Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777603

A NOVEL APPROACH TO ADDRESS DATA SECURITY CONCERNS IN THE IOT ENVIRONMENT FOR HEALTHCARE DOMAIN USING BLOCKCHAIN TECHNOLOGY

Ochchhav Patel[a], Dr. Hiren Patel[b]
[a]SVKM, KSV University, LDRP-ITR, Gandhinagar, Gujarat 382015, India
[b]SVKM, KSV University, VS-ITR, Kadi, Gujarat 382715, India
ochchhavpatel@gmail.com, hbpatel1976@gmail.com

ABSTRACT

The Internet of Things is a powerful combination of wireless devices, radio-frequency identification, and numerous sensors that offer the challenging but powerful potential of shaping current systems with the aim of making them smarter. IoT has many different areas of application; one such area is healthcare. The health sector is another promising area for IoT, and several businesses are exploring its application in this sector. In this study, it is proposed to collect healthcare data through the IoT and store it in the Interplanetary File System using Ethereum-based blockchain technology for data security. Blockchain technology is used in IoT to ensure safety of collected data. Smart contracts are used to automatically execute, control, and record events following the terms contained in them, enhancing the characteristics already present in the blockchain. IoT-based healthcare solutions are tested on many blockchain networks. A file was used five times on both a distributed database hosted on IPFS, and a centralized database hosted on Firebase, and the times at which it was uploaded and downloaded were recorded. The method suggested addresses the scalability issue of existing approaches using public blockchain while still satisfying the data security requirements for data storage in IPFS utilizing encryption.

Keywords: Internet of Things, Blockchain, Healthcare sector, Data security, Interplanetary File System

1. INTRODUCTION

The term "Internet of Things" is used to describe a network of linked objects that may exchange data and other information through the internet. Things in the IoT are high-tech gadgets that have sensors, apps, and other electronics within. Though limited in power, these gadgets can detect their surroundings and respond accordingly. Because of the IoT's superior automation, optimization, and analytical capabilities, it has had a profound influence on virtually every sector. With the use of sensors or items incorporated in smart devices, data gathering, administration, and processing have become simpler in today's technological world. Wearables, smartphones, smart automobiles, and many more are just some of the smart gadgets that can connect to the internet and form a network that allows them to share and receive information. Inventory management, smart farming, retail, smart cities, smart healthcare, security systems, and so on all benefit from this form of network connection. The healthcare sector has also undergone revolutionary change as a direct result of the rapid growth of IoT [1].

Users may have trouble finding enough storage space for the massive volume of data generated by the proliferation of IoT-connected gadgets. As a result, numerous businesses and academic organizations frequently use the method of storing data in a cloud environment. The level of safety offered to data kept in the cloud, however, is largely dependent on the security strategy used by the cloud service provider [2]. Owing to the fact that the user has no control over the cloud data storage, the data may be in danger from the presence of a large number of hackers and malicious users. In order to link IoT devices to the digital world, a communication network is necessary. This is true regardless of the environment, whether it be a cloud or another sort. Maintaining a high level of security is therefore important in order to guarantee that the sensitive data of users will not be compromised by any adversaries [3]. In addition, the enormous amounts of data and files that are produced by IoT apps may result in an unacceptably long transmission delay, which can lower the quality of service provided by real-time applications [4]. Figure 1, given below, illustrates the exchange of data in an IOT environment.

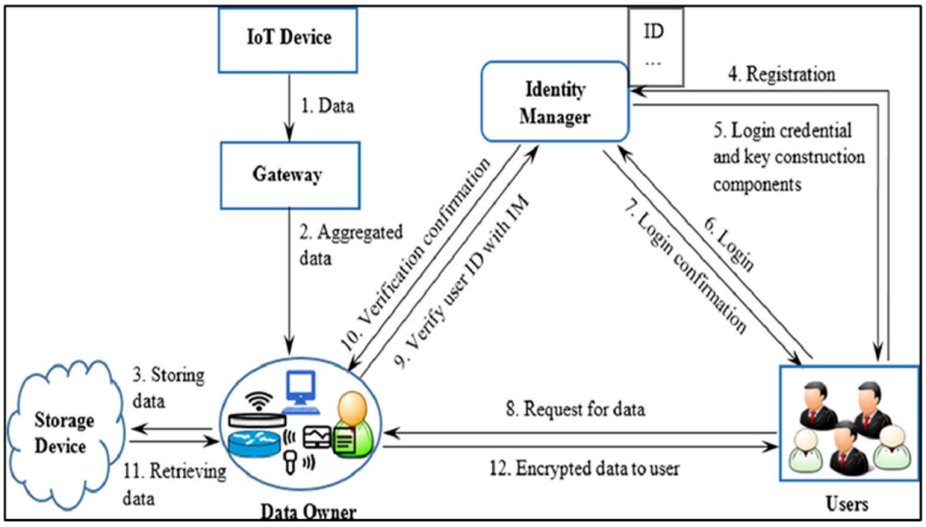

Figure 1. Data exchange in an IOT environment [5]

IoT sensors and IoT devices are utilized in the healthcare industry to track and record a patient's vital signs and other health information. Before creating any form of healthcare infrastructure model, it is imperative to safeguard the privacy of this data. To keep track of their health data, a patient, for instance, can use smart, connected devices. The patient must send the data to a remote server, such as the cloud, as local storage is insufficient. IoT sensors and gadgets are used to collect health data. Before creating any form of healthcare infrastructure model, it is imperative to safeguard the privacy of this data. A patient, for instance, might use smart IoT devices to monitor their vital signs. Because there isn't enough room on-site, the patient uploads the data to the cloud or another type of remote storage. If patient data is exposed to a malicious environment during transit, where it might be utilized for financial gain, it may be compromised [6]. As a result, patients are at risk of losing control over their medical records. As a direct result of this, patients run the risk of losing control over their medical records. Encrypting healthcare data before transmission to ensure the data's security is

thus highly suggested by a large number of experts. Several different security methods, including digital signatures, public-key cryptosystems, and authentication algorithms, can guarantee the secrecy, authenticity, and integrity of stored data. However, the majority of the available systems do not ensure the confidentiality of healthcare data, the unforgeability of ciphertext, or the integrity of the data. The issues that were discussed earlier serve as motivation for the development of a system that ensures the identities of patients are not revealed during the process of transmission and that an attacker is unable to get the ciphertext [5]. Blockchain technology is constantly being improved and is finding more and more applications in the current world. Cybersecurity is one of the relevant fields in which it has been researched and utilized successfully. The infrastructure of blockchain makes it very practical to handle the existing security concerns in areas such as IoT devices, networks, and data while it is being sent and stored. Figure 2, given below, depicts the role of blockchain in data security.

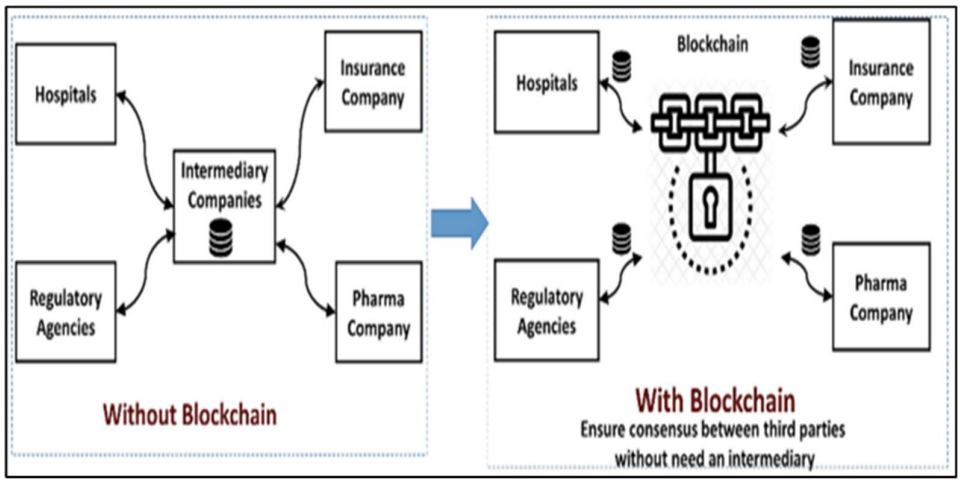

Figure 2. Role of blockchain in security [7]

As far as security for IoT devices is concerned, blockchain is becoming increasingly popular. Additionally, blockchain data [8] and network security are also important components. Better authentication and data transmission protocols may be implemented using blockchain technology to safeguard IoT devices. Due to the default weak security settings, hackers might be deterred from breaking into these devices. Networks can be protected by the technology's strict architecture to thwart illegal connections and communication. Blockchain's encrypted blocks, which can only be seen by the persons involved in the communication, make data transfer and storage safe and immune to tampering. The security needs of the IoT can be met with the help of blockchain technology because its most notable characteristics, such as decentralization, integrity, and anonymity, can boost IoT security. We identified a research gap in our planned study were found that some unresolved issues, such as centralization, data privacy, scalability, user anonymity, and performance, still need to be addressed. The aforementioned problems can be resolved by using blockchain technology, which also offers security, immutability, scalability, a trustworthy platform, and decentralization in the IoT based healthcare industry.

This study is organized into the following sections: In the first section, an overview of IoT and blockchain technology and their applications in healthcare, as well as the challenges of data security and the solutions offered by blockchain, are presented. In Section 2, the related work of the authors is discussed that has already been accomplished with medical healthcare system enabling technologies like the IoT and blockchain also mentioned the background study is given, followed by problem formulation. Proposed methodology and research objectives of this study mentioned in Section 3. Section 4 is the result and discussion, which describes various techniques used in this study along with the proposed methodology and results, and workflow of the IoT-blockchain-based medical healthcare system. Final Section 5, presents the conclusion and future scope of the study.

2. METHOD

The following section provides a brief overview of the literature reviewed by various authors.

Wu et al., (2023) [9] observed that most medical data is sent without encryption across a potentially vulnerable channel, putting patients at risk of unauthorized access and manipulation. The inefficient storage and archival of large amounts of unprocessed medical data on the cloud is another problem. As a result, this work offers a block-chain and multi-access edge computing (MEC)-based strategy for sharing medical resources in the near domain. The method employs device-to-device (D2D) communication to provide reliable and productive information exchange between various medical gadgets. Using ShangMi cryptography techniques, medical data is encrypted and decrypted before being processed by the MEC. Finally, the blockchain is implemented to safeguard information and prevent alterations. The simulation results demonstrate that the method is efficient; the security analysis proves that it is secure.

Ali et al., (2022) [10] explained that device connectivity raises security, trustworthiness, dependability, confidentiality, and other issues. This study proposed a hybrid deep neural network group theory (GT)-based binary spring search (BSS) technique to address these concerns. IoT network intrusion is detected using the provided method. Blockchain was used to develop privacy-preserving technologies first. Blockchain is employed as a database, however, these solutions have concentrated on data storage. Blockchain is recommended as a distributed database with homomorphic encryption to protect search and keyword-based access in this study. A secure key revocation mechanism and policy changes are also included. As a consequence, a safe patient healthcare data access scheme is created using blockchain and trust chains to address the efficiency and security difficulties in present schemes for exchanging both forms of digital healthcare data.

Almaiah et al., (2021) [11] summarized that the purpose of this study was to present a novel system that makes use of heuristic, signature, and voting detection techniques to determine the most effective preventative steps that can be taken to identify harmful and security risks that make use of blockchain technology. In this system, the cluster head node (CN) combines the functions of the three detection systems with those of Blockchain to identify malicious sensor nodes. Additionally, to detect malicious nodes in WSNs, CN makes use of essential criteria such as sensor node-hash value, node signature, and voting degree. During the

simulation of the proposed method, the total outcomes statistic showed that 94.9% of malicious messages were effectively recognized and identified.

Panda et al., (2021) [12] This study attempts to solve these problems by developing a distributed IoT architecture that is built on the blockchain and makes use of hash chains for cryptographic key management. The suggested architecture takes advantage of some of the most important features of blockchains to protect users' data privacy in IoT and provide a safe framework for communication. In addition to that, a method for the production and administration of keys that are both safe and effective for mutual authentication across communication entities is proposed in this study. The suggested method makes use of a technique called a one-way hash chain to deliver a collection of public and private key pairs to the IoT devices. This gives the key pairs the ability to independently validate themselves at any moment. The results of the study demonstrate that the suggested method performs significantly better than the standard techniques.

Velmurugadass et al., (2021) [13] developed a blockchain architecture that is put to use in the IaaS cloud for evidence collection and provenance preservation. Registration of users, authentication of users, encryption of data, storage of data, tracking of user activity, and data mining from the controller are the components that make up the system that is being presented. The Elliptic Curve Integrated Encryption Scheme (ECIES) technique is used to encrypt the packets before they are sent to the cloud server from the IoT devices. The system's overall safety has significantly increased as a direct result of the decision to implement a distributed design. The most recent approach was implemented, in addition to producing excellent outcomes that require a minimal amount of processing overhead. The data from the software-defined networking (SDN) controller and the blockchain are both available for analysis. This information may be put to very good use in determining who is responsible for the changes that have been made to the data.

Rajawat et al., (2021) [14] assumed that there is a rise in both human resources and security dangers associated with managing huge amounts of data, such as that generated by IoT devices or individuals' medical records. Healthcare IoT addresses these problems by improving the standard of care provided to patients while decreasing healthcare spending. Blockchain technology provides a safeguard for sensitive medical information by ensuring that any changes to the data are immediately reflected in updated simulation results by generating a unique SHA256 hash for each record. As each node verifies each block using the SHA256 hash technique, no malicious actor can tamper with the contents. Based on the criteria of verifiability, appropriateness, extensiveness, uniqueness, robustness, and coercion resistance, a blockchain-based model with a consensus mechanism and the SHA256 hash algorithm was proposed.

Chenthara et al., (2020) [15] examined the way to protect patients' personal information while allowing healthcare professionals and other organizations to collaborate on patient care in a decentralized setting. Using blockchain technology, the authors of this study create a privacy-protecting framework called Health Chain, which protects the confidentiality, availability, scalability, and integrity of electronic health records. This health chain infrastructure is based on Hyperledger Fabric, a distributed ledger system that uses Hyperledger Composer to store electronic health records (EHRs) in a distributed ledger. In addition, the IPFS data is secured with the SHA-256 hashing technique, making it a secure blockchain

alternative for EHRs. Results show that the proposed model is effective in terms of security, improved information privacy, improved data scalability, interoperability, and data integrity when it comes to the sharing and accessing of health records between many stakeholders across the health chain network.

Mohanta et al., (2019) [16] suggested that to make the most of the IoT, concerns around data privacy and data security must be adequately addressed. As a decentralized system, blockchain technology has shown a lot of promise in the field of cybersecurity. According to the findings of the study, the majority of the concerns regarding the privacy and safety of IoT devices may be resolved by utilizing blockchain technology in the form of smart contracts, digital signatures, and the mining process. It is possible to construct an IoT application using a blockchain platform such as Hyperledger Fabric or Ethereum. This type of application offers a secure and tamper-proof solution. Blockchain technology's distributed architecture explains its high level of security and resistance to manipulation. The study concluded that the distributed blockchain approach can provide a solution to the present problems with privacy and security that are associated with IoT applications. Further study could aim at putting IoT into real-time applications.

Werder et al., (2022) [17] This study presented an overview of the most recent advancements in blockchain and artificial intelligence (AI) and discussed some of the innovative solutions that could be put into place to speed up biomedical research and give patients more control over their health data while also offering financial incentives for continuous monitoring of their vitals. This study offers a fresh concept for assessing and rating individual files, such as taking the information's value across time and in various circumstances into account. This study lays out a roadmap for a decentralized personal health data ecosystem powered by blockchain that uses consensus algorithms to support novel approaches to drug discovery, biomarker development, and preventative healthcare. If the data is dispersed in a secure and open market supported by blockchain and deep learning technology, regulators might be able to come up with a solution, and everyone, including patients, might recover ownership over their data, including medical information.

Li, F. (2021) [18] Secure storage, dependable exchange, access management, and privacy protection of medical data are the primary points of discussion in the research article [18]. They developed EHR Chain, a blockchain-based EHR system utilizing attribute-based and homomorphic cryptosystems, to overcome problems and achieve the integrity and traceability of medical data. In order to achieve high capacity and safe storage of EHR data, they first combined blockchain with IPFS.

Zaabar (2021) [19] Utilizing blockchain technology to improve the security and privacy of electronic health records (EHRs) is the main objective of HealthBlock [19]. To overcome the drawbacks of centralized storage, they developed a novel approach that makes use of decentralized databases. Patients' electronic health records (EHRs) are stored in the decentralized OrbitDB using the IPFS database. Additionally, by utilizing Hyperledger Composer to store hashes of saved data and manage access when retrieving it, they have established a blockchain network based on the Hyperledger fabric. By addressing recognized security flaws in existing systems for smart healthcare, the suggested blockchain-based architecture intends to improve the stability of healthcare management systems.

El Majdoubi (2021) [20] Researchers [20] developed the SmartMedChain architecture, an end-to-end blockchain-baseband privacy-preserving solution, for data sharing in the context of s-healthcare. They have used the Kafka consensus protocol with a permissioned blockchain. The InterPlanetary File System (IPFS), a distributed data storage system with excellent durability and scalability, has been used to store encrypted health data.

2.1 Background study and problem formulation

In the past ten years, the IoT has evolved into an innovative transformation. IoT is concerned with many different types of networked smart devices. Various smart application environments may be monitored, read, and accessed via smart things. There are several obstacles that must be overcome to develop a successful IoT application, including network traffic, capacity constraints, mobile devices, security concerns, and privacy issues. In order to use IoT in the real world, issues related to accessibility must be resolved. These issues include concerns over data security, privacy, administration, and so on. This study begins by describing the present state of security and privacy issues in IoT software. The study indicates that many concerns with the privacy and safety of IoT devices may be solved with the help of blockchain technology, including its smart contracts, digital signatures, and mining operations. The Hyperledger Fabric or Ethereum blockchain platform may be used to build an IoT application that is both tamper-proof and secure [15]. There are a variety of security and privacy concerns that need to be addressed before an IoT application can be developed and deployed, and before the underlying security of the system can be considered. Threats to users' security and privacy are only two examples of the many problems that might arise while implementing an IoT application. In order to solve these issues, this study uses the combination of IoT and blockchain to enable the autonomous operation of a smart device without using any centralized authority. It can also track how devices communicate with each other. In this study, the data file is encrypted with the Advanced Encryption Standard-Cipher-Block Chaining (AES-CBC) cryptographic technique before being stored on IPFS. The blockchain-based approach ensures that only authorized parties may access the patient's data file. The current security and privacy issues of IoT applications would be addressed by the distributed blockchain method.

2.2 Research objectives and methodology

To provide security solutions for cyberattacks and strengthen healthcare information-sharing platforms by using blockchain.

- To solve security and privacy challenges, by integrating blockchain with IoT.
- To resolve integrated network technology by applying radio frequency devices in the healthcare domain.

To produce responsive output modules using IPFS for generating cryptographic output regarding the hash value. In this section, various techniques and technologies used in the proposed methodology are discussed, which include blockchain, the Interplanetary File System (IPFS), radio frequency identification (RFID), etc.

2.3 Techniques used

2.3.1. Blockchain

Through the use of blockchain technology, several individuals or organizations may conduct data transmission as well as financial transactions with one another without the need for a trusted third party. It is the responsibility of certain types of nodes to check and confirm these exchanges. A blockchain may be thought of as an inclusive financial log or record that contains approved and authenticated copies of every transaction. A blockchain is a distributed ledger that is built on a network of millions of computers, which are referred to as nodes. It is an architecture for a distributed database in which each node takes on the role of a network administrator and joins the network of their own volition. A blockchain cannot be hacked because there is no centralized information in its design. This makes it almost impossible to hack. The design of a blockchain may accommodate a growing list of ordered documents that are referred to as blocks. Each block is responsible for keeping a timestamp as well as a link to the prior block. Figure 3, given below, illustrates the general framework of blockchain.

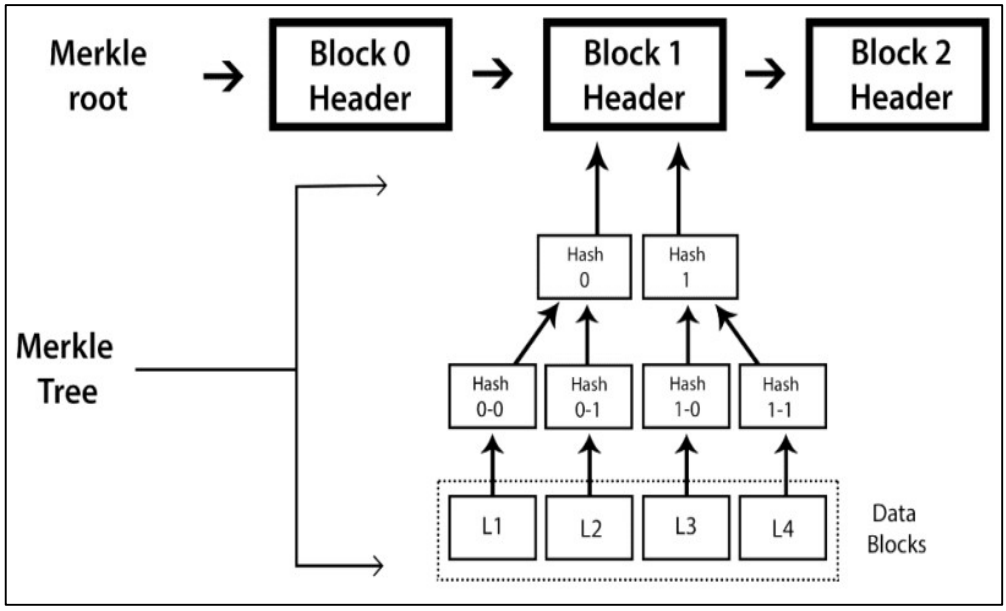

Figure 3. A general framework of Blockchain [21]

The information on a blockchain is stored in a distributed ledger made up of computers called nodes. It's a great method of keeping sensitive information safe within the system. With the use of this technology, sensitive information may be safely sent between parties. With this handy tool, all the relevant files could be stored safely in one convenient place. The use of blockchain technology expedites the search for trial participants who meet specified criteria. The blockchain is a P2P network of computers, known as nodes, that securely saves and records information about past transactions without relying on any central authority [22]. Figure 4, given below, illustrates the step-by-step workings of blockchain technology.

The network's capacity to store and transmit data enables reliable cooperation by maintaining a running log of past and present events. This tool can link many systems to

provide insight on the value of a patient's treatment. Blockchain's immutability and security are so widely understood. The three key terms in blockchain are "blocks," "nodes," and "miners." Information is not kept in a single repository on the blockchain. The blockchain is instead distributed and duplicated over a network of computers. Every computer in the world automatically updates the blockchain as a new block is added [24].

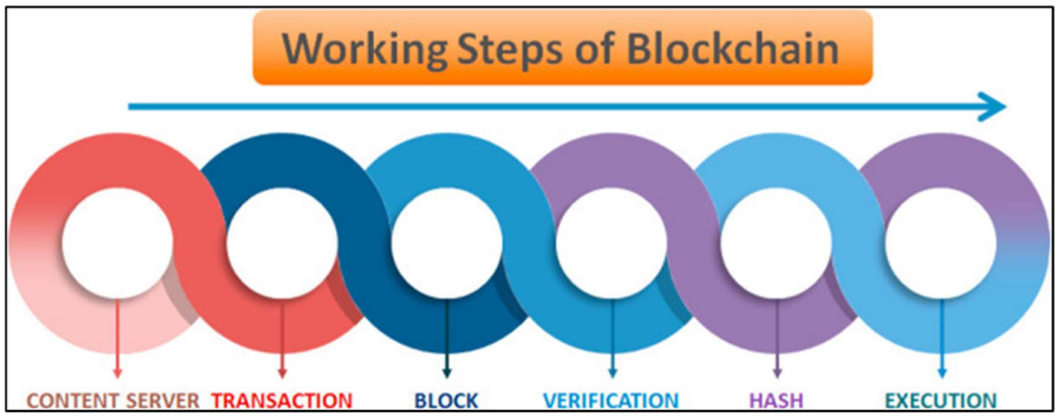

Figure 4. Working of Blockchain [23]

2.3.2. Ethereum

Ethereum is a blockchain platform that is open source, decentralized, and distributed across several computers. It was created in 2014 by Vitalik Buterin after being influenced by the Bitcoin cryptocurrency. In the same way that it is utilized in Bitcoin, the elliptic curve digital signature algorithm is put to use in Ethereum. The discrete logarithm problem serves as the basis for elliptic curve cryptography, which, when solved, results in a pair of keys. Ethereum uses an elliptic curve known as Secp256k1 to secure its network.

2.3.3. IPFS

A decentralized file-sharing network called IPFS identifies files based on the information they contain. It uses cryptographic hashes, which are conveniently stored on a blockchain. However, users cannot directly share files with other users via IPFS [25]. It uses a distributed hash table to collect data on file locations and node connections. A peer-to-peer, decentralized file-sharing system called IPFS. The innovative contribution of IPFS is the replacement of conventional geolocation with content-based addressing. To put it another way, the hash function is required rather than the data's address. An individual hash is assigned to each file that is posted to the IPFS. This file's hash might be easily located if it is known. IoT data is created in a safe environment and then preserved in IPFS to guarantee that only permitted parties have access to it. The study utilized the AES-CBC cryptographic method to encrypt data files. The primary concern of this study is ensuring the privacy, veracity, and management of sensitive medical information [26].

2.3.4. RFID Reader-Writer and Tags with MCP3008

(i) Radio Frequency Identification (RFID)

RFID offers a solution that may be used to establish the "last mile" link in a connected world, often known as the IoT. In terms of supply-chain management, RFID has been largely used by the retail and construction sectors, where it has shown to be quite useful. RFID [27] has also been used in the healthcare industry to track the activities of patients and medical staff to enhance service quality. RFID's wireless and inexpensive nature raises privacy issues. But there are privacy concerns with RFID use, such as tracking and the possibility of an attacker obtaining private information contained in the RFID tag. RFID is a technology that uses radio waves and frequencies. Objects may be automatically identified using this technique. The items in this case are completely open-ended. Items may be anything from books at a library to clothes in a department store to an automobile, etc. They're versatile enough to be utilized for tracking everything from vehicles to people to birds to animals. Its technology resembles that of barcodes in many ways. The barcode relies on direct visual contact, but radio frequency identification does not require such proximity. An RFID system consists of a reader and a tag. There are two types of RFID tags: active and passive. RFID has many practical applications, such as individual monitoring, vehicle tracking, parking lot selection, healthcare, logistics, and production [28].

(ii) MCP3008

An inexpensive analog-to-digital (ADC) converter with 8 channels and 10 bits is the MCP3008. The Raspberry Pi can read a variety of analog data thanks to the 8 channels and its ADC's precision, which is comparable to that of an Arduino Uno. This chip is an excellent choice for reading straightforward analog signals, such as those from a temperature or light sensor. The ADS1x115 series is used when more precision or additional functionality is required. It is advised to be familiar with using the MCP3008 with a Raspberry Pi in order to get the most out of your experience with the chip. Having the MCP3008 datasheet on hand is also a smart choice for a quick check [29]. Through a serial connection and the Serial Peripheral Interface (SPI) protocol, the MCP3008 talks to the Raspberry Pi. Either the hardware SPI bus or any four General Purpose Input/Output (GPIO) pins can be used to interact with the MCP3008. Software SPI is more adaptable since it can use any available Pi pins, in contrast to hardware SPI, which is a little faster but less flexible because it needs a specific set of pins. Because software SPI is easier to set up, it is typically advised to utilize it. Before the chip can be linked to the Pi, it must be placed on a breadboard. It is necessary to press a bare Dual In-Line Package (DIP) chip, like the MCP3008, onto a breadboard so that its legs cross the middle channel. Each leg of the chip cloud is connected to the breadboard in this way and reaches all of the pins on the chip [30].

3. PROPOSED METHODOLOGY

In this section, an approach to address data security issues in the IoT environment for the healthcare domain is proposed using blockchain technology. Firstly, the sender sends the patient data file, and this file is converted into a protected data file then encryption is done to transform the symmetric key using the receiver’s public key. Then the protected data file is stored on IPFS, and the fixed-value hash along with the transformed key are stored on the blockchain. Now, when the receiver sends a request for the patient data file to IPFS through the blockchain, the value of the hash is matched based on which IPFS sends the protected data file. The decryption of the protected data file is done at the receiver’s end, and the key is

transformed to its initial form. Finally, the original patient data file is extracted from the protected data file and sent to the receiver. The flowchart given in Figure 5 represents the workflow of the proposed approach.

The following steps describe the workings of the above flowchart and show how the process of data transmission takes place from the sender end to the receiver end.

Step 1: First, the sender will send the patient data file (D_P).

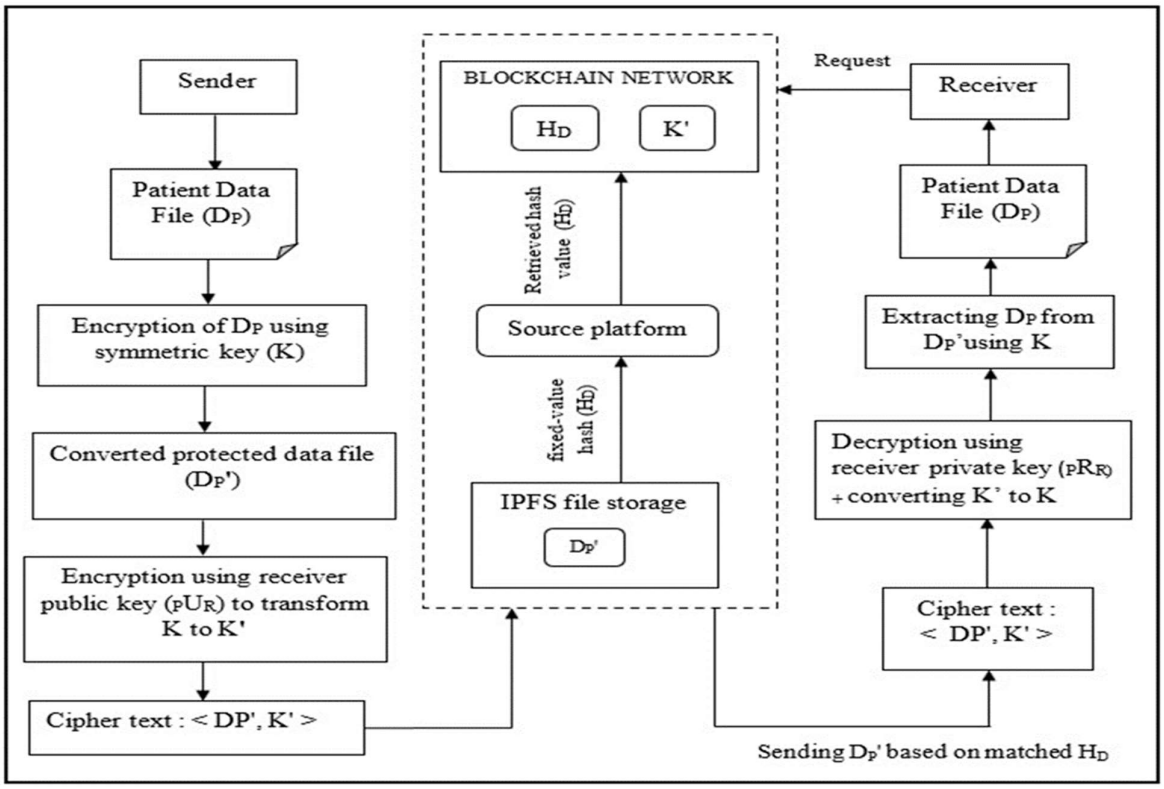

Figure 5. Proposed Methodology

Step 2: Next, a protected data file (D_P') is created by encrypting the patient's data file (D_P) using the symmetric key (K), and the original DP file is then transformed into the $D_{P'}$ file.
Step 3: Further, the encryption process (E_K) is carried out with the help of the receiver's public key ($_PR_R$). The $_PR_R$ key is then utilized to convert the symmetric key (K), into its encrypted form, K'.
Step 4: Next, a protected data file ($D_{P'}$) is sent to IPFS file storage.
Step 5: Then, the IPFS will send the fixed-value hash (H_D) to the source platform as an acknowledgment to make it easier for the data to be stored in a blockchain.
Step 6: Now, in this step, the retrieved hash value (H_D) is stored on a blockchain platform. Along with H_D the blockchain also serves as storage for another entity called K'.
Step 7: At this stage, the receiver can submit the request to IPFS for the patient's data file (D_P) through the blockchain.
Step 8: Now, the IPFS will send the data file $D_{P'}$ in response on the basis of a matched hash (H_D).

Step 9: In this step, decryption (D_K) of the protected data file is carried out using the receiver's private key ($_PU_R$), and then the encrypted key (K') is again retransformed into its initial form (K).

Step 10: Finally, the original data file of the patient (D_P) is extracted from the protected data file (D_P') using the symmetric key (K) and then provided to the receiver.

3.1 Algorithm of the proposed approach

Start

1. Sender →S, Receiver → R, patient data file → D_P, K→ Symmetric key
2. Send D_P for encryption
3. Encrypted $D_P' \leftarrow E_k (D_P)$
4. (K) → encryption, ($E_{K,\ _PU_R}$):: Key encryption receiver's public key ($_PU_R$)
5. K' = $E_{\ _PU_R}$ (K)
6. Cipher text: < D_P', K' >
7. Send (D_P') Patient Datafile to IPFS
8. IPFS stores (D_P') Datafile and assigns a hash value to it.
9. A hash value is returned from IPFS as an acknowledgment of a stored file (D_P')
10. IPFS hash value is sent to the Blockchain
11. Encrypted Key K' is sent to Blockchain
12. Request for D_P by R
13. Sending D_P' based on matched H_D
14. Decryption ((D'_P), K', E_K)
15. (K) ← Decryption, (E_K ,$_PR_R$) :: Key Decryption using Receiver's Private Key ($_PR_R$)
16. $D_P \leftarrow D_K (D_P', K)$

End

4. RESULTS AND DISCUSSION

The proposed approach was first validated on Ganache, and then the behavior of the main net was simulated with the help of Kovan, Binance, Rinkeby, and the Matic network. There is only a single instance of the Ganache platform that acts as a simulation of the blockchain network. The front end that allows users to add and view records is constructed using ReactJS, while the back end is constructed using JavaScript. In addition, the patients' cryptographic keys have been stored in the MongoDB database. In order to recreate a blockchain network, the Ethereum platform in combination with the Solidity programming language was utilized as a test blockchain, and Web3-JS was utilized to interface with the blockchain. INFURA is used to offer trustworthy, secure, and scalable access to the IPFS

gateway and to put the IPFS network through its paces throughout the testing phase. The Firebase and IPFS platforms were used to build the suggested solution, hence, how quickly data files could be uploaded and downloaded is evaluated. The file (.JSON) of 160 kilobytes (KB) was used five times on both a distributed database hosted on IPFS and a centralized database hosted on Firebase, and the times at which it was uploaded and downloaded were recorded.

Table 1: A comparative analysis of proposed work with existing blockchain technology

Scheme	Confidentiality	Data Integrity	Scalability	Blockchain Platform
EHRChain [18]	Yes	Yes	No	Private Blockchain
Healthchain [19]	Yes	Yes	No	Consortium Blockchain
SmartMedChain [20]	Yes	Yes	No	Hyperledger Fabric
Proposed Work	Yes	Yes	Yes	Ethereum based Public Blockchain

It is a comparison of the proposed work's confidentiality, data integrity, and access control with existing blockchain techniques. The proposed framework is contrasted with other blockchain-based solutions already in use, including [18, 19, 20]. Table 1 makes it clear that the proposed solution addresses existing systems' shortcomings in terms of data security, access management, data integrity, and scalability using a public blockchain platform.

Result 1

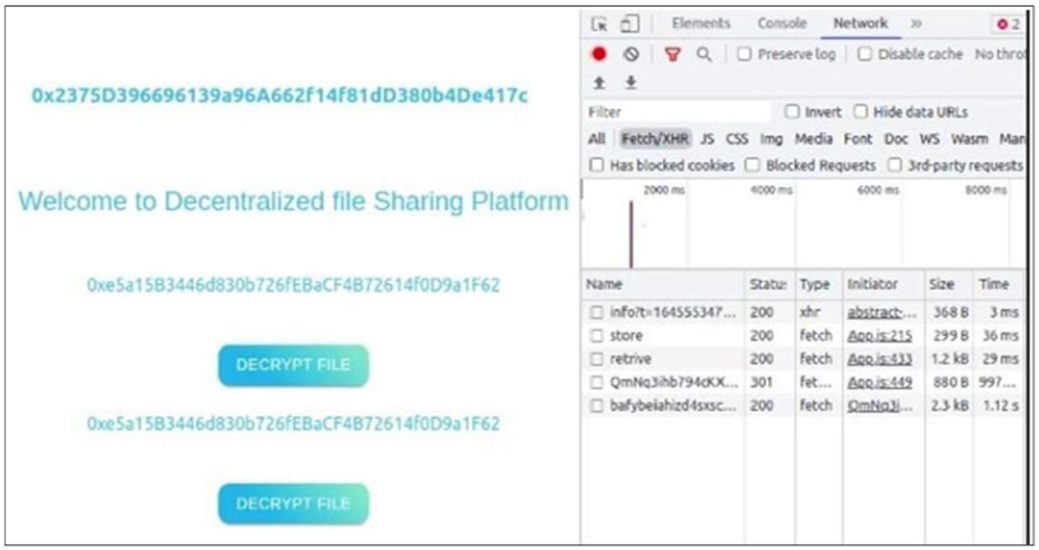

Figure 6. A platform that shows the received data file with the sender's address

Result 2

As can be seen in Figure 7, the receiver's private key ($_PR_R$) and symmetric key (K) are used to decrypt the encrypted file (D_P') so that it may be transformed into the original file (D_P).

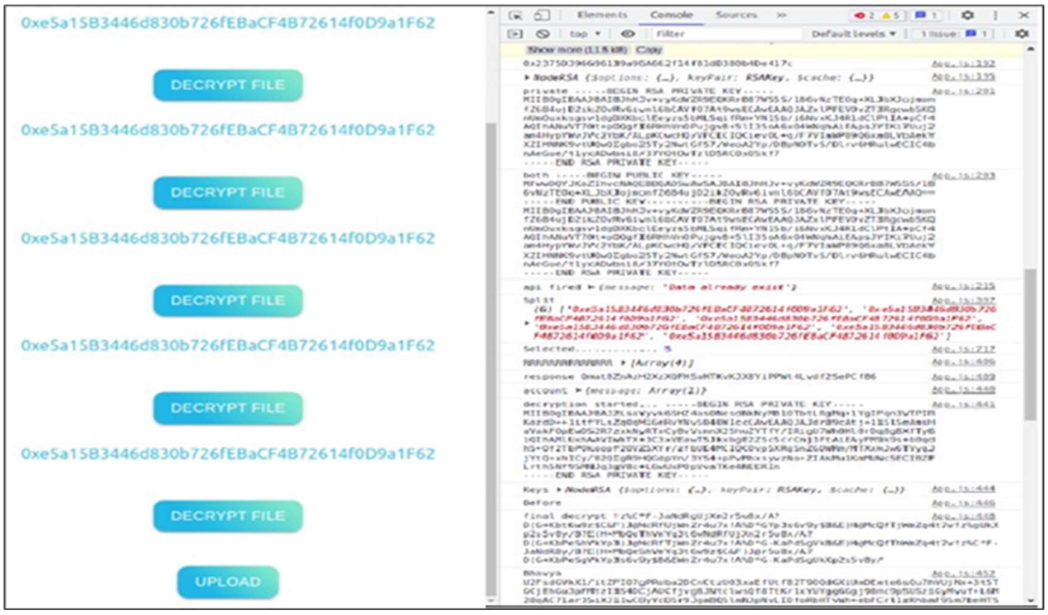

Figure 7. Decryption using the private key ($_PR_R$) and symmetric key (K)

Result 3

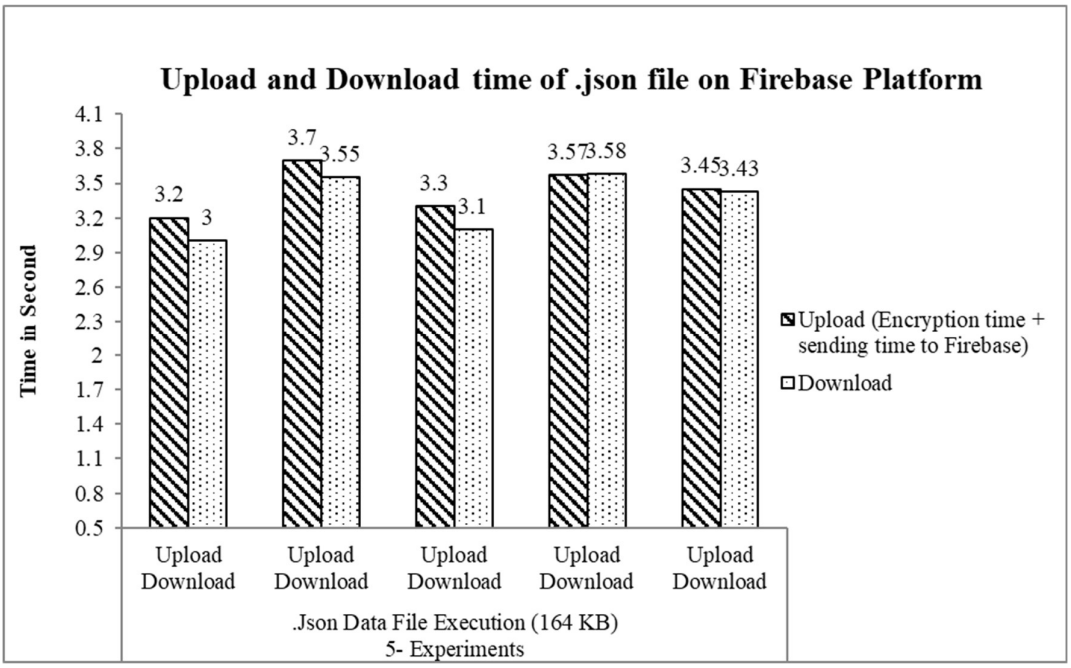

Figure 8: Upload-Download times on the Firebase platform

The result given in Figure 8 illustrates the upload and download speeds of data files for the recommended solution that makes use of the Firebase platform. The relevant file on the Firebase centralized database (.JSON) with a size of 164 KB was used five times, and the times at which it was uploaded and downloaded were recorded.

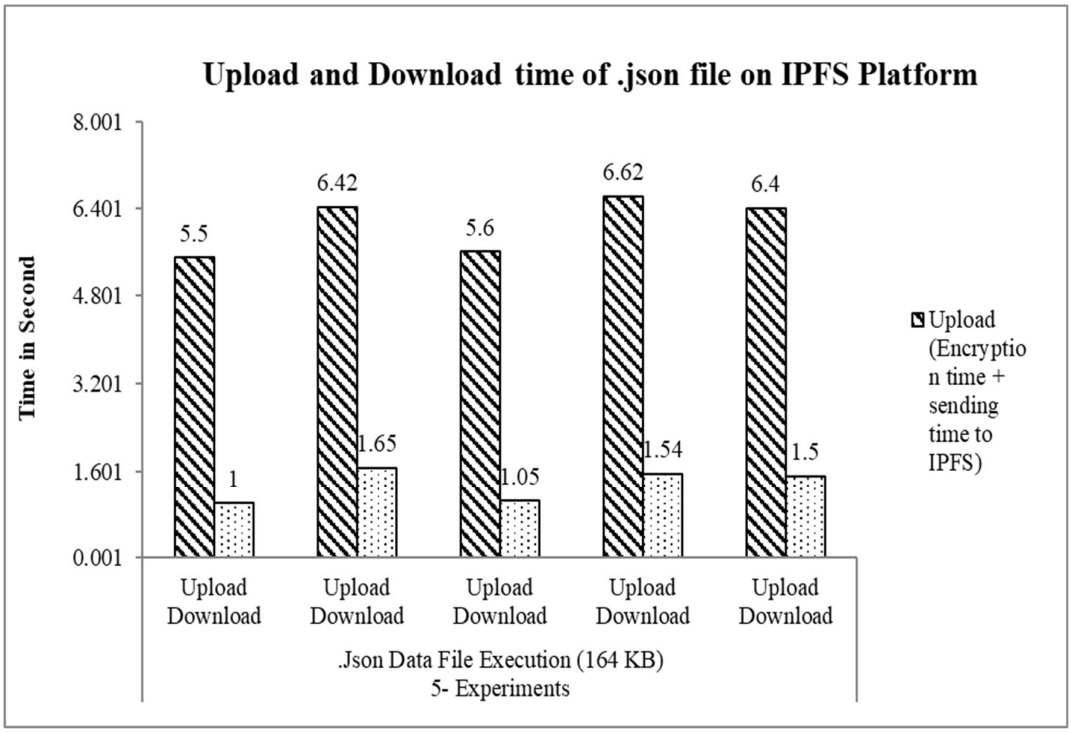

Figure 9. Upload-Download times on the IPFS platform

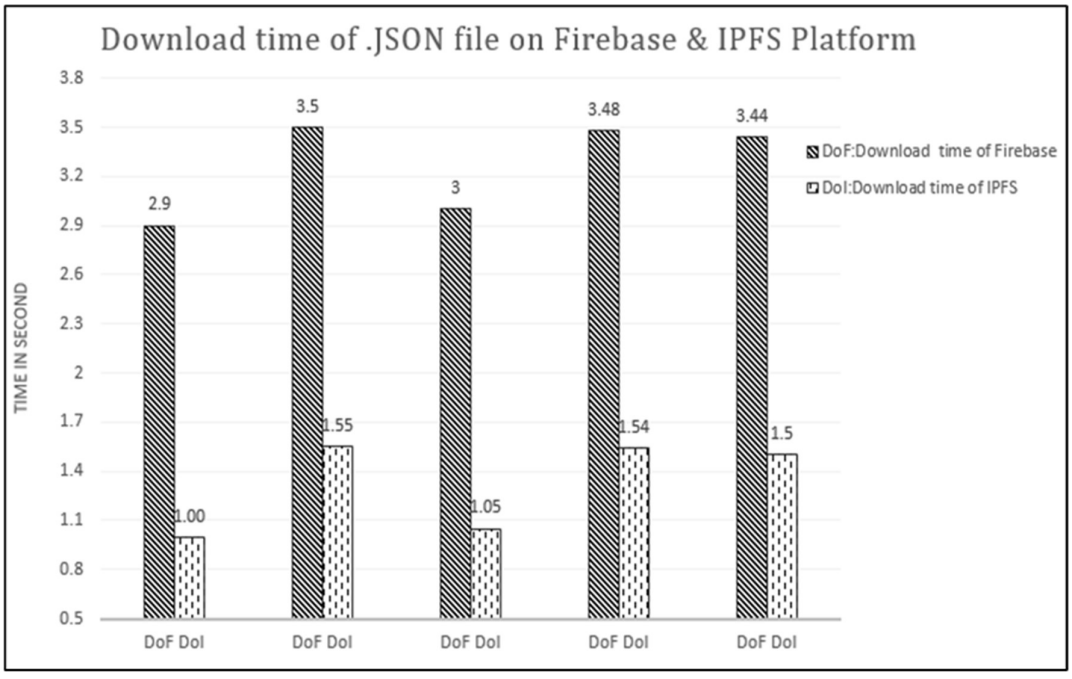

Figure 10. Comparison of download times for .json file on Firebase and IPFS platform

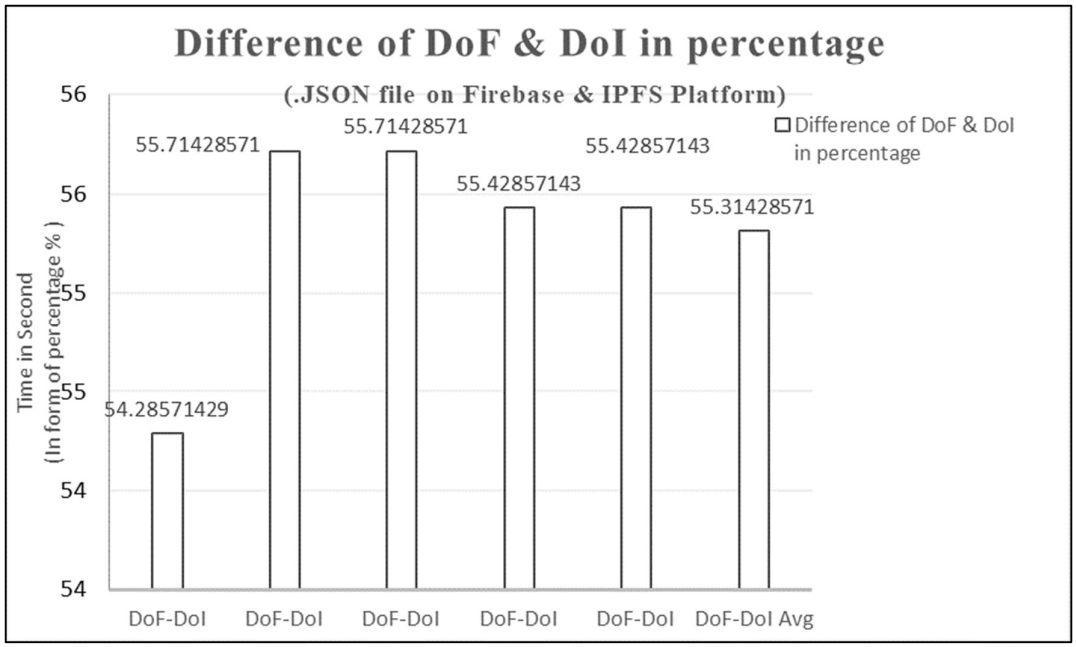

Figure 11. Difference of download times of .json file on Firebase and IPFS platform in form of percentage (%)

The result shown in Figure 9 displays how quickly data files may be downloaded and uploaded using the suggested solution's IPFS platform. The relevant file (.JSON), which has a size of 164 KB on the IPFS distributed database, was used five times, and the upload and download timings were noted. The outcome in Figure 10 illustrates how the Firebase and IPFS systems differ in the amount of time it takes to download. json data file. We came to the conclusion that the IPFS platform takes less time to download than the centralized Firebase platform. Our system provides data security for IoT-based healthcare data by processing all transactions (connected to IPFS) over a blockchain network based on Ethereum. Figure 11 shows the % difference between the download times for the. json data file from Firebase and IPFS.

5. CONCLUSION AND FUTURE SCOPE

The performance of the IoT ecosystem is degraded by a wide variety of problems. Some of these problems are caused by unsupervised, resource-constrained, heterogeneous devices, which might give rise to privacy and trust difficulties. The primary objective of this study was to demonstrate and share the possibilities of blockchain technology in the medical field. In this study, encryption and other forms of access control are applied to build a blockchain architecture on the Ethereum platform to ensure the safety of stored data and facilitate its sharing across many parties, such as patients, physicians, pharmacists, etc. The Raspberry Pi Internet of Things (IoT) device has been utilized to create IoT data and apply a cryptographic

algorithm employed in several approaches for data encryption on the IoT platform for the present prototype implementation. Data encryption is performed before being stored in IPFS, which is required for decentralized file storage in many peer-to-peer data transfer contexts. In this study, the Solidity programming language, which is built on the Ethereum platform, is used to create a smart contract. Due to the exponential growth of health data, this framework could be further improved by running extensive scalability simulations and comparing it to alternative blockchain setups, both of which will warrant more focus in upcoming studies. Further, various blockchain platforms could be used in the future in place of Ethereum for signing agreements between system participants.

REFERENCES

[1]. C. Thirumalai, S. Mohan, and G. Srivastava, "An efficient public key secure scheme for cloud and IoT security," *Computer Communications*, vol. 150, pp. 634–643, Jan. 2020, doi: https://doi.org/10.1016/j.comcom.2019.12.015.

[2]. S. A. Bello et al., "Cloud computing in construction industry: Use cases, benefits and challenges," Automation in Construction, vol. 122, p. 103441, Dec. 2020, doi: https://doi.org/10.1016/j.autcon.2020.103441.

[3]. [1]P. Sharma, M. D. Borah, and S. Namasudra, "Improving security of medical big data by using Blockchain technology," Computers & Electrical Engineering, vol. 96, p. 107529, Dec. 2021, doi: https://doi.org/10.1016/j.compeleceng.2021.107529.

[4]. R. W. L. Coutinho and A. Boukerche, "Modeling and Analysis of a Shared Edge Caching System for Connected Cars and Industrial IoT-Based Applications," IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 2003–2012, Mar. 2020, doi: https://doi.org/10.1109/tii.2019.2938529.

[5]. S. Das and S. Namasudra, "A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure," Computers and Electrical Engineering, vol. 101, p. 107991, Jul. 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.107991.

[6]. Domingo-Ferrer, O. Farràs, J. Ribes-González, and D. Sánchez, "Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges," Computer Communications, vol. 140–141, pp. 38–60, May 2019, doi: https://doi.org/10.1016/j.comcom.2019.04.011.

[7]. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, "The benefits and threats of blockchain technology in healthcare: A scoping review," International Journal of Medical Informatics, vol. 142, p. 104246, Oct. 2020, doi: https://doi.org/10.1016/j.ijmedinf.2020.104246.

[8]. Cyber Security through Blockchain Technology," International Journal of Engineering and Advanced Technology, vol. 9, no. 1, pp. 3821–3824, Oct. 2019, doi: https://doi.org/10.35940/ijeat.a9836.109119.

[9]. H. Wu, X. Liu, and W. Ou, "A Novel Blockchain-MEC-Based Near-Domain Medical Resource Sharing Model," Machine Learning for Cyber Security, pp. 40–56, 2023, doi: https://doi.org/10.1007/978-3-031-20096-0_4.

[10]. A. Ali et al., "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network," Sensors, vol. 22, no. 572, p. 572, Jan. 2022, doi: https://doi.org/10.3390/s22020572.

[11]. M. A. Almaiah, "A New Scheme for Detecting Malicious Attacks in Wireless Sensor Networks Based on Blockchain Technology," Studies in Big Data, pp. 217–234, 2021, doi: https://doi.org/10.1007/978-3-030-74575-2_12.

[12]. S. S. Panda, D. Jena, B. K. Mohanta, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, "Authentication and Key Management in Distributed IoT Using Blockchain Technology," IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12947–12954, Aug. 2021, doi: https://doi.org/10.1109/jiot.2021.3063806.

[13]. P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand, and V. Vasudevan, "Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm," Materials Today: Proceedings, Nov. 2020, doi: https://doi.org/10.1016/j.matpr.2020.08.519.

[14]. A. S. Rajawat, R. Rawat, K. Barhanpurkar, R. N. Shaw, and A. Ghosh, "Blockchain-Based Model for Expanding IoT Device Data Security," Advances in Applications of Data-Driven Computing, pp. 61–71, 2021, doi: https://doi.org/10.1007/978-981-33-6919-1_5.

[15]. S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, "Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology," PLOS ONE, vol. 15, no. 12, p. e0243043, Dec. 2020, doi: https://doi.org/10.1371/journal.pone.0243043.

[16]. B. K. Mohanta, U. Satapathy, S. S. Panda, and D. Jena, "A Novel Approach to Solve Security and Privacy Issues for IoT Applications Using Blockchain," IEEE Xplore, Dec. 01, 2019. https://ieeexplore.ieee.org/abstract/document/9031931?casa_token=6z7JgJ1yUvgAAAAA:1MedpG22tuvURa_SCmCkXcC8mDud1fkwTn_wIV7FGSEh-PebB4U4LRtMHXdklnhIiIYBCBOpXBw

[17]. K. Werder, B. Ramesh, and R. (Sophia) Zhang, "Establishing Data Provenance for Responsible Artificial Intelligence Systems," ACM Transactions on Management Information Systems, vol. 13, no. 2, pp. 1–23, Jun. 2022, doi: https://doi.org/10.1145/3503488.

[18]. F. Li, K. Liu, L. Zhang, S. Huang, and Q. Wu, "EHRChain: A Blockchain-based EHR System Using Attribute-Based and Homomorphic Cryptosystem," IEEE Transactions on Services Computing, pp. 1–1, 2021, doi: https://doi.org/10.1109/tsc.2021.3078119.

[19]. B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "HealthBlock: A secure blockchain-based healthcare data management system," Computer Networks, vol. 200, p. 108500, Dec. 2021, doi: https://doi.org/10.1016/j.comnet.2021.108500.

[20]. D. El Majdoubi, H. El Bakkali, and S. Sadki, "SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework," Journal of Healthcare Engineering, vol. 2021, pp. 1–19, Nov. 2021, doi: https://doi.org/10.1155/2021/4145512.

[21]. "Understanding Blockchain basic structure," DEV Community. https://dev.to/mairelin/understanding-blockchain-basic-structure-5efg

[22]. A. Varshney et al., "Challenges in Sensors Technology for Industry 4.0 for Futuristic Metrological Applications," MAPAN, vol. 36, no. 2, pp. 215–226, Jun. 2021, doi: https://doi.org/10.1007/s12647-021-00453-1.

[23]. A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," International Journal of Intelligent Networks, vol. 2, no. 2, pp. 130–139, 2021, doi: https://doi.org/10.1016/j.ijin.2021.09.005.

[24]. K. Mohammad Hossein, M. E. Esmaeili, T. Dargahi, A. Khonsari, and M. Conti, "BCHealth: A novel blockchain-based privacy-preserving architecture for IoT healthcare applications," Computer Communications, Aug. 2021, doi: https://doi.org/10.1016/j.comcom.2021.08.011.

[25]. R. Kumar, R. Tripathi, N. Marchang, G. Srivastava, T. R. Gadekallu, and N. N. Xiong, "A secured distributed detection system based on IPFS and blockchain for industrial image and video data security," Journal of Parallel and Distributed Computing, vol. 152, pp. 128–143, Jun. 2021, doi: https://doi.org/10.1016/j.jpdc.2021.02.022.

[26]. H.-S. Huang, T.-S. Chang, and J.-Y. Wu, "A Secure File Sharing System Based on IPFS and Blockchain," Proceedings of the 2020 2nd International Electronics Communication Conference, Jul. 2020, doi: https://doi.org/10.1145/3409934.3409948.

[27]. M. Shariq, K. Singh, M. Y. Bajuri, A. A. Pantelous, A. Ahmadian, and M. Salimi, "A Secure and reliable RFID authentication protocol using digital schnorr cryptosystem for IoT-enabled healthcare in COVID-19 scenario," Sustainable Cities and Society, vol. 75, p. 103354, Dec. 2021, doi: https://doi.org/10.1016/j.scs.2021.103354.

[28]. S. Jangirala, A. K. Das, and A. V. Vasilakos, "Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment," IEEE Transactions on Industrial Informatics, pp. 1–1, 2019, doi: https://doi.org/10.1109/tii.2019.2942389.

[29]. R. Ettiyan and G. V., "A hybrid logistic DNA-based encryption system for securing the Internet of Things patient monitoring systems," Healthcare Analytics, p. 100149, Feb. 2023, doi: https://doi.org/10.1016/j.health.2023.100149.

[30]. I. El-Sayed, K. Khan, X. Dominguez, and P. Arboleya, "A Real Pilot-Platform Implementation for Blockchain-Based Peer-to-Peer Energy Trading," IEEE Xplore, Aug. 01, 2020. https://ieeexplore.ieee.org/abstract/document/9281855 (accessed Aug. 12, 2022).