International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

Enhancing Data Security in Healthcare IoT: An Innovative Blockchain-based Solution

Ochchhav Patel[1], Dr. Hiren Patel[2]
[1]Department of Computer Engineering, LDRP-ITR
SVKM, KSV, LDRP-ITR, Gandhinagar
Gandhinagar, Gujarat, India
e-mail: ochchhavpatel@gmail.com
[2]Prinicpal, VSITR, KSV, SVKM
Kadi, Gujarat, India
e-mail: hbpatel1976@gmail.com

Abstract— The Internet of Things (IoT) has revolutionized the healthcare industry by enabling the seamless integration of medical devices, sensors, and data-driven applications. However, the large influx of sensitive healthcare data and the proliferation of linked devices have caused grave worries about data security and privacy. Traditional centralized security systems are unable to handle the changing threats and problems in the IoT healthcare setting. This study suggests a novel strategy for boosting data security in the healthcare industry that makes use of blockchain technology. The main goal of this research is to develop and deploy a trustworthy framework that safeguards private healthcare information in IoT networks. Blockchain, as a distributed and decentralized ledger, offers inherent security features such as immutability, transparency, and cryptographic mechanisms. In this research, it is suggested that healthcare data be gathered via the IoT and stored in the Interplanetary File System (IPFS) using Ethereum-based blockchain technology for data security. The suggested method creates a reliable environment for managing healthcare data by exploiting the special features of blockchain. The json and jpeg files are utilized five times on a distributed database housed on IPFS and a centralized database hosted on Firebase, and the upload and download times are recorded. For IoT-based healthcare systems, we have also investigated the cost and length of time required to implement smart contracts on blockchain platforms like Rinkeby, Binance, and Matic. This research suggests implementing the Blockchain platform in an IoT-based healthcare system to provide data confidentiality, integrity, and accessibility.

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

I. INTRODUCTION

A. Internet of Things (IoT) in Healthcare

The Internet of Things (IoT) refers to the network of interconnected devices embedded with sensors, software, and other technologies that enable them to collect and exchange data over the internet. The implementation of IoT in the healthcare sector has revolutionized the provision and management of healthcare services, improving patient care, enabling remote monitoring, and enhancing operational effectiveness. In order to use IoT in healthcare, a network infrastructure must be connected to a variety of smart devices, medical equipment, wearables, and sensors. These gadgets can collect and send real-time information about environmental conditions, patient activity, adherence to medicine, and vital signs. The gathered information can be used to manage chronic illnesses, provide preventive care, track patient health, and improve hospital operations [1].

Here are some crucial facets and applications of IoT in healthcare [2]:

- Remote Patient Monitoring: With the use of IoT-enabled gadgets, medical professionals may remotely check patients' vital indicators like heart rate, blood pressure, glucose levels, and oxygen saturation. With the use of this technology, anomalies can be detected early, actions can be made quickly, and frequent trips to the hospital can be avoided.
- Wearable Devices: The use of wearable IoT devices for health and wellness monitoring is growing, such as smartwatches and fitness trackers. These gadgets can monitor physical activity, sleep patterns, and offer individualized health advice, encouraging the use of preventative treatment and leading a healthy lifestyle.
- Connected Medical Devices: Medical devices like ECG monitors, infusion pumps, and ventilators may communicate with each other and share data thanks to IoT integration. By enabling in-the-moment warnings and notifications, this connectivity streamlines processes, increases data accuracy, and improves patient safety.
- Asset Tracking and Management: Healthcare facilities can track and manage medical supplies and equipment with the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

aid of IoT technologies. This involves keeping an eye on inventory levels, identifying where things are, maximizing asset use, and automating maintenance plans to cut costs and improve operational effectiveness.

- Smart Environments: The IoT facilitates the creation of smart healthcare environments by integrating sensors and automation systems. In order to provide the best comfort and energy efficiency, this includes monitoring and managing the lighting, temperature, humidity, and energy usage in hospitals, clinics, and patient rooms.
- Data Analytics and Decision Support: Advanced analytics and decision support systems can be used to make use of the enormous amount of data that IoT devices in the healthcare industry generate. Healthcare workers may make well-informed decisions, increase diagnosis accuracy, and tailor treatment programs with the use of real-time data analysis, predictive modeling, and machine learning algorithms.

However, the adoption of IoT in healthcare also brings with it difficulties and worries, particularly in regards to data security, privacy, interoperability, and regulatory compliance. In healthcare IoT situations, it's critical to safeguard patient data and maintain the confidentiality and integrity of sensitive information.

B. Data Security Challenges in Healthcare IoT

Healthcare IoT (Internet of Things) data security difficulties cover a range of worries and hazards related to the gathering, transmission, storage, and use of sensitive healthcare data. The interconnectedness of IoT devices, their vulnerability to threats, and the importance of healthcare data all contribute to these difficulties. The following list of typical IoT data security issues in healthcare includes [3]:

- Data Privacy and Confidentiality: Personal health information (PHI) and electronic medical records (EMRs) are two types of highly sensitive patient data that are collected and transmitted as part of the healthcare IoT. To safeguard patients' rights and avoid unauthorized access or disclosure, it is essential to ensure the privacy and confidentiality of this data.
- Device Vulnerabilities: Wearables, medical sensors, and linked medical equipment are examples of IoT devices that may have flaws in their hardware, software, or network interfaces. Attackers may take advantage of these flaws to obtain access without authorization, intercept data, or alter device functioning.
- Inadequate Authentication and Access Control: Unauthorized access to IoT devices or healthcare systems can be caused by inadequate access control policies, default or easily guessable passwords, and weak authentication mechanisms. This may lead to vital medical devices being compromised, data breaches, or illegal data alterations.
- Network Security Risks: Healthcare IoT devices are vulnerable to network-based assaults since they depend on network access for data transmission. The confidentiality and integrity of data sent between devices and healthcare systems can be jeopardized by man-in-the-middle attacks, listening devices, and unauthorized network access.
- Data Integrity and Trustworthiness: Accurate diagnosis, treatment, and decision-making depend on the integrity and reliability of healthcare IoT data. Medical fraud, poor medical judgment, and patient injury can all result from unauthorized data manipulation or change.
- Interoperability Challenges: The Internet of Things (IoT) in healthcare entails the integration of several systems and devices from various vendors, each with its own protocols and standards. Interoperability issues can result in security holes because devices may not be able to implement security measures or communicate properly, which leaves the system as a whole vulnerable.
- Data Breaches and Cyberattacks: The value and sensitivity of the data involved make healthcare IoT environments desirable targets for cybercriminals. Cyberattacks and data breaches can endanger patient safety and result in data theft, ransomware attacks, disruption of healthcare services, and other problems.

A complete strategy that incorporates strong encryption and authentication systems, secure network architecture, access control policies, regular security assessments, and employee awareness and training programs is needed to address these data security concerns. Additionally, by supplying decentralized and intelligent security mechanisms, emerging technologies like Blockchain and artificial intelligence can improve data security in healthcare IoT [4].

C. Blockchain Technology and its Potential in Data Security

Blockchain technology has the potential to revolutionize data security across various industries, including healthcare. Its special qualities solve the drawbacks of conventional centralized systems and offer a base for reliable and secure data administration. Blockchain is a decentralized network that makes it impossible for a single point of failure or control to exist, making it challenging for hackers to alter or manipulate data. Data integrity is ensured by the immutability of data once it has been stored on the Blockchain. Furthermore, Blockchain's transparency and auditability enable all network users to confirm the veracity and integrity of data, promoting confidence and facilitating effective auditing procedures. Blockchain's cryptographic security system uses robust encryption algorithms and distinctive digital signatures to guarantee the confidentiality

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

and integrity of data. Additionally, Blockchain networks' consensus algorithms validate and verify transactions to make sure that only allowed data is uploaded to the Blockchain, improving overall security and dependability. Blockchain technology provides improved data privacy, integrity, and openness with these attributes, making it a promising answer to data security issues in a variety of industries, including healthcare [5].

D. Open Issues about Blockchain Integration with IoT

Integration of Blockchain technology with the IoT (Internet of Things) presents several open issues and challenges that need to be addressed for successful implementation. These problems include compatibility worries, scalability and performance restrictions, and consensus methods. First and foremost, combining Blockchain with IoT presents substantial scalability and performance concerns. Due to the constrained processing and storage capabilities of IoT devices, the Blockchain network may experience scalability problems as the number of IoT devices and transactions rises. Because each node in the network keeps a copy of the complete Blockchain, Blockchain technology is decentralized, which can result in higher resource needs and longer transaction processing times. For widespread adoption, it is essential to find effective ways to scale Blockchain networks and improve their functionality in IoT settings [6].

Second, IoT devices with limited resources might not be able to use the consensus procedures used in Blockchain networks. For IoT devices with low processing power and energy constraints, traditional consensus procedures, such as proof-of-work (PoW), may need significant computing resources. To balance security, energy efficiency, and resource requirements, lightweight consensus algorithms must be developed specifically for IoT contexts. A hurdle still exists in establishing compatibility between various Blockchain networks and IoT devices. IoT devices frequently use several communication standards and protocols, therefore connecting them with Blockchain networks would require more levels of compatibility. Realizing the full potential of Blockchain in the IoT domain requires achieving frictionless data interchange, interoperability, and standardization across multiple IoT devices and Blockchain platforms [7].

It will take constant study and cooperation between the Blockchain and IoT communities to resolve these open problems. The successful integration of Blockchain technology with IoT will open up new opportunities for secure and effective data management in IoT ecosystems by finding creative methods to increase scalability, improve consensus algorithms, and develop interoperability standards.

II. LITERATURE REVIEW

The primary goal of the literature review is to conduct a critical analysis of the literature on data security and Blockchain technology in relation to the Internet of Things (IoT) and healthcare industries. To find gaps, obstacles, and viable solutions for protecting healthcare data inside the IoT ecosystem, it entails a thorough analysis of academic articles, conference papers, and pertinent sources. The review combines and assesses a variety of methodologies, concepts, and approaches put forth by scholars, highlighting their advantages, drawbacks, and suitability for the identified issue. This study, which examines the body of literature, seeks to advance the subject by presenting fresh perspectives, suggestions, and insights. It presents a cutting-edge method for employing Blockchain technology to improve data security in the healthcare IoT setting.

A. Review of Literature

Rathee, G. et al. (2020) [8] developed a security framework for healthcare multimedia data using the Blockchain approach. They did this by creating hashes for each data so that any changes to the data or breaches involving drugs would be visible to all users of the Blockchain network. The results have been compared to the conventional way and validated with enhanced simulated results that provide an 86% success rate over scenarios involving product drop ratio, falsification attack, worm hole attack, and probabilistic authentication due to the Blockchain technique.

The survey conducted by **Ratta, P., and his colleagues (2021) [9]** revealed that three key areas—drug traceability, remote patient monitoring, and medical record management—are where IoT and Blockchain are being applied in the medical industry. IoT-based medical healthcare can gain more strength from Blockchain.

In a smart home environment, **Dorri et al. (2017)** [10] describe a lightweight implementation of a Blockchain. The response specifies local private Blockchains, which keep records of transactions and policies in an unchangeable ledger. The proposed local Blockchain is owner-controlled and does not employ PoW. A local miner controls the neighborhood Blockchain in each smart house. These miners process all transactions to and from smart homes and keep a list of gadgets. A shared key is used to encrypt unicast communication between devices; however, these keys are also created by the local miner.

Using Blockchain technology, a system called MedChain is suggested by **Daraghmi, E., and his team (2019) [11]** to manage medical records. With its interoperable, secure, and efficient access for patients, healthcare professionals, and other third parties to access medical records while maintaining patient privacy, MedChain is intended to enhance the present systems.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

To regulate transactions and limit access to electronic medical records, MedChain uses time-based smart contracts. Regarding the round-trip execution time of transactions, they have conducted a comparison between the established relational database management system and the suggested Blockchain system. The PoA (Proof of Authority) consensus technique that they adopted has a substantial impact on enhancing system performance and reducing computing time and cost because it can handle more transactions per second.

According to **Rajawat et al. (2021) [12],** managing massive amounts of data, such as that generated by IoT devices or people's medical information, entails an increase in security and human resource concerns. Healthcare IoT, which decreases healthcare expenses while boosting patient care standards, addresses these concerns. By creating a unique SHA256 hash for each record and ensuring that any changes to the data are immediately reflected in updated simulation results, Blockchain technology secures sensitive medical data. Each node utilizes the SHA256 hash technique to verify each block, making it impossible for a malicious actor to change the contents. Based on the criteria of verifiability, appropriateness, extensiveness, uniqueness, robustness, and coercion resistance, a Blockchain-based architecture with a consensus mechanism and the SHA256 hash algorithm was recommended.

The "BlocHIE" system, created by **S. Jiang et al. (2018) [13],** is a Blockchain-based network for exchanging medical data. They investigated the different requirements for transferring health data from diverse sources. They have used two loosely coupled Blockchains to manage various forms of healthcare data and integrated off-chain storage and on-chain verification in order to satisfy the demands of both authenticity and privacy. To properly protect privacy and authentic ability, they incorporate off-chain storage and on-chain verification approaches within the EMR-Chain. To improve system speed and customer fairness, they also suggested two transaction packing techniques.

The Blockchain-based architecture that **El Majdoubi and his team (2021) [14]** propose attempts to address known security flaws in existing systems for smart healthcare and increase the stability of healthcare management systems. Researchers developed the Smart Med Chain architecture, an end-to-end Blockchain-base privacy-preserving solution, for data sharing in the context of s-healthcare. The InterPlanetary File System (IPFS), a distributed data storage system with extraordinary scalability and durability, has been used to store encrypted health data.

The health chain system, created by **J. Xu et al. (2019) [15],** encrypts health data to carry out fine-grained access control. It is constructed to ensure the privacy of enormous amounts of health data and is based on Blockchain technology. Health Chain makes assure that both IoT data and medical diagnoses cannot be changed or withdrawn in order to prevent medical conflicts. They have employed the Doc chain network with Practical Byzantine Fault Tolerance (PBFT) consensus and the User chain (public Blockchain) network with proof of work consensus in the aforementioned architecture. In the health chain, the IPFS system is managed and maintained by a consortium of healthcare providers.

The BCHealth architecture, as described by **K. M. Hossein and his team (2021) [16],** tackles the problem of compromised transparency and access control and allows data owners to specify the necessary access controls over their privacy-sensitive healthcare data. BCHealth consists of two separate chains for the storage of access controls and data transactions. They used a updated Blockchain network and the Proof-of-Authority (PoA) consensus method to improve system performance and scalability. Python was used to implement the BCHealth components and evaluate their performance.

In order to enable a secure method of sharing medical data, **K. Christodoulou et al. (2020) [17]** proposed the COVID-19Pandamics system, which is based on a peer-to-peer network powered by the distributed Interplanetary File System coupled with on-chain tagging. Medical data is securely safeguarded using an open-source variant of the Pretty Good Privacy (PGP) encryption method. The suggested design uses the recipient's public key to encrypt medical data using asymmetric cryptography. Encryption occurs at the client side prior to the data being re-pushed for storage on a peer-to-peer file storage system managed by an IPFS cluster. The system manages the identity data of each participant using public-key cryptography. The smart contract can connect users' social security numbers or any other frequently used form of identification with their Ethereum public addresses, even though identity is pseudonymous to protect privacy. An Ethereum public/private key pair is produced using the secp256k1 Elliptic Curve Digital Signature Algorithm. This pair acts as the authentication method on the Ethereum Blockchain.

The idea for a private blockchain-based encryption framework utilizing a computational intelligence method is put out by **Ghazal, T. M., et al. [18]** for the purpose of encryption. Private blockchain, training phase, and validation phase make up the three sections of the suggested system. For the aforementioned training and validation purposes, the dataset is further divided into two categories: training, consisting of 212 samples, and validation, consisting of 90 samples.

The proposed BHIIoT architecture, as suggested by **Khan, A. A., and his team, [19]** aims to address E-healthcare data security concerns by utilizing a combination of blockchain

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

technology and distributed ledger technology. In this architecture, they have incorporated the NuCypher threshold re-encryption mechanism for data encryption, as well as for safeguarding shared resources in the form of blocks stored in an immutable blockchain storage. Team has improved the security and privacy of E-healthcare data by incorporating the NuCypher threshold re-encryption technique into the BHIIoT architecture. The use of blockchain technology further strengthens the overall security by providing immutability, transparency, and decentralized consensus.

Chaudhury, S., and his team (2023) [20], highlight the potential of Computational Intelligence (CI) and Artificial Intelligence (AI) technologies, specifically Gated Recurrent Units (GRUs), in improving healthcare systems, particularly in the domain of breast cancer diagnosis and treatment. The integration of IoT devices and advanced machine learning techniques offers promising opportunities for intelligent and sustainable healthcare solutions.

B. Literature Review Findings

According to this paper's and our published article's [21] literature reviews, most academic researchers have used a private Blockchain network, notably the Hyperledger network, to assure data security. In contrast, our research focuses on utilizing a public Blockchain network. By employing a public Blockchain platform, our proposed system allows anyone to join and participate. In our approach, the recipient's public key is used to transfer the data file while maintaining the confidentiality of the patient's identity. Only the sender's public key is visible to the recipient. One key distinction between private and public Blockchain networks is the level of security they provide. In private (permissioned) Blockchain networks, there are a limited number of validators who review blocks or transactions, making them comparatively unsafe than permissionless (public) Blockchain networks. In permissionless Blockchains, each block and transaction must be confirmed by multiple participants before being included. Given our focus on an IoT-based healthcare system that utilizes IPFS storage on a public Blockchain built on Ethereum, we favor the aforementioned sources for our research.

C. Research Objective and Problem Formulation

The primary objectives of this study are to address security issues relating to confidentiality, integrity, and access control, as well as to investigate and suggest mechanisms for improving scalability in a Blockchain environment within the context of an IoT-based healthcare system. In terms of scalability, the study aims to investigate methods such as layer-2 protocols and off-chain transactions to boost system capacity and transaction throughput while preserving the advantages of Blockchain technology. The research also focuses on addressing security issues by implementing consensus mechanisms to maintain data integrity and prevent tampering, smart contracts and permission models to establish effective access control measures, and cryptographic methods to ensure confidentiality of sensitive healthcare data stored on the Blockchain. By attaining these goals, the study hopes to contribute to the creation of a Blockchain architecture that is secure, scalable, and allows for efficient data management while protecting patient privacy and guaranteeing regulatory compliance in IoT-based healthcare systems.

III. METHODOLOGY

A. Research Design

The research design includes both qualitative and quantitative elements to guarantee a thorough investigation of the data security issues and the efficiency of the novel approach that has been offered. Conducting deep conversations with professionals in the fields of healthcare data security, IoT, and Blockchain technology is part of the research design's qualitative component. These conversations offer insightful information on the current data security issues encountered in the healthcare IoT environment. It also assists in comprehending the possible advantages and restrictions of applying Blockchain technology to address these issues. In addition to a thorough examination and analysis of the existing literature, academic papers, industry reports, and best practices, the qualitative component focuses on data security, IoT, and Blockchain technologies in the healthcare industry. The quantitative component of the research design focuses on assessing the efficacy of the unique technique that has been suggested. To do this, a proof-of-concept system incorporating the suggested method to improve data security in the IoT environment for healthcare will need to be designed and put into practice. To evaluate the system's functionality, scalability, and security, data from real-world scenarios, including simulated IoT devices and healthcare data exchanges, is gathered. To assess the viability and performance of the suggested approach, quantitative measures such as file download-upload time, data confidentiality, data integrity, and access control effectiveness are studied.

A comparison analysis is part of the research design, and it will compare the proposed novel technique to already-in-use data security solutions in the IoT for healthcare context. This will shed light on the special benefits and contributions of the suggested approach.

B. Data Collection and Analysis

In this research, we consider the healthcare domain, where various kinds of detectors and sensors are available that estimate significant physical quantities such as human temperature, pulse rate, oxygen level, etc. There are various layers that are

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

important from the IoT's functionality point of view. The perception layer of the IoT is responsible for ordering data and transmitting it to the network layer. It also enables one gadget to collaborate with other gadgets. The network layer is accountable for managing communication and transmitting the piled-up data from the perception layer to the storage servers via gateways. The application layer manages the gathered data, and processed information is sent to the applications or end users' communities.

The temperature, oxygen saturation, pulse rate, and other generated data from the data generator are stored in a file. The RFID (Radio Frequency Identification) device offers a specific file naming convention that is used to save the data. The json and jpeg file formats are used to create the patient data file. Here, a data file is encrypted using the AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) cryptographic algorithm, and that encrypted file is stored on IPFS storage. The robustness of AES, a symmetric cryptosystem, is confirmed by the theory of computational complexity. It is related to a procedure that explains how to encrypt the data blocks. There are numerous operational modes. We operate in CBC mode, which ensures the confidentiality and integrity of the data. The main advantage of the AES algorithm is the availability of multiple key lengths. The size of the key used to secure communication has a direct impact on how long it takes to decrypt data using a given encryption algorithm. Due to the Blockchain-based mechanism, only authenticated users can access the patient's data file from the data storage.

IV. IMPLEMENTATION AND EVALUATION

A. Overview of the Proposed Solution

This section describes a technique using Blockchain technology to address data security issues in the context of the IoT in the healthcare industry. The recipient's public key is used to alter the symmetric key after the sender's patient data file has been converted to a protected data file. The protected data file is then kept on IPFS after the fixed-value hash and converted key are both made public on the Blockchain. Now, when the recipient sends a request for the patient data file to IPFS through the Blockchain, IPFS responds with the protected data file based on the hash value. At the receiving end, the encrypted data file is decrypted, and the key is restored to its initial condition. The recipient then receives the original patient data file after the protected data file has been opened. The workflow of the suggested method is depicted in the flowchart in Figure 1.

Algorithm 1: Data Encryption

1: Function Encryption: Input Data File (D_P), Output Encrypted File (D'_P)

2: Collect a symmetric key K (from Key Distribution Centre)

3: Select the encryption algorithm (E.g., AES)

4: Generate a random initial vector IV

5: $D'_P \leftarrow E_K$ (D_P, IV)

6: Return the encrypted file D'_P on public channel and IV & K on private channel

Algorithm 2: Proposed Approach

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.
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)

B. Experimental Setup

The two phases of our experimentation are as follows: In the initial stage of IoT deployment, tags, medical sensors, and a Raspberry Pi are used. In the second stage, the Blockchain side is developed using the Ethereum platform, IPFS for distributed storage, Solidity for programming, Metamask (a Blockchain wallet), and other technologies. We successfully integrate two

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

technologies in this execution, outlining how medical data is produced and safeguarded in the context of the Internet of Things. It also included instructions on how to store that data in IPFS storage and how the Blockchain network may use it. The RFID gadget created a file with the patient's individual ID. The output data is subsequently filtered to fulfill requirements, and the file is then cryptographically encrypted. The Raspberry Pi can interface with a variety of sensors and RIFD tags using its built-in Python library. The Raspbian operating system was installed using the Berryboot operating system, which may be used to install any Raspbian operating system and act as an all-purpose operating system. The Raspberry Pi is integrated with the RFID RC522 chip using the MFRC522.py Python package, which is used to read and write data to and from the RFID tags.

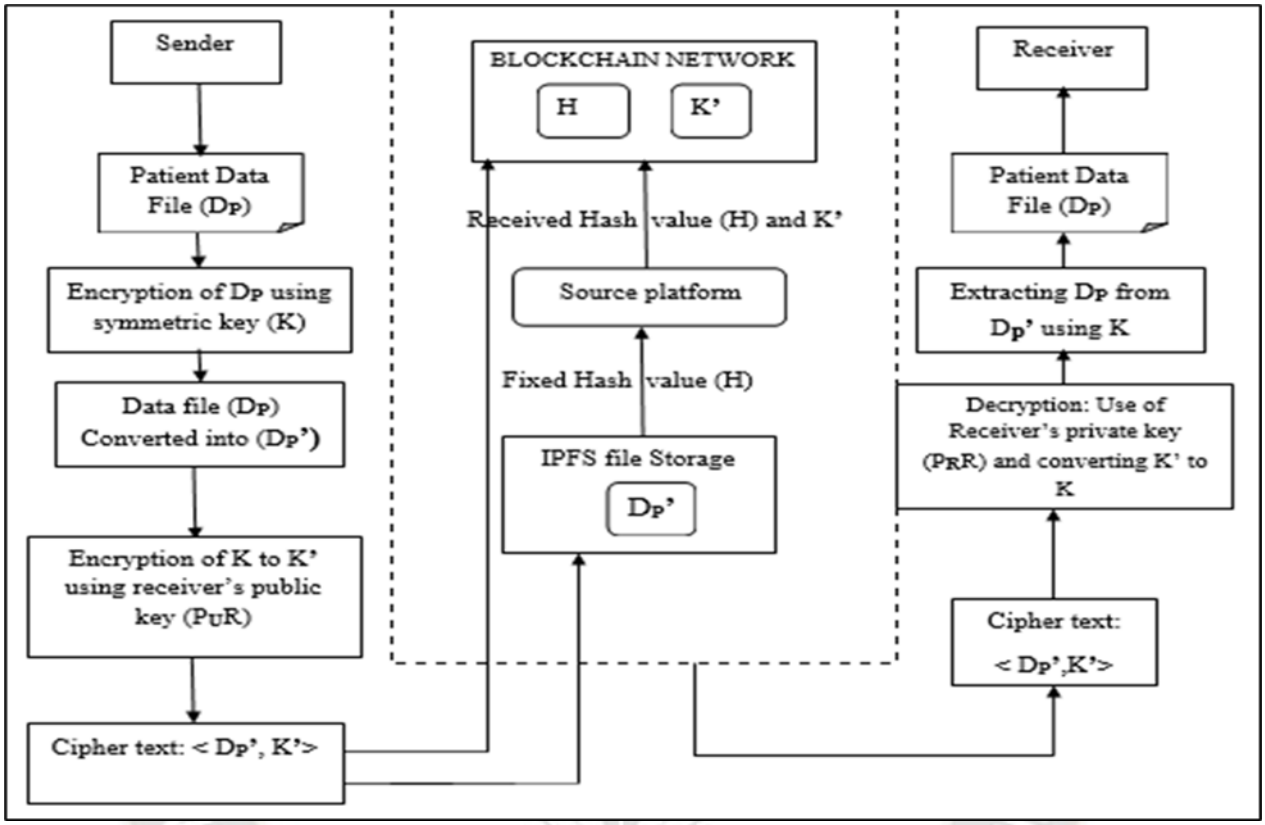


Figure 1. Proposed Methodology [21]

The steps that follow highlight the flowchart's general layout and demonstrate how data is transferred from one place to another.

- The sender first transmits the patient data file (D_P).
- The patient's data file (D_P) is then encrypted with the symmetric key (K), creating a protected data file (D'_P), and the original (D_P) file is changed into the (D'_P) file.
- The public key ${}_PU_R$ of the recipient is used to carry out the encryption process (E_K). The symmetric key (K) is subsequently transformed into its encrypted form, K', using the ${}_PR_R$ key.
- Sending a protected data file (D_P) to IPFS file storage.
- In order to make it simpler for the data to be kept in a Blockchain, the IPFS transmits the fixed-value hash (H) to the source platform as an acknowledgment.
- The receiver uses the Blockchain to submit a request to IPFS for the patient's data file (D_P).
- On the basis of a matched hash (H), IPFS will now provide the data file (D'_P) in response.
- Using the receiver's private key (${}_PR_R$), the protected data file is decrypted (D_K) in this stage, and the encrypted key (K') is then once more transformed back into its original form (K).
- 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.

The IPFS platform is used to store the data file (D_P), which is encrypted using the encryption technique AES. The hash value (H) for that file saved in IPFS storage is returned. The Blockchain platform stores the hash value and symmetric key that were obtained. The recipient's public key (${}_PU_R$) encrypts

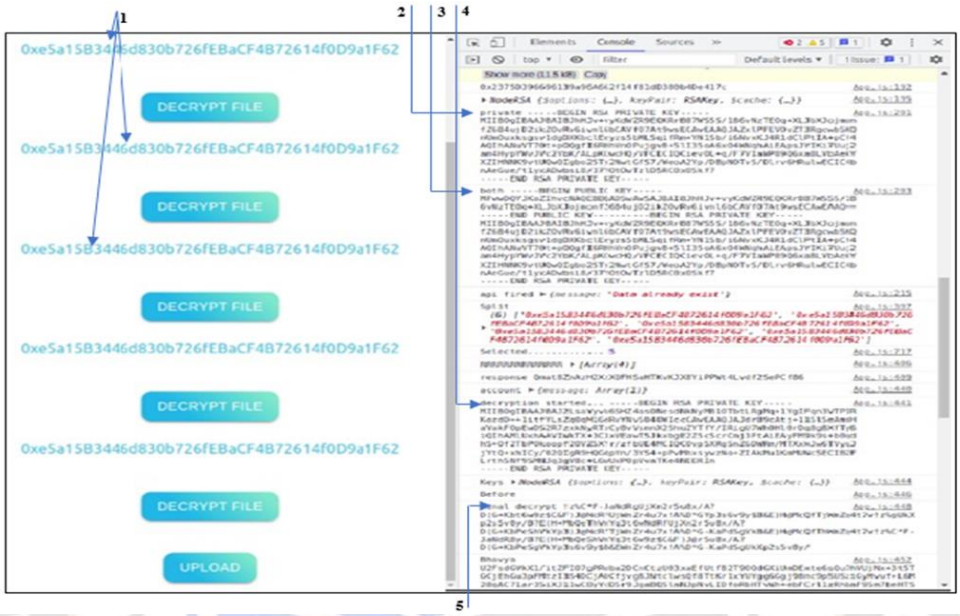
International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

the symmetric key (K). As shown in Figure 2, the recipient must visit the Blockchain platform, use their private key (pR_R), and the hash value (H) of the saved data file to decrypt it in order to obtain the original data file (D_P) from IPFS.

C. Experimental Outcomes and Analysis

Outcome:

Figure 3 illustrates the large file in json (1 MB) format and shows the recorded upload and download times for centralized platform Firebase and distributed platform IPFS. As per our previous published article [21], we had used a small json data file (164 kb), but now we have experimented with a large json file format and listed upload and download times for the Firebase and IPFS platforms. Also, in this paper, we have included the results of the image (jpeg) file format and marked the download and upload times. Other data file formats like pdf are also supported in our implementation.



1: List of Sender's Blockchain wallet addresses 2: Private key of Receiver 3: Public key of Receiver for symmetric key encryption 4: Decryption Process 5: Decryption key for original data file conversion.
Figure 2: Using the private key with a symmetric key to decrypt data

Outcome 1: Upload and Download time for json (1 MB) file on Firebase Platform

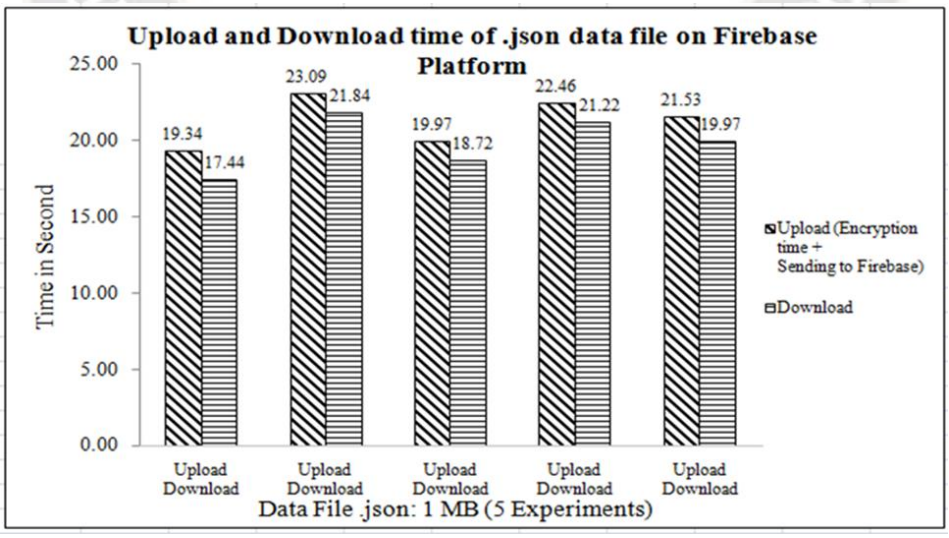


Figure 3: Upload and Download time for json (1 MB) file on Firebase Platform

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

Outcome 2: Upload and Download time for json file on IPFS Platform

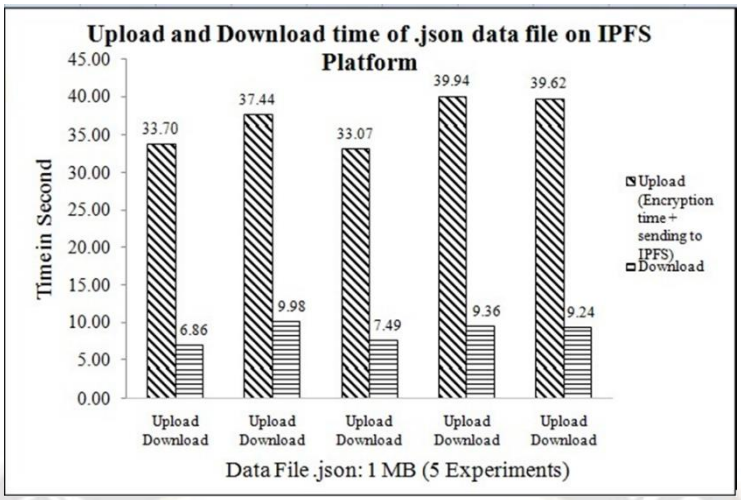


Figure 4: Upload and Download time for json (1 MB) file on IPFS Platform

Outcome 3: Comparison of download time for json file on Firebase and IPFS platform

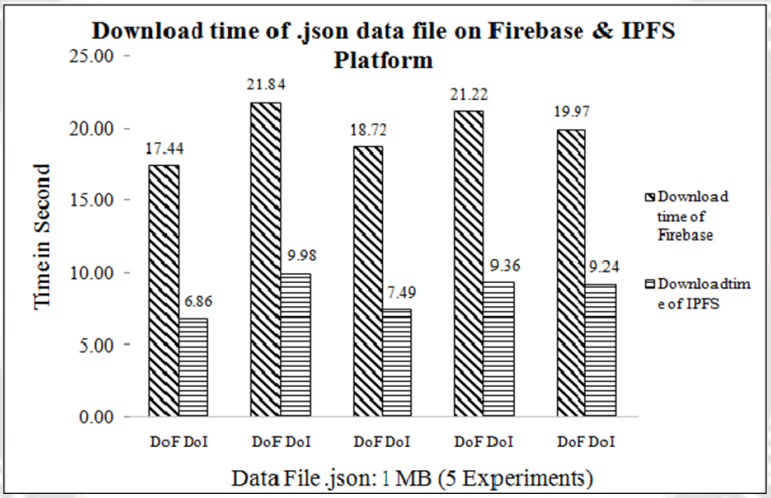


Figure 5: Download time for json (1 MB) file on Firebase and IPFS platform

Outcome 4: Download time in percentage and average time for json file on Firebase and IPFS platform

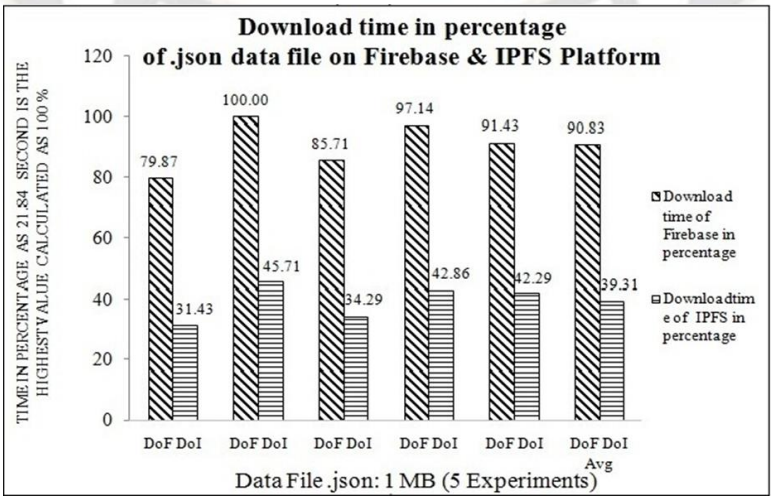


Figure 6: Download time in percentage for json (1 MB) file on Firebase and IPFS platform

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
Article Received: 30 May 2023 Revised: 24 July 2023 Accepted: 12 August 2023

Outcome 5: Difference of DoF (Download time of Firebase) & DoI (Download time of IPFS) in percentage for json file on Firebase and IPFS

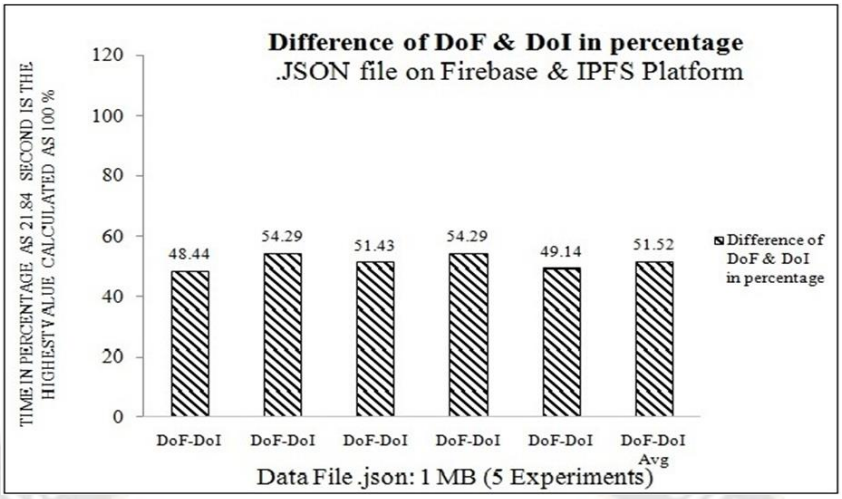


Figure 7: Difference of DoF & DoI in percentage for json file on Firebase and IPFS platform

Outcome 6: Comparison of download times for of jpeg file on Firebase and IPFS platform

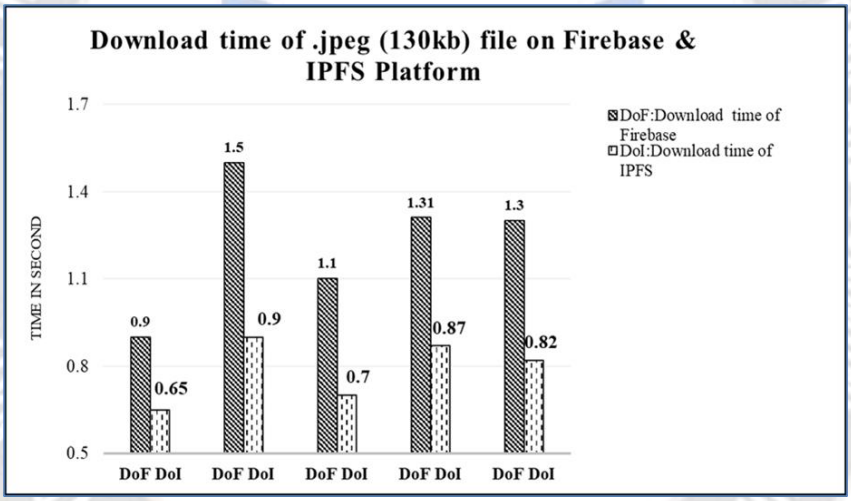


Figure 8: Download time for jpeg file (130 kb) on Firebase and IPFS platform

Outcome 7: Comparison of download times for jpeg file on Firebase and IPFS platform with percentage (%)

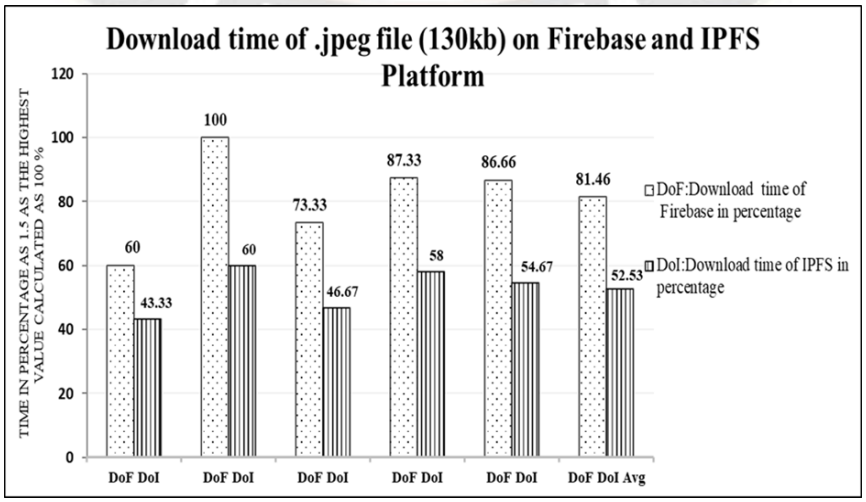


Figure 9: Comparison of download times for jpeg file on Firebase and IPFS platform with percentage (%)

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

Outcome 8: Difference and average of download times for of jpeg file on Firebase and IPFS platform in form of percentage (%)

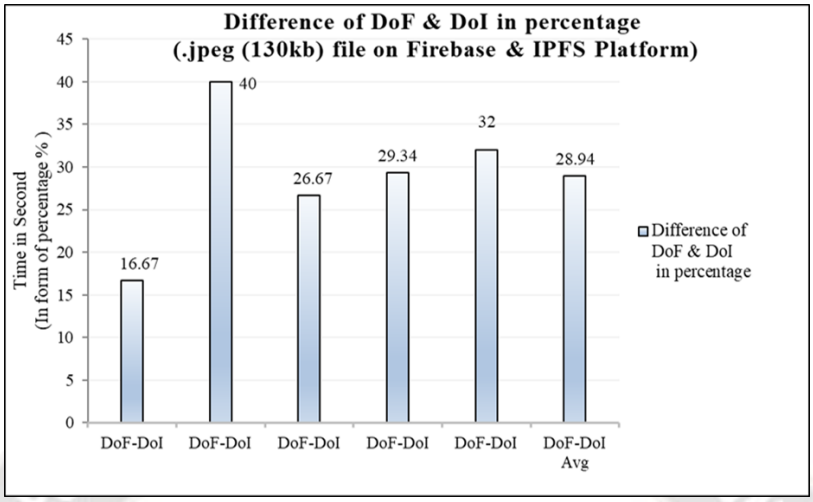


Figure 10: Difference and average of download times for jpeg file on Firebase and IPFS platform in form of percentage (%)

The proposed method was first verified on Ganache the platform, and then Kovan, Binance, Rinkeby, and the Matic network were used to imitate the main network's activity. The Ganache platform, which is a replica of the Blockchain network, exists only in a single instance. ReactJS is used to build the front end, which lets users add and view records, while JavaScript is used to build the back end. Additionally, the MongoDB database contains the patients' cryptographic keys. The Ethereum platform was used as a test Blockchain together with the Solidity programming language, and Web3-JS was used to communicate with the Blockchain in order to replicate a Blockchain network. In addition to putting the IPFS network to the test, INFURA is used to provide dependable, secure, and scalable access to the IPFS gateway. Due to the offered solution's usage of the Firebase and IPFS platforms, it is possible to evaluate the speed at which data files can be uploaded and downloaded. Figures 3 and 4 show the record times at which the 130 kb jpeg and 1 MB json data files were downloaded and uploaded. On both a distributed database hosted on IPFS and a centralized database housed on Firebase, the file has been used five times.

V. DISCUSSION

We found that downloading using the distributed IPFS platform is faster than downloading via the centralized Firebase platform. By processing all transactions over an Ethereum-based Blockchain network (connected to IPFS), our system protects IoT-based healthcare data. Figure 5 displays download times for json files on the Firebase and IPFS platforms, and figures 6 and 7 show differences and average times of the download process in the form of percentages for both platforms. These figures likely provide a more detailed analysis of the download speeds, showcasing the variations and averages between the two platforms. It illustrates that downloading json data files from the centralized Firebase platform is about 52% slower than downloading them through the decentralized IPFS network using the Blockchain. Using a decentralized architecture, IPFS distributes files around a network of linked nodes. IPFS gets an image file from the closest network node when a user requests one. This decentralized strategy reduces the distance that data must travel, which lowers latency and speeds up downloads. To uniquely identify files based on their content, IPFS uses content addressing. The cryptographic hash assigned to each file serves as the file's address. This makes it possible to cache and replicate files across the IPFS network effectively. As a result, image files can be obtained simultaneously from several sources, accelerating the download rate even more. In conclusion, our extensive evaluation of the two platforms reveals that the download speed of image files on the IPFS platform is conclusively 29% faster than on Firebase.

VI. CONCLUSION

In order to ensure the security of stored data and enable its distribution across several parties, including patients, doctors, pharmacists, and other healthcare professionals, this study applies encryption and other types of access control to create a Blockchain architecture on the Ethereum platform. In order to create IoT data and execute the current prototype, an Internet of Things (IoT) device called the Raspberry Pi was used. IoT data was created, and an encryption algorithm that has been used in a number of other IoT platform approaches was applied. IPFS performs data encryption before storing it because decentralized file storage is necessary in many peer-to-peer data transfer scenarios. The suggested architecture shows download speeds

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10s
DOI: https://doi.org/10.17762/ijritcc.v11i10s.7597
***Article Received**: 30 May 2023 **Revised**: 24 July 2023 **Accepted**: 12 August 2023*

that are 52.53% (on average) quicker for json data files and 28.94% faster for jpeg data files over the IPFS platform when compared to a centralized platform like Firebase.

VII. FUTURE SCOPE

In this study, a smart contract was created using the solidity programming language and executed on the Ethereum (permissionless Blockchain) platform, which offers greater strength and scalability than private or consortium Blockchain platforms. This approach should be further enhanced by conducting extensive scalability simulations and comparing it to various Blockchain configurations due to the exponential growth of health data; these two areas will require more attention in subsequent studies. Researchers may explore other options of Blockchain platforms apart from Ethereum for issues such as scalability, feasibility and security.

REFERENCES

[1]. Singh, P. D., Dhiman, G., & Sharma, R. (2022). Internet of things for sustaining a smart and secure healthcare system. Sustainable computing: informatics and systems, 33, 100622.

[2]. Salehi-Amiri, A., Jabbarzadeh, A., Hajiaghaei-Keshteli, M., & Chaabane, A. (2022). Utilizing the Internet of Things (IoT) to address uncertain home health care supply chain network. Expert Systems with Applications, 208, 118239.

[3]. Can, Y. S., & Ersoy, C. (2021). Privacy-preserving federated deep learning for wearable IoT-based biomedical monitoring. ACM Transactions on Internet Technology (TOIT), 21(1), 1-17.

[4]. Singh, A. K., Anand, A., Lv, Z., Ko, H., & Mohan, A. (2021). A survey on healthcare data: a security perspective. ACM Transactions on Multimidia Computing Communications and Applications, 17(2s), 1-26.

[5]. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. IEEE Cloud Computing, 5(1), 31-37.

[6]. Sharma, P. K., Kumar, N., & Park, J. H. (2020). Blockchain technology toward green IoT: Opportunities and challenges. IEEE Network, 34(4), 263-269.

[7]. Biswas, K., & Muthukkumarasamy, V. (2016, December). Securing smart cities using blockchain technology. In 2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS) (pp. 1392-1393). IEEE.

[8]. Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimedia Tools and Applications, 79(15-16), 9711-9733.

[9]. Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. Journal of Food Quality, 2021, 1-20.

[10]. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops) (pp. 618-623). IEEE.

[11]. Daraghmi, E. Y., Daraghmi, Y. A., & Yuan, S. M. (2019). MedChain: a design of blockchain-based system for medical records access and permissions management. IEEE Access, 7, 164595-164613.

[12]. 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.

[13]. S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blochie: a Blockchain-based platform for healthcare information exchange," in 2018 ieee international conference on smart computing (smartcomp). IEEE, 2018, pp. 49–56.

[14]. El Majdoubi, D., El Bakkali, H., & Sadki, S. (2021). SmartMedChain: a blockchain-based privacy-preserving smart healthcare framework. Journal of Healthcare Engineering, 2021.

[15]. J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A Blockchain-based privacy preserving scheme for large-scale health data," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8770–8781, 2019.

[16]. Mohan, A., Prabha, G. ., & V., A. . (2023). Multi Sensor System and Automatic Shutters for Bridge- An Approach. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 278–281. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2665

[17]. K. M. 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, vol. 180, pp. 31–47, 2021.

[18]. K. Christodoulou, P. Christodoulou, Z. Zinonos, E. G. Carayannis, and S. A. Chatzichristofis, "Health information exchange with Blockchain amid covid-19-like pandemics," in 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS). IEEE, 2020, pp. 412–417.

[19]. Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Bakar, K. A. A., & Al Hamadi, H. (2022). Private blockchain-based encryption framework using computational intelligence approach. Egyptian Informatics Journal, 23(4), 69-75.

[20]. Khan, A. A., Bourouis, S., Kamruzzaman, M. M., Hadjouni, M., Shaikh, Z. A., Laghari, A. A., ... & Dhahbi, S. (2023). Data Security in Healthcare Industrial Internet of Things with Blockchain. IEEE Sensors Journal.

[21]. Paul Garcia, Ian Martin, Laura López, Sigurðsson Ólafur, Matti Virtanen. Automated Grading Systems: Advancements and Challenges. Kuwait Journal of Machine Learning, 2(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/165

[22]. Chaudhury, S., & Sau, K. (2023). A blockchain-enabled internet of medical things system for breast cancer detection in healthcare. Healthcare Analytics, 100221.

[23]. Patela, O., & Patelb, H. (2023). A Novel Approach to Address Data Security Concerns in the IoT Environment for Healthcare Domain using Blockchain Technology. Journal of Data Acquisition and Processing, 38(3), 11.