LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATION

S.NO	ACRONYMS	ABBREVIATION
1	IoT	Internet of Things
2	IPFS	InterPlanetary File System
3	ESP	Electrically Stimulated Periphery
4	MQTT	Message Queuing Telemetry Transport
5	HTTP	Hypertext Transfer Protocol
6	Wi-Fi	Wireless Fidelity
7	CID	Content Identifier
8	IDE	Integrated Development Environment
9	UI	User Interface
10	API	Application Programming Interface
11	OS	Operating System
12	JSON	JavaScript Object Notation
13	SSL	Secure Sockets Layer
14	TLS	Transport Layer Security
15	HTTP	Hypertext Transfer Protocol
16	GPIO	General Purpose Input/Output
17	LAN	Local Area Network
18	WAN	Wide Area Network
19	DNS	Domain Name System
20	IP	Internet Protocol
21	P2P	Peer-to-Peer
22	GUI	Graphical User Interface
23	VPN	Virtual Private Network
24	SDK	Software Development Kit
25	DHT	Distributed Hash Table
26	PoS	Proof of Stake

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. We discuss the advantages of using IPFS in terms of scalability, security, and privacy, and compare it to traditional centralized approaches. Additionally, we explore the potential challenges and limitations of using IPFS in IoT environments, such as network latency, resource constraints, and compatibility issues. To demonstrate the practical application of IPFS in IoT communication, we present a case study involving a decentralized sensor network. The case study illustrates how IPFS can be used to securely store and share sensor data, enabling real-time monitoring and analysis. We also discuss the implementation de tails, including the choice of IPFS libraries, network configuration, and security measures. In conclusion, this paper provides a comprehensive overview of IPFS and its potential as a decentralized and secure solution 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.