

BLOCKCHAIN FOR MASS IOT DATA STORAGE AND DISTRIBUTED DATA MANAGEMENT

Kanwal Naheed¹, Fatima Anjum^{*2}, Ayesha Iqbal³, Saima Farhan⁴, Samra Habib⁵, Misha Asif⁶

^{1,*2,3,4}Department of Computer Science, Lahore College for Women University, Lahore, Pakistan

^{5,6}Department of Computer Science, University of Central Punjab, Lahore.

¹kanwal.naheed46@gmail.com, ²fatima.anjum@lcwu.edu.pk, ³ayesha.iqbal@lcwu.edu.pk,
⁴saima.farhan@lcwu.edu.pk, ⁵sammrahabib@gmail.com, ⁶mishaasif333@gmail.com

DOI:<https://doi.org/10.5281/zenodo.17511499>

Keywords

Security, IoT, Massive data storage, IPFS, Blockchain Data Management

Article History

Received: 12 September 2025

Accepted: 18 October 2025

Published: 31 October 2025

Copyright @Author

***Corresponding Author:**
Fatima Anjum

Abstract

The Internet of Things (IoT) has become an integral part of modern life, enabling seamless connectivity across industries, homes, healthcare systems, and autonomous vehicles. With this rapid adoption, the volume of data generated by IoT devices has grown exponentially, creating major challenges in secure storage and management. Traditional IoT architectures commonly employ the Interplanetary File System (IPFS) for data sharing among distributed devices and servers. Although IPFS offers efficient decentralized storage, it lacks data traceability – a crucial requirement for transparency and regulatory compliance in future digital ecosystems. Conversely, blockchain technology ensures immutability and traceability through distributed ledgers but is limited by its inefficiency in handling large-scale data. To address these limitations, this study proposes a hybrid framework, Eth-IPFS, which integrates the Ethereum blockchain with IPFS. The Ethereum blockchain, enhanced through smart contracts, manages data integrity and traceability, while IPFS handles large-scale decentralized storage. Experimental results demonstrate that Eth-IPFS enhances reliability, data accessibility, and traceability, offering a robust and scalable solution for managing massive IoT data. This framework provides a secure, efficient, and transparent data management model suitable for next-generation IoT systems.

1 INTRODUCTION

The Internet of Things (IoT) is an extended network that connects objects and humans through unique address schemes so that they exchange information with each other and interact to achieve mutual tasks [5, 27]. Smart sensors, objects, actuators and devices are the key components of the IoT and can interrelates with the user and themselves. The Internet of Things (IoT) is an idea aimed at connecting the objects of the physical world with the virtual world of information technologies [7, 24]. In the new era of information technology, where information is produced, collected, managed and examined automatically rather than followed by a typical traditional processing system. All things

communicate with one another, work independently, show measurements, AS results everything becomes smarter and makes man's life much easier [35, 21]. Existing research shows that all IoT devices would be available online in the future and that they generate a lot of data that must be managed efficiently. This demands a decentralized and trustworthy storage system. For IoT, 20 billion devices are expected to be connected to the Internet by 2020, with a data limit of 507.5 ZB created by these devices. Currently, many models follow a centralized system to detect, approve and transfer data between various IoT nodes, but it fails due to a one-time failure.

The decentralized data management architecture ensures reliability, efficiency and improved data management. Therefore, it is easier and more efficient to analyze the data. Currently, IoT solutions are a centralized architecture that connects to cloud servers through the Internet [12, 37]. It continues to face a variety of security and data management challenges. The single point of failure is one of the major drawbacks of the centralized architecture through which the accessibility of the data set will be at risk. Hence it's very important to implement a fault-tolerant network as well as a tamper-proof location for the large amount of IoT objects [10, 13]. To minimize these problems, the system must exclude client server-based models and provide a decentralized storage structure. The objective therefore, is to provide a decentralized data access model for IoT, which ensures that user-data are not entrusted to centralized entities or companies, but instead is made the property of the users themselves. A distributed ledger which stores IoT data independently on several grid nodes is part of the decentralized data management solution.

To efficiently solve IoT system problems such as scalability, reliability and security, IPFS uses a peer-to-peer file storage system. Easy data storage and recovery also makes IoT networks easier thanks to IPFS. IPFS is more efficient with a shorter storage time. IPFS provides more space for big data than the blockchain can store big data files. But in IPFS everyone is able to access the file with the hash. Once the file is uploaded in IPFS the owner will no longer control the accessibility of a file. To overcome the drawbacks of the two technologies, in this architecture, a stack of blockchain and IPFS software (the peer-to-peer interplanetary file system) is used to provide decentralized data access control. Furthermore, the blockchain provides an immutable record of all data actions of IoT devices containing sensor data formation and access to IoT data. The principal objective of an improved data management system is to provide accurate data on the exact time. In the future blockchain and IoT technologies will play an important part in intelligent systems [15]. Recent studies show that blockchain technology is used to provide distributed access control and data management.

Blockchain is a special kind of database that provide a decentralized network of nodes to store data. As Blockchain's name involves a blockchain. Blockchain is the most famous technology due to its Bitcoin financial application, the digital currency that stores transactions on a blockchain. Blockchain technology is used to manage IoT data storage at the network periphery and also provides a decentralized storage system [21]. Blockchain technology cannot be used to store big data generated by IoT devices due to its cost is higher bandwidth and extra storage space. IPFS handles large files, but works like a public blockchain. Files kept on IPFS can be viewed and accessed by anyone who connects to IPFS network. The combination of IPFS and Ethereum Blockchain (Eth-IPFS) provides a decentralized network structure and resolves the downsides of both technologies. Thus, Eth-IPFS provides a fault tolerant architecture which offers reliability and accountability of data. It is a suitable platform in which miners co-operate with each other and work in groups. The activities carried out by the blockchain are continuously recorded so that no one may steal or falsify the data.

In the modern era, data is the most valuable asset, so its management is also a major concern. The large amount of data is produced within an IoT environment that must be stored and managed. In many IoT applications the enormous amount of sensors and data receivers send information to the server, which becomes huge in a short time and IoT applications have to deal with the challenges of real time data management and extraction of useful information from the whole gathered data on the server. An efficient data management is most needed for the entire situation which occurs in it network [7]. The idea of Internet of Things seems to let small devices generate consistent data which will help the service providers to take a decision based on the massive amount of data collected from heterogeneous objects. Although, IoT devices generating data at a high rate, that require extensive storage space to store it, IoT applications use a centralized system to store data that is confronted with problems such as security and failure at a single point. Moreover, this data is available to unauthorized users through

third parties who manage cloud applications. To address these concerns, the involvement of third parties should be removed from the architecture. Blockchain technology has gained popularity because of Bitcoin crypto-currency in the financial field and can also use for the non-financial field of areas to provide a secure data storage and management system. The main objective is to provide decentralized data access system with the combination of IoT and blockchain technology, so the user can get accurate data at right time with good speed and also store the huge data securely using decentralized storage system like IPFS and Ethereum Swarm and blockchain is used to store links of the data stored in these systems. Both the storage cost question and the transaction rate are managed using this technique.

As IoT technology has quickly developed to improve human life, it also faces issues related to the processing of data generated by IoT devices. This section defines the main challenges of IoT applications which are Imprecision, Heterogeneity, Scalability, Security, Availability and Integrity which are also graphically depicted in Figure 1 [33].

Inaccuracy: Data values are continuously stored for any device or object and they have to be accurate. For best data management, data quality cannot be compromised. If data is inaccurate in any system or environment all further processes and decisions are expected to be poor. Working on limited data sets is a reason of inaccuracy. Adding more data can be helpful to reduce inaccuracy [22].

- **Heterogeneity:** Different devices produces

different types of data with the variation of data type from character to integer. Managing of data produced by heterogeneous devices is one of the main challenge faced by IoT applications. Data produced by devices in parallel routine so all nodes have different execution commands. Due to heterogeneity of data, access to any specific information on request can be challenging [1].

- **Scalability:** A system or computer application should be able to deal with large amount of data. Some computer systems are limited to a specific size of data and performance is effected in case of growth of data. Scalability is a main issue in many systems. Upward scalability is always better for a system as every user or system utilizes full resources of a system so data scalability should be high that if there is a need to shift data from a small OS to large OS, it doesn't affect performance.

- **Security:** Protection of data from unauthorized user is a main element of data management. Data security contains hashing, digital signatures and many cryptographic methods. Data encryption while storing or transmitting data is a very important aspect. If data is not secured properly it can be easily hacked or tampered by unauthorized systems [22, 12].

- **Integrity:** Data consistency and maintenance is guaranteed in data integrity. To store, process and retrieve data from a system, integrity is essential. Integrity of data assures user that no outside force can tamper or hack information. Data should be trustworthy throughout lifecycle.

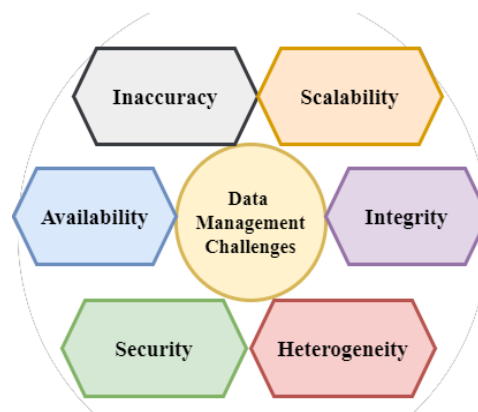


Figure 1. Data Management Challenges.

- **Availability:** Data availability is a term which ensures that data which has to be accessed and needs to be function is always accessible when it is needed. This capability shows the level to which data can be continually retrieved by applications, processes and end users [22].

2 Related Work

Many researches have been done on Internet of Things and Blockchain, but the area of focus of this research is to data management created by IoT devices. Mostly researchers proposed the models for data management were centralized. In this research work, focus is on 'decentralized system with secure data management' instead of centralized approach.

Bachhav and Mahalle proposed 6-layer architecture which is used for better data production, collection, storing, processing, combination and delivery. The data layer deals with data processing for filtering, preprocessing and processing. To address both archival query and real time exploration and service needs cross layer approach is also added in proposed framework [7]. Another efficient system which identified the collection, administration, positioning and removal parts of IoT data is defined in [10], Which provides necessary data tracing of items as they transfer data to cloud platform, accurate information value at higher speed with flexible resources. Park et.al. (2018) introduces an efficient and flexible Ethereum based system which covers drawbacks of centralized systems. It runs on p2p systems and assures integrity and immutability and has low maintenance cost [23]. A dynamic sensor data in which the system continuously captured the data from heterogeneous sensor and transformed it to unified format for processing [20]. For data compression PSO algorithm is used which avoid the redundancy and reduce the load of database. A solution to overcome the drawbacks of centralized system such as their delay on server side and single point failure was proposed by [3], which presented improved system efficiency and throughput, a decentralized system has been introduced integrated with a file storage system IPFS. Joseph presented new weather monitoring

system which uses various sensor values. Raspberry Pi is used to graphically show parameters of weather monitoring like temperature and humidity. Here raspberry Pi is used as server [18].

A relative analysis designed topology architecture system to provide energy efficient solution for a smart building, in order to manage collected sensors' data is presented in [25] to find better and new solutions for smart city which has low cost, better environment and friendly applications. Swamy & Sowmyarani proposed a system which examines the composed data from the sensors to observe the environment periodically. To store the gathered data mongo DB is used and also supports high availability of operations. Sensors produced huge and repeated data to overcome the load of network RDMA algorithm is used [29]. A secured mechanism to stock the IoT devices data on cloud by applying AES and RSA cryptographic methods was presented in [9]. The system upload IoT devices data on public cloud but store organizational information on private cloud so the organizations have more secured and managed cloud architecture. In 2019 [11] discussed different fifteen NoSQL databases basic characteristics such as the key value store, column store, graph databases and document store and then analyzed which database provide better performance for data processing, then some key points described to help the enterprise choose best according to their need. Different research topics focused on common problems of on-going data management and analytics difficulties in the development of real-world applications. Decentralized architectures for IoT environment which handles the data privacy and data access management were presented in multiple researches such as [32, 36, 26, 6].

As the growth of data generated by IoT devices lemmatized the transactions throughput and storage capacity of blockchain Systems. It also conclude that the combination of both IOT and blockchain technologies can provide a powerful methodology which helps to give best business models for distributed IoT applications and also focus to find further research on this open challenge [2, 14, 16, 4].

An improved version of management and monitoring of IoT devices by handling the CRUD operations and data is stored in blockchain is discussed in [19]. When any change occur in the system, configuration set to new default setting, Chaintable is most important part of this framework to handles authorization and access to blockchain.

3 Research Methodology

The proposed system (Eth-IPFS) explained in this section is intended to integrate IoT sensor data with IPFS to store the actual data and then store the pointers of actual data in blockchain. To calculate results and conclusions, dataset of weather forecasting and monitoring is used as a case study. Different parameters of weather like temperature, humidity and pressure values are collected by sensors and are available in csv file format [30]. Large data costs very high to store in blockchain. To overcome this issue, IPFS is used to store data. The scope of Eth-IPFS is to store data which has non repetitive value of

weather forecasting in Ethereum using decentralized storage system (in this case IPFS) because blockchain costs very high to store large scale data [31, 8].

3.1 Proposed System Architecture

To explain the Eth-IPFS architecture, a layer architecture is depicted in figure 2 showing the 4 layers including the data collection layer, the network layer, the storage layer and the application layer.

3.1.1 Data Collection Layer:

Within the data collection layer, data is collected from a variety of IoT sensors and devices. To get the sensor data generally raspberry Pi is connected to the hardware and software to manage the data. However, for the present study, a set of weather monitoring data is used to conduct various operations. The gathered data is available in the CSV file. It contains data from various sensors named in the table 1.

Table 1: Different Sensors used in Experiment.

No	Sensor Name
1	Humidity
2	Air Pressure
3	Temperature
4	Light

3.1.2 Network layer:

The devices used in this layer are used to connect the devices to the Internet or network and help accomplish the task of collecting the sensor data. This layer is used for inter-device communication so that they can exchange information.

3.1.3 Storage Layer:

The storage layer is used to store important data collected by the sensors within the IPFS peer-to-peer network. It is also responsible for managing the blockchain which is used as the pointer for real stored data. Each node is replicated with the same storage data. This layer integrates the IoT environment with the IPFS network by storing sensor data into the Inter Planetary File System (IPFS); a decentralized file system. The use of the

blockchain keeps a record of the stored data and also provides the characteristics of time-stamping and data verifiability.

3.1.4 Application Layer:

The application layer provides different services and applications to users or clients by retrieving processed data. Applications used for tasks such as registering and observing devices. The proposed model offers an improved and efficient data storage network, enabling users to store and process application data.

3.2 Proposed Storage System Design

Eth-IPFS is a distributed storage system that includes IPFS (interplanetary filesystem) and Ethereum blockchain. The Eth-IPFS design

shown in Figure 2. Weather monitoring data are used as a case study to analyze the results of the proposed system. The data file is stored in IPFS,

IPFS creates a hash of the file and then hash is stored in an Ethereum blockchain.

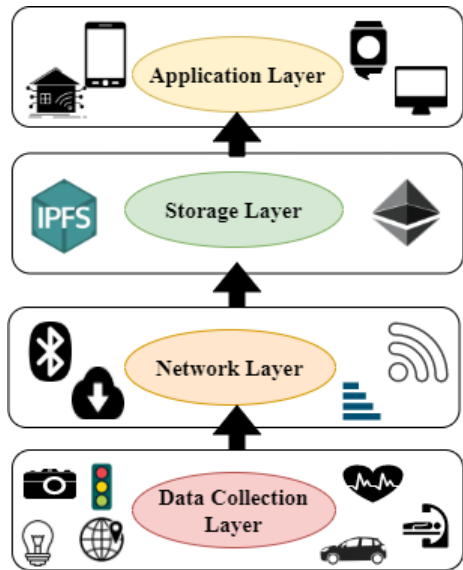


Figure 2. Proposed System Architecture Layers.

A decentralized application is created that displays the hash of the IPFS file, the block number, the Ethereum contract address and the gas used.

Ethereum blockchain returns the transaction hash according to a set of clever contract rules. The data can be recovered by the users later on if needed.

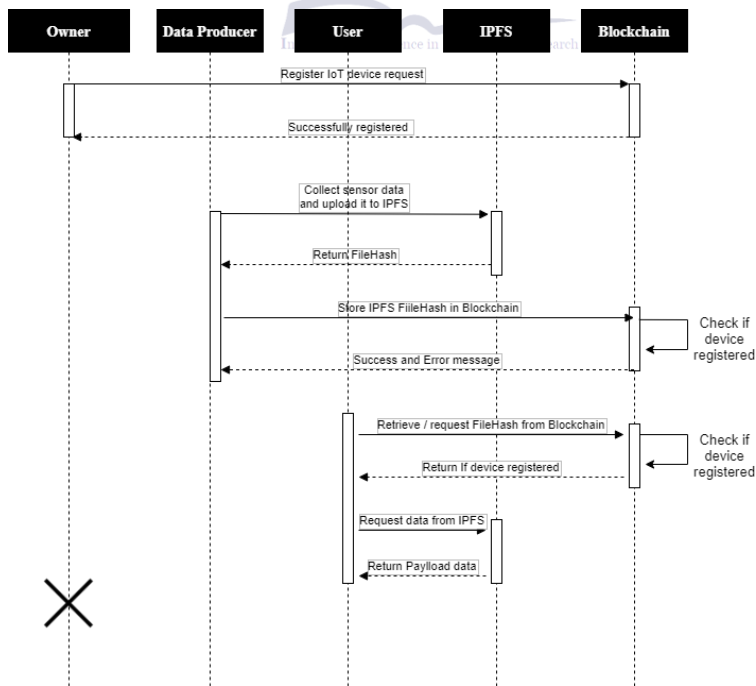


Figure 3. Interaction between different components of the system.

Figure 3 defines the basic steps for collecting and retrieving data after pretreatment, verification and storage.

3.3 Data Collection and Retrieval Algorithms

Sensor's Data Collection in IPFS:

The overall steps for storing sensor data or payload in IPFS explained in Algorithm 1. In this case, the dataset is Australian Meteorological Monitoring dataset that is recorded by the amount of time per hour. As with meteorological monitoring, several sensors are used to monitor the climate and produce data. To store the readings per day of the sensor package SensorDataList is used and the structure is as follows.

```
"data": "type": "SensorDataList",
"links":
["hash": "QmQduvUQBdnNtuhBB6fUuf4NZCG
hxDo3GwT3gigZMX14o6",
"name": "2017091112", "size": "545"]
```

Table 2: System Specifications.

Resource Name	Specifications
System Model	Dell Latitude E6540
Operating System	64 bit Windows 10 Pro
CPU	Intel Core i74810MQ
RAM	12GB

Sensor's Data Retrieval from IPFS:

In Algorithm 2 steps are described to fetch the file hash from Ethereum blockchain and then retrieve the information or data file stored in IPFS. The file is requested from the authenticated user device. The registered user can one only access and use the data.

Algorithm 2: Sensor's Data retrieval and Usage

- 1 Input: data, sensor information
- 2 Result: Retrieve data, Payload from IPFS. information retrieval request from node n
- 3 Check the registration of node n node n is registered
- 4 Check the requested hash hash matched with the requested one

It gives the whole idea which steps need to follow to implement the proposed systems as we require.

The type is store in data element. The links attribute store the IPFS hash address of sensor data package. The name attribute or variable store the name of the file or Object ID.

Algorithm 1: Data Collection & Payload Storage in IPFS

- 1 Input data, sensor information.
- 2 Result Collect and read data, Store in IPFS. true
- 3 Get sensors data information
- 4 Get timestamp
- 5 Create payload of data
- 6 Store payload in IPFS
- 7 Get IPFS file hash of the assigning files stored
- 8 Send the IPFS file hash in blockchain.

- 5 Return the requested file hash from blockchain blockchain payload hash matched with IPFS file hash
- 6 Return file from IPFS
- 7 File not found error
- 8 Permission denied for file
- 9 n node is not registered

Performance and cost analysis of blockchain based data management system is tested upon local machine which specifications described in Table 2.

4 Results and Discussion

4.1 Centralized & Decentralized Storage System Comparison

Research concludes that many organization used centralized data storage system for data management and storage but it is not a good approach. Centralized systems have many drawbacks as many researchers explained. The results shows the comparison of performance with existing model vs the proposed model Eth-IPFS using different parameters.

4.2 Mongo DB Storage & Access Time

For proposed research analysis, results have concluded for an existing data storage system

MongoDB which is a NoSQL database. It has less storage space and has no ACID guarantee. It has data redundancy that's why it consumes extra memory usage. It stores maximum 16mb document but for large files it uses gridsapi which helps to store large files like images and video etc. Data storage time and access time per second is calculated and graph is given in Figure 4. MongoDB access files in less time because files are already available in system but its drawback is if server is down data cannot be accessed.

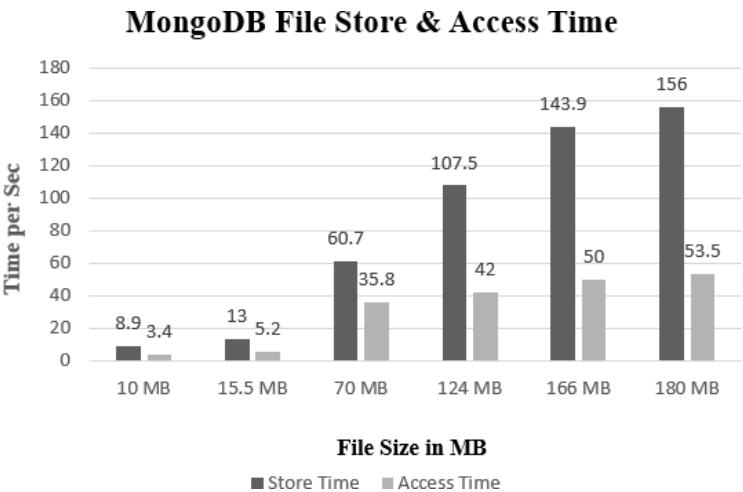


Figure 4. MongoDB Storage & Access Time.

4.3 Eth-IPFS File Upload & Download Time

Eth-IPFS contains Ethereum blockchain based system. It is a decentralized storage system which can stores large data files in form of hashes. It acts like a digital register which provides immutability and large space for IoT data files. Blockchain stores data in form of blocks with has data and its

timestamp with it [34, 28]. Blockchain itself can't store large files, so a file storage system IPFS is integrated with Ethereum. Data files are stored in IPFS, it creates hash of file and then hashes are stored in Ethereum blockchain. Ethereum stores and manages data efficiently. Data storage time per second is calculated and graph is given in Figure 5:

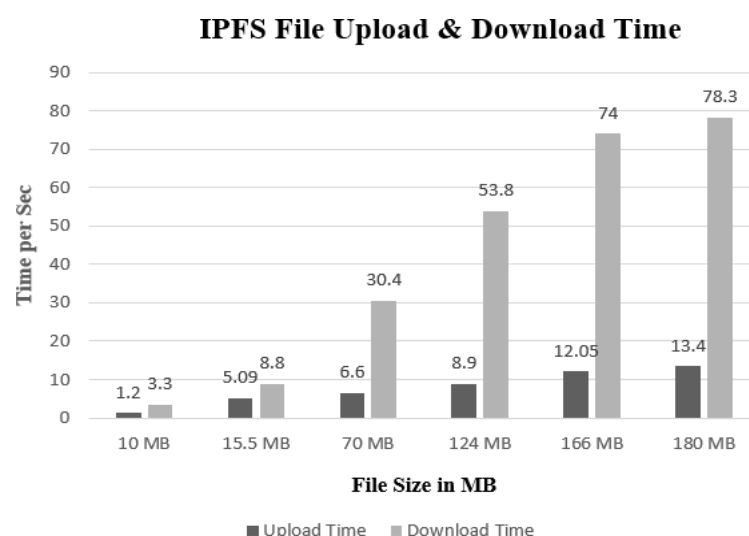


Figure 5. Eth-IPFS File Upload & Download Time.

The transaction per second is computed in the event of block chain. During data storage, the transaction requires certain charges to be paid for the calculation by the user. For example 20gwei (Gwei is also called nanoether, or simply nano, to denote the ninth power of the fractional ETH) per unit of gas has to be paid for deploying smart contracts. Gwei is the most commonly used unit of ether because "gas" prices are easily specified in gwei. For example, rather than saying that your gas costs 0.000000001 ether, you can say that your gas costs 1 gwei. The implementation of a proposed framework obtains data from the sensors of a data set, generates a useful load and then stores it in IPFS. It returns a file hash that is later submitted to the blockchain to be exploited and stored. IPFS uses the smallest processor power and its performance was very fast. The proposed model is fully decentralized and addresses all existing

storage architecture issues. While its download time is more than Mongo dB, but it does not have a single fail point. Data availability is high for the Ethereum and IPFS blockchain.

4.4 Eth-IPFS & MongoDB Storage Time Comparison

Figure 6 describes file storage time in distributed and centralized storage systems that are at-IPFS and MongoDB, respectively. As shown in Figure, Eth-IPFS is more effective at storing the file in the system than MongoDB.

4.5 MongoDB & Eth-IPFS Throughput Comparison

The figures 7 below represents the flow rate of the MB/sec system. In case of Ethereum blockchain integrated with IPFS (Eth-IPFS), the throughput of the system is high, so it is efficient compared to existing storage systems.

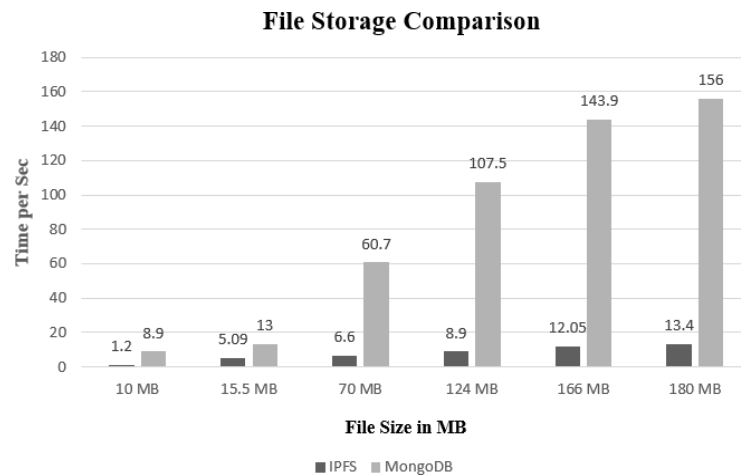


Figure 6. Eth-IPFS & MongoDB Data Storage Time Comparison.

In case of bitrate MongoDB indicates the number of operations per second (ops/sec) carried out by the threads. The graph shows that the increment of threads performs more operations per second, but when threads drastically increase the performance of MongoDB starts to fall. Since it is a centralized system, it is much less tolerant to failures. The Earth-IPFS system functions like megabits per second (MB/sec) and the Mongo DB

system functions like operations per second (ops/sec).

4.6 MongoDB and IPFS Stats Comparison

Table 3 shows stats of `mongodb.DB.Stats()` function is used to conclude stats of the database. It shows data storage sizes, index details and total data size. IPFS divide file into small chunks and send data to connected peers.

Table 3: Mongo DB Statistics.

Attributes Name	Values	Description
Db name	myDB	Database name.
Collections	2	Count the number of collections in that database.
Views	0	Count the number of views.
Objects	113140	Count the number of objects in the database across all collections.
avgObjSize	432.1847003	The average size of each document in bytes.
datasSize	48897377	Total size of the uncompressed data in this database.
storageSize	8458240	Total amount of space allocated to collections.
indexes	2	Count of the total number of indexes.
indexSize	1040384	Total size of all indexes created.
fsUsedSize	1.05041E+11	Total size of all disk space in use on the filesystem where MongoDB stores data.
fsTotalSize	1.20032E+11	Total size of all disk capacity on the filesystem where MongoDB stores data.

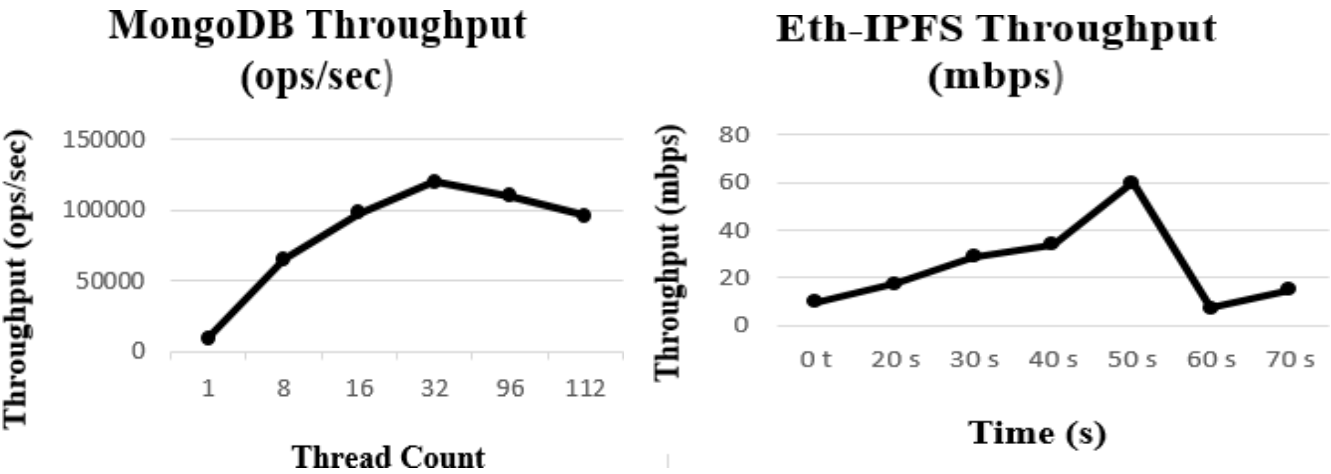


Figure 7. Throughput Comparison.

Bitswap is an IPFS module for exchanging datasets. Bitswap is integrated with IPFS to retrieve the file, create a wish list and recover the performance of the IPFS blockchain while connecting peers and storing data. The output of the IPFS performance shown with bitswap is given

in the Table 4. The output window displays the bit swap state when the peers are connected, shows the blocks sent and received. Additional information relates to the list of data files bitswap, sent and received by users and the number of peers in the network.

Table 4: IPFS Statistics.

Attributes Name	Values	Description
Blocks received	91	Blocks received by this peer.
Blocks sent	74	Blocks sent by this peer.
Data received	2351044	Data received by this peer.
Data sent	2509711	Data sent by this peer.
Dup Blocks received	57	How much duplicate blocks received.
Dup Blocks sent	1267051	How much duplicate blocks sent.
Wantlist	0 keys	Show blocks currently on wantlist by other peers.
Partners	760	Peer connected to the network at that time.

4.7 Ethereum & IPFS File size Comparison

In Eth-IPFS, IPFS stores the Main Data File and the Ethereum Ledger stores the metadata of each file stored in IPFS [17]. This ensures that large files are stored on IPFS and that only the IPFS hash is saved on the Ethereum block chain. Figure 8 shows that the problem of storing large data on the blockchain is addressed and that only log data

is stored in the ledger. Afterwards, the Ethereum size grows at a very slow rate and remains stable because it only records the transaction has even the size of the files added to the IPFS increases extremely. As mentioned in-IPFS solves the problem of storing massive data directly on the blockchain.

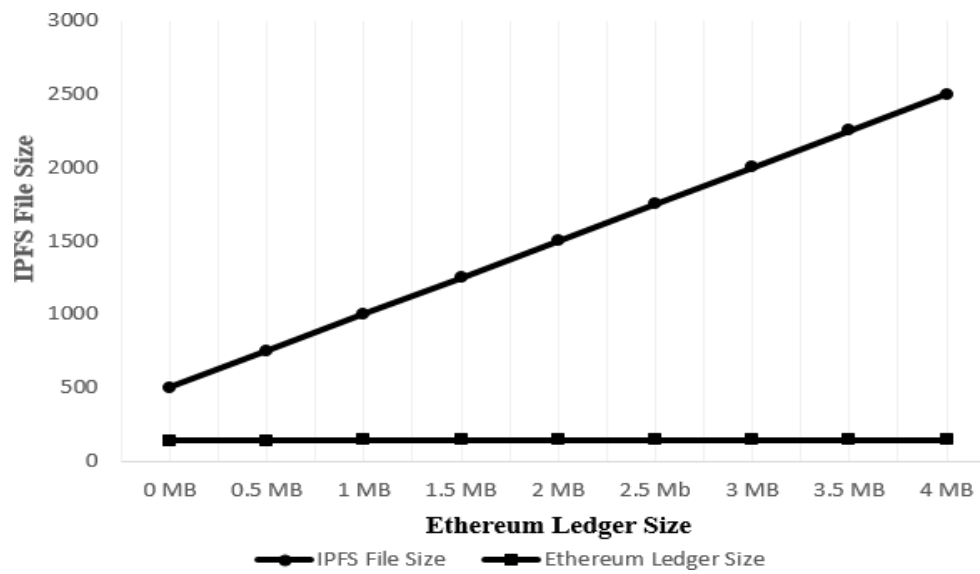


Figure 8. Comparing the size of files on Eth-IPFS and the size of file metadata on Ethereum blockchain ledger.



5 Conclusion and Future Work

The integration of IoT and blockchain technology is at its peak to deliver better systems for organizations and stakeholders. In recent years, many researchers have explored this combination of these two technologies with many benefits as well as challenges. Because of its applications, human life is very comfortable and effective. It also produces large quantities of data to process and store for processing and decision-making purposes. In this search, a decentralized data storage system based on the blockchain is proposed. To store a huge amount of distributed file system data known as IPFS is used because it deals with the challenge of scalability. It also deals with trust issues regarding third parties. The IPFS private network integrates with the Ethereum private network to show how the proposed model works and address data management challenges. The proposed DApp (Distributed Application) improves data availability and also addresses a single point of failure. The results of the storage model show that the files are well distributed among peers on the IPFS private network, where all nodes contribute to providing data. Data privacy is ensured by this feature, because files are distributed only on the IPFS private network. Moreover, transactions stored IPFS file hashes on the Ethereum block chain. Transactions cannot be modified, because they are time-stamped, digitally signed with Ethereum accounts, and validated by all network peers. The proposed model is fully decentralized in nature relative to those that already exist to ensure trust between users. The architecture also eliminates control of the third-party service provider. Another advantage of the distributed storage system offered is that users can recover data anytime. Because instead of saving the file to one centralized server, it saves the data to all IPFS network nodes. As a result, if one node is disabled, others may provide the same file.

In the future, the schema of this system should be improved by implementing the device registration process so that only authorized data could be stored in blockchain. There is also a need to enhance the scalability of the system as scalability is very important for the future as data generates and consumes more space. The storage system must filter through the sensor data, only the necessary data must be stored to reduce memory consumption.

Acknowledgment Not applicable

Declaration

Authors declare that the work presented is original and currently not under review in any other conference or journal.

Conflicts of interest

The authors declare that there is no conflict of interest in this paper.

REFERENCES

- Abbasi, M. A., Memon, Z. A., Memon, J., Syed, T. Q., Alshboul, R., 2017. Addressing the future data management challenges in iot: A proposed framework. *International Journal of Advanced Computer Science and Applications* 8 (5), 197–207.
- Ali, M., Nelson, J., Shea, R., Freedman, M. J., 2016. Blockstack: A global naming and storage system secured by blockchains. In: 2016 {USENIX} annual technical conference ({USENIX} {ATC} 16). pp. 181–194.
- Andrian, Y., Kim, H., Ju, H., 2019. A distributed file-based storage system for improving high availability of space weather data. *Applied Sciences* 9 (23), 5024.

- Atlam, H. F., Alenezi, A., Alassafi, M. O., Wills, G., 2018. Blockchain with internet of things: Benefits, challenges, and future directions. *International Journal of Intelligent Systems and Applications* 10 (6), 40-48.
- Atzori, L., Iera, A., Morabito, G., 2010. The internet of things: A survey. *Computer networks* 54 (15), 2787-2805.
- Ayoade, G., Karande, V., Khan, L., Hamlen, K., 2018. Decentralized iot data management using blockchain and trusted execution environment. In: 2018 IEEE International Conference on Information Reuse and Integration (IRI). IEEE, pp. 15-22.
- Bachhav, B., Mahalle, P. N., 2017. Data management for internet of things: a survey and discussion. *International Research Journal of Engineering and Technology (IRJET)* 4 (11), 1512-1517.
- Benet, J., 2014. Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561.
- Bokefode, J. D., Bhise, A. S., Satarkar, P. A., Modani, D. G., 2016. Developing a secure cloud storage system for storing iot data by applying role based encryption. *Procedia Computer Science* 89, 43-50.
- Cai, H., Xu, B., Jiang, L., Vasilakos, A. V., 2016. Iot-based big data storage systems in cloud computing: perspectives and challenges. *IEEE Internet of Things Journal* 4 (1), 75-87.
- Chen, J.-K., Lee, W.-Z., 2019. An introduction of nosql databases based on their categories and application industries. *algorithms* 12 (5), 106.
- Da Xu, L., Lu, Y., Li, L., 2021. Embedding blockchain technology into iot for security: a survey. *IEEE Internet of Things Journal*.
- Deepthi, K. J., Balakrishnan, T. S., Krishnan, P., Ebenezar, U. S., et al., 2024. Optimized data storage algorithm of iot based on cloud computing in distributed system. In: 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0. IEEE, pp. 1-5.
- Fan, L., Gil-Garcia, J. R., Werthmuller, D., Burke, G. B., Hong, X., 2018. Investigating blockchain as a data management tool for iot devices in smart city initiatives. In: Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. pp. 1-2.
- Hang, L., Kim, D.-H., 2019. Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors* 19 (10), 2228.
- Hewa, T. M., Hu, Y., Liyanage, M., Kanhare, S., Ylianttila, M., 2021. Survey on blockchain based smart contracts: Technical aspects and future research. *IEEE Access*.
- Honar Pajooh, H., Rashid, M., Alam, F., Demidenko, S., 2021. Hyperledger fabric blockchain for securing the edge internet of things. *Sensors* 21 (2), 359.
- Joseph, F. J. J., 2019. Iot based weather monitoring system for effective analytics. *International Journal of Engineering and Advanced Technology* 8 (4), 311-315.
- Koṣṭạl, K., Helebrandt, P., Belluṣ, M., Ries, M., Kotuliak, I., 2019. Management and monitoring of iot devices using blockchain. *Sensors* 19 (4), 856.
- Li, M., Liu, Y., Cai, Y., 2015. A dynamic processing system for sensor data in iot. *International Journal of Distributed Sensor Networks* 11 (8), 750452.

- Li, T., Liu, Y., Tian, Y., Shen, S., Mao, W., 2012. A storage solution for massive iot data based on nosql. In: 2012 IEEE International Conference on Green Computing and Communications. IEEE, pp. 50-57.
- Ma, M., Wang, P., Chu, C.-H., 2013. Data management for internet of things: Challenges, approaches and opportunities. In: 2013 IEEE International conference on green computing and communications and IEEE Internet of Things and IEEE cyber, physical and social computing. IEEE, pp. 1144-1151.
- Park, J.-S., Youn, T.-Y., Kim, H.-B., Rhee, K.-H., Shin, S.-U., 2018. Smart contract-based review system for an iot data marketplace. *Sensors* 18 (10), 3577.
- Pawar, A. B., Ghumbre, S., 2016. A survey on iot applications, security challenges and counter measures. In: 2016 International Conference on Computing, Analytics and Security Trends (CAST). IEEE, pp. 294-299.
- Plageras, A. P., Psannis, K. E., Stergiou, C., Wang, H., Gupta, B. B., 2018. Efficient iot-based sensor big data collection-processing and analysis in smart buildings. *Future Generation Computer Systems* 82, 349-357.
- Robles, T., Bordel, B., Alcarria, R., Sa´nchez-de Rivera, D., 2018. Blockchain technologies for private data management in ami environments. In: *Multidisciplinary Digital Publishing Institute Proceedings*. Vol. 2. p. 1230.
- Schoder, D., 2025. Introduction to the internet of things. *Internet of things A to Z: technologies and applications*, 1-40.
- Sun, J., El Saddik, A., Cai, W., 2024. Smart contract as a service: A paradigm of reusing smart contract in web3 ecosystem. *IEEE Consumer Electronics Magazine* 14 (1), 46-55.
- Swamy, S. N., Sowmyarani, C., 2018. Repeated data management framework for iot: A case study on weather monitoring and forecasting. In: 2018 4th International Conference on Recent Advances in Information Technology (RAIT). IEEE, pp. 1-7.
- Tahmasebi, S., Habibi, J., Shamsaie, A., 2020. A scalable architecture for monitoring iot devices using ethereum and fog computing. In: 2020 4th International Conference on Smart City, Internet of Things and Applications (SCIOT). IEEE, pp. 66-76.
- Valadares, D. C. G., Sobrinho, A´. A. d. C. C., Perkusich, A., Gorgonio, K. C., 2021. Formal verification of a trusted execution environment-based architecture for iot applications. *IEEE Internet of Things Journal*.
- Vo, H. T., Kundu, A., Mohania, M. K., 2018. Research directions in blockchain data management and analytics. In: *EDBT*. pp. 445-448.
- Wang, Y., Deng, Q., Liu, W., Song, B., 2012. A data-centric storage approach for efficient query of large-scale smart grid. In: 2012 Ninth Web Information Systems and Applications Conference. IEEE, pp. 193-197.
- Weerasinghe, N., Hewa, T., Liyanage, M., Kanhere, S. S., Ylianttila, M., 2021. A novel blockchain-as-a-service (baas) platform for local 5g operators. *IEEE Open Journal of the Communications Society* 2, 575-601.
- Wu`st, K., Gervais, A., 2018. Do you need a blockchain? In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE, pp. 45-54.

Zˇarko, I. P., Pripuzˇic´, K., Serrano, M., Hauswirth, M., 2014. Iot data management methods and optimisation algorithms for mobile publish/subscribe services in cloud environments. In: 2014 European conference on networks

and communications (EuCNC). IEEE, pp. 1-5.

Zulkarnain, M. M., Ramli, N., Nordin, A. N., 2025. Performance benchmarking of hyperledger fabric on heterogeneous hardware for iot applications. IIUM Engineering Journal 26 (3), 156-170.

