-Enabled IoT Data Management for Smart Healthcare." Journal of Ambient Intelligence and Humanized Computing. DOI: 10.1007/s12652-022-03559-6

20. Choudhury, S., & Gupta, S. (2023). "Enhancing IoT Security Using Blockchain and Decentralized Storage." Journal of Information Security and Applications, 70, 103246. DOI: 10.1016/j.jisa.2023.103246

21. Patel, S. S., & Singh, S. (2024). "Smart Home Automation Using IoT and Decentralized Blockchain." IEEE Transactions on Consumer Electronics. DOI: 10.1109/TCE.2024.3210123

22. Thakur, D. S., & Sharma, R. (2022). "Decentralized Architecture for IoT Security Based on Blockchain." Future Generation Computer Systems, 139, 302-312. DOI: 10.1016/j.future.2022.04.007

23. Kumar, A., & Sahu, R. (2023). "Data Privacy in Smart Homes: A Blockchain and IPFS Approach." Journal of Cybersecurity and Privacy, 3(1), 143-161. DOI: 10.3390/jcp3010010

24. Gaurav, A., & Srivastava, S. K. (2022). "IoT-based Smart Home Automation: Challenges and Solutions." IEEE Access, 10, 10245-10258. DOI: 10.1109/ACCESS.2022.3146684

25. Khan, M. A., & Ahmad, F. (2023). "Secure Smart Health Monitoring System Using Blockchain and IoT." Sensors, 23(4), 2101. DOI: 10.3390/s23042101