Vol. XVII & Issue No. 06 June - 2024
INDUSTRIAL ENGINEERING JOURNAL

INNOVATIVE BLOCKCHAIN SOLUTIONS FOR SECURING IOT HEALTHCARE DATA: ADDRESSING DATA CONFIDENTIALITY AND INTEGRITY IN IOT BASED HEALTHCARE SYSTEM

Ochchhav Patel
LDRP-ITR, KSV, Sarva Vidyalaya Kelvani Mandal, Gujarat, Gandhinagar- 382015, India
Email: ochchhavpatel@gmail.com

Hiren Patel
VS-ITR, Sarva Vidyalaya Kelvani Mandal, Gujarat ,Kadi-382715, India
Email: hbpatel1976@gmail.com

Abstract

As a powerful amalgamation of wireless devices, radio-frequency identification (RFID), and various sensors, the Internet of Things (IoT) has provided a challenging yet powerful prospect of shaping existing systems with the goal of making them more intelligent. IoT is used in smart healthcare, virtual and augmented reality, self-navigating cars or drones, vehicle telematics, smart home automation, and many more domains and applications. IoT has great potential in the healthcare domain too, and many companies are working to find new ways to use this technology to assist in the medical biosphere. In this paper, we have mentioned IoT-based healthcare data that is protected by Ethereum-based blockchain technology and Interplanetary File System (IPFS) storage. Blockchain technology can be used to secure IoT data. The inherent features of the blockchain are enhanced by smart contracts, which are computer programs that will automatically execute, control, and record events consistent with the terms written in them. Using a variety of blockchain networks we have observed the efficiency of IoT-based medical health care systems. This research emphasizes confirming data security while sharing sensitive data across the same or different organizations, as well as healthcare providers, in a distributed environment.

Keywords: Blockchain, Healthcare, Internet of Things, IPFS, Security.

1. INTRODUCTION

We can see today's trend on the internet is making life easier for people with the use of internet-based devices, which are known as "Smart Devices." In simple terms, we can say it is a technology that connects various devices together and makes human life easy. This trend leads the whole world's technocrats to the Internet of Things (IoT) concept. It is mainly used to connect real-world devices across the world at any time. The main aim of IoT is to automate your routine tasks using some sensors and chipsets that are collecting real-time data, sending it to be processed using various networks, and performing tasks according to the computed data. To make IoT robust and handle tremendous data, it should follow a 5-layer architecture, like the perceptron layer, network layer, middleware layer, application layer, and business layer [1]. IoT is an emerging technology, and the leading technology companies have understood its value for the future. Many investors are investing tremendous volumes in that sector. IoT has gained importance in various fields such as analysis and detection, smart living, the medical sector, agriculture, the automobile sector, and the surveillance field [2].

The industry's most important segment is healthcare. In addition to routine medical examinations, patients' bodily states, including heart rate, blood sugar, diabetes, electrocardiogram, and other important biomedical signals, can be tracked using a variety of medical monitoring devices and sensors for diagnosis or health quality improvement. Data security and privacy are more important than ever in the healthcare sector and around the globe. Violations of security and privacy can cost you a lot of money, in addition to harming the reputation of your organization and endangering patient relationships. Patient health information is required to be preserved by healthcare facilities like hospitals, clinics, and for-profit healthcare companies. Although the vast majority of healthcare organizations make sure that private information is encrypted and stored safely, no one has total control over security [3]. A single error leaves your data open to third parties. The provision of more effective and efficient treatment is aided by the use of the Internet of Things for real-time patient tracking. All IoT devices and networks need to be connected to other technologies in order to help healthcare facilities transform themselves in a meaningful way. In the health industry, appropriate and effective technologies help to address issues with product integrity and traceability in the drug supply chain, increase the overall security of patients' electronic medical information, and enable effective interoperability. IoT-based healthcare currently faces a myriad of issues, including data security, service quality, data. transparency, mobility, patient identity, and ongoing monitoring [4].

A blockchain is some kind of data structure that can provide immutable transactions across the world and can help address the above issues [5]. Basically, it is working on hashing techniques, which means if you change the content of your

block, the hash will be drastically changed according to the changes in the block. This effect is known as the "avalanche effect" [6]. The real beauty of this hashing process is that you can get the hash of your data, but you will not be able to retrieve data from that hash. It removes the centralized authority for the transactions. There is a shared ledger using peer-to-peer technology that is available for every node in the chain. Each block in the blockchain is made up of two parts: a block header and a data block. The blocks have to be mined for the accumulation of blocks in the real test network. This mining process uses various consensus algorithms like PoW (Proof of Work), PoS (Proof of Stack), PoI (Proof of Importance), and many more consensus mechanisms. In a blockchain network, for the mining process, miners have to solve some cryptographic problems [7].

There are three types of blockchain networks: the first is the public blockchain, and the remaining are private and consortium blockchain networks. There are no restrictions on public blockchains, and anyone is free to join and contribute to the core activities of the blockchain network. We can say a public blockchain is a democracy where all the computers and organizations decide together where they are going and what changes to implement. The most used and popular public blockchains are bitcoin and ethereum. In a private blockchain, only an authorized person can participate in the chain network [8]. Also, in private, there is generally a dictatorship because everything is owned by one company. Examples of private blockchains are the Corda, Liquid, and Hyperledger Fabric networks. The consortium blockchain is a subset of a private blockchain in which only a small number of authorized members can participate in the chain network. It incorporates features from both public and private blockchain networks. Power does not reside with a single authority in a consortium network. It is operated under the direction of a group. So, a consortium blockchain is a private network for a group of companies or entities. "Quorum" and "r3" are blockchain consortium networks [8].

Blockchain is currently transforming many industries, including retail, healthcare, agriculture, automobiles, and medicine. Some exciting applications of blockchain are in cryptocurrency, the IoT sector, swarm intelligence, the automobile field, decentralized finance, and the medical field. IoT-based devices are transmitting a tremendous amount of data for various purposes over the network. The security of this transmission of data is very important because that data may contain some personal and important information. It means transmitted data should be available only to recognized services or people. It needs proper encryption so that unrecognized entities cannot access important data [9]. Data integrity also plays an important role in the IoT. It refers to the genuineness of data. Protection of each layer of the IoT architecture is mandatory. Otherwise, it can lead the whole network to immense problems. Lack of protection gives access to unauthorized parties, and they can make attacks on the network like spoofing, DoS attacks, session hijacking, botnets, and many more. For IoT devices, manufacturers should give device updates at certain times to avoid these kinds of security issues. In the current world, people are using so many IoT gadgets to operate their resources centrally, but this mechanism should be secure; otherwise, attackers might take control of resources or hijack your resources also. Identity protection, data integration, and other issues plague the IoT [10]. The properties of blockchain's decentralized nature and its tamper-proof security can solve many problems in the IoT.

This paper is organized as follows: Section 1 introduces a primer view of the healthcare domain, an overview of IoT and blockchain technology, an overview of data security issues, and how to address security issues using blockchain. The work that has already been done using supporting technologies for the medical healthcare system, like IoT and blockchain, is covered in Section 2. The research proposal, workflow, and IoT-blockchain-based medical healthcare system are all described in Section 3. In Section 4, multiple blockchain networks are used to discuss the latency of the blockchain network. The implementation of our suggested work with mathematical derivation is covered in Section 5. In Section 6, we outline the results and numerous security risks that we have implemented. Section 7 describes the conclusion of our examined work. Section 8, which is the final section, is a future direction for an innovative researcher.

2. RELATED WORK

In recent years, numerous academics have put forth various designs and techniques to offer authentication for accessing IoT data. We'll look at a couple of them in this part of the study. Researchers in [11] implemented a blockchain-based privacy-preserving architecture called healthchain that protects e-health data. To create this healthchain architecture, the blockchain has been built on Hyperledger Fabric, a permissioned distributed ledger solution that uses Hyperledger Composer and stores EHRs using IPFS. Researchers [12] presented the Bell-LaPadula model and classified the peers and transactions into various clearance and security levels to address the issue of scalability. Blockchain-based secure management and analysis of healthcare data are provided by Dwivedi et al. and his team [13]. To prevent various attacks, including denial of service and modification attempts, they have added security and privacy aspects to the proposed paradigm. Applying smart contracts, an advancement of blockchain technology, to the healthcare industry might lead to improved social and personal health data security [14]. MedChain is an efficient data-sharing system, Shen2019medchain and his colleagues [15] developed it. It combines blockchain, digest chain, and structured P2P network techniques to address inefficiencies in the current methods for exchanging healthcare data. Using a session-based healthcare data-sharing system based on MedChain, data sharing is flexible. According to the evaluation's findings, MedChain can increase productivity while meeting security standards for data exchange. A significant infrastructure is needed for the Internet of Medical Things (IoMT) to store and process a massive amount of medical data. IoMT systems with a blockchain data structure are said to give better security and privacy than a central data storage repository because the need

for IoMT applications and platforms on a centralized cloud is incompatible with security [16]. In contrast to the hash codes on the blockchain, a significant quantity of data is saved on a decentralized platform in the IoMT system.

The Oracle [17] has been described by researchers as a smart device that can analyze the data presented and send alarms to both the patient and the healthcare professional. It interfaces directly with smart contracts. One of the modules focuses on the method of collecting and analyzing data from wearable devices and biosensors, either those that patients are wearing themselves or those that are present in the surroundings where patients are being monitored. The authors of the suggested work have utilized two blockchain networks, especially the personal healthcare blockchain and the external record management blockchain. Researchers proposed BlocHIE [18], which is a blockchain-based platform for healthcare information exchange. They examined the various criteria to retain and communicate two different types of healthcare data, namely electronic medical records and personal healthcare data. Researchers built BlocHIE on two loosely coupled blockchains, namely EMR-Chain for electronic medical records and PHD-Chain for personal healthcare data, as a result of their analysis. To properly protect privacy and authentic ability, they combined off-chain storage and on-chain verification procedures within the EMR chain. Researchers also suggested two transaction packing methods to boost system speed and guarantee customer fairness. Dwivedi and his team [19] introduced a novel hybrid approach that combines the advantages of the private key, public key, blockchain, and many other lightweight cryptographic primitives to develop a patient-centric access control for electronic medical records that is capable of providing security and privacy. They have also raised open questions about how to reduce various attacks such as DoS, modification attacks, etc. A unique decentralized approach that guarantees reliable device identification and verification was proposed by researchers and given the name "bubbles of trust" [20].

The availability and integrity of the data are also protected. Their method depends on the security benefits that blockchains offer in order to accomplish this goal and works to establish safe virtual areas (bubbles) where objects may recognize and trust one another. The C++ programming language and the Ethereum blockchain have been used to give a practical implementation of their system. Researchers [21] have developed a secure electronic health record (EHR) system that uses attribute-based cryptosystems and blockchain technology to achieve medical data's secrecy, authentication, integrity, and support for fine-grained access control. They have used attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data, as well as identity-based signatures (IBS) for digital signatures. The suggested blockchain-based architecture attempts to resolve known security flaws in existing smart healthcare systems and increase the reliability of healthcare management systems. The SmartMedChain architecture, an end-to-end blockchain-based and privacy-preserving solution, was developed by researchers [22] for data sharing in the s-healthcare environment. Using the InterPlanetary File System (IPFS), a distributed data storage system with remarkable scalability and durability, encrypted health data has been saved using Hyperledger Fabric.

The Healthchain system, created by researchers in [27], encrypts health data to implement fine-grained access control. It is constructed to safeguard the privacy of enormous volumes of health data and is based on blockchain technology. Healthchain makes guarantee that both IoT data and medical diagnosis cannot be changed or withdrawn in order to prevent medical disputes. They have employed the Userchain (public blockchain) network with proof of work consensus and the Docchain network with Practical Byzantine Fault Tolerance (PBFT) consensus in the aforementioned design. A group of healthcare practitioners manages and maintains the IPFS system in Healthchain.

3. SYSTEM ARCHITECTURE

Since IoT devices are adaptable in terms of deployment and management as well as in terms of interacting with other networks or devices, they may be utilized in a wide range of applications, from smart cities and homes to healthcare, agriculture, and education. In this study, we focus on the healthcare industry, where a variety of detectors and sensors are available to gauge important physical parameters like body temperature, heart rate, oxygen saturation, etc. From the perspective of the IoT's functionality, many layers are significant. Data ordering and transmission to the network layer are tasks of the IoT's perception layer. It also makes it possible for devices to cooperate with each other. In order to transfer the piled-up data from the perception layer to the storage servers via gateways, the network layer is responsible for managing communication. The gathered data is managed by the application layer, and the community of apps or end users receives the processed data. The AES-CBC cryptographic algorithm is used to encrypt the data file in this instance, and the encrypted file is saved on IPFS storage. Because of the blockchain-based mechanism, only authorized individuals can access the patient's data file from the data storage.

3.1 Proposed Model

IoT data is produced by numerous IoT medical sensor types and wearable technology in our proposed architecture. The data is then filtered and inflated as necessary before being placed on IPFS storage. A blockchain network allows for the access of data by authorized users. Applications for the healthcare industry align with the layered architecture of the IoT. The first level consists of sensors or medical devices that serve as a data collection unit for information like pulse rate, oximeter readings, and body temperature. The services that gather data from the first layer and deliver it to the following layer are included in the second level, which also includes communication. Results acceptance and data processing are done at the third layer. Medical researchers retain patient data for both clinical and research goals.

Users are typically divided into two categories: primary users, such as physicians, nurses, and close relatives, and secondary

users, such as health insurance providers, researchers, and drug development creators. IoT inherits the current underlying weaknesses because it operates on top of the conventional Internet. In order to address problems like confidentiality, integrity, and authentication for resource-constrained IoT, cryptographic steps must be employed.

3.2 Preliminaries, Requirements, and Proposed Work

3.2.1. Raspberry Pi

A cheap, compact, and portable computing board is the Raspberry Pi [23]. It can be plugged into a computer monitor, keyboard, mouse, flash drive, etc. The Raspberry Pi comes with software like Scratch that lets users create entertaining videos, games, and animations. Python, the primary core language of the Raspbian operating system, can also be used by programmers to create scripts or programs. The Model B has evolved into the Raspberry Pi B+. The client/server communication script in this work was written in the Python programming language. There are also enhancements like more USB ports, increased GPIO header PIN, decreased power consumption, etc.

3.2.2. RFID Reader-Writer and Tags with MCP3008

Along with the Internet and mobile technology, which are bringing the globe closer together, RFID is a crucial component of the technological revolution. All RFID systems include three fundamental parts. The RFID tag that is affixed to a possession or object is the first. The tag may have sensors in addition to information on the asset or item. The RFID interrogator, which communicates with the RFID tags, is the second element. The backend system, which connects the RFID interrogators to a centralized database, is the third element. The three types of RFID technology are passive RFID, active RFID, and semi-passive RFID. Passive RFID technologies are often divided into low-frequency (LF), high-frequency (HF), ultra-high-frequency (UHF), and microwave categories depending on the radio frequency employed. Since RFID technology has been widely embraced, it is currently used in a variety of applications. RFID antennas, readers, scanners, and printers are a few RFID uses. RFID, or radio frequency identification, refers to a system that wirelessly broadcasts an object's or person's identity. radio waves that are encoded with a special serial number [24].

Tags, transponders, tag readers, antennae, and interfaces are some examples of the components that can make up an RFID system. Individual objects are outfitted with a small, cheap tag in a conventional RFID system. A transponder with a digital memory chip and an exclusive electronic product code is found inside the tag. The interrogator, which consists of an antenna, transceiver, and decoder, activates the RFID tag with a signal so it may read and write data to it. The activation signal from the reader is detected by an RFID tag as it moves through the electromagnetic field. Data that has been encoded in the integrated circuit of the tag is decoded by the reader and sent to the host computer. To reduce the multiple, frequently redundant reads of the same tag to a smaller and more usable data set, the application software on the host analyses the data and may carry out a variety of filtering procedures.

The 8-channel, 10-bit MCP3008 is an inexpensive analog-to-digital converter. This chip is an excellent choice if you only need to read straightforward analog signals, such as those from a temperature or light sensor. A SPI serial connection is used to link the MCP3008 to the Raspberry Pi. To communicate with the MCP3008, you can use either the hardware SPI bus or any four GPIO pins and software SPI. Software SPI is slightly more flexible than hardware SPI since it can utilize any of the Raspberry Pi's pins, whereas hardware SPI is slightly quicker but less flexible because it can only use certain pins [25].

3.2.3. Blockchain

Blockchain technology enables the transmission and storing of transactions. It keeps the information in a block-based ledger. A chain of blocks is created by connecting each block to the one before it. A peer-to-peer network ensures data transfer. Blockchain is a safe and decentralized distributed ledger as a result. Blockchain has attracted a lot of attention in the banking and financial industries over the past several years. These days, it is finding use in additional fields like insurance, energy, industry, and healthcare. Due to its characteristics namely, that it is decentralized, distributed, and secure blockchain gains such widespread adoption in practically all industries. Since the network is decentralized, a centralized authority is not required to run it. To achieve consensus among nodes, data is archived using this approach. Each node in the network contributes to the distribution and upkeep of the ledger. Numerous factors, including cryptography, the consensus mechanism, immutability, traceability, and data replication, contribute to the security of the blockchain [9]. The public-key cryptography used by blockchains. This type of cryptosystem includes a number of security features, including: identity, encryption, decryption, and digital signature. Blockchain generates a set of public and private keys using an asymmetric cryptography method. The accounts of users are identified and authenticated using these keys. The blockchain's append-only immutability technology. The blockchain can't be altered because every block is connected by a cryptographic hash. The blockchain's consensus technique, which is utilized to obtain consensus, relies on processing power to find the block hash by employing a complex mathematical problem. Because the data is distributed, it replicates across all nodes. Blockchain hence lacks a single point of failure. Because blockchain keeps a complete and timestamped history of every transaction, it enables traceability.

3.2.4. Ethereum

Ethereum [26] is an open source, decentralized, distributed computer blockchain platform. In 2014, Vitalik Buterin developed it as a result of being inspired by the Bitcoin cryptocurrency. The Elliptic Curve Digital Signature Algorithm is used in Ethereum, much like it is in Bitcoin. The discrete logarithm issue is the foundation of elliptic curve cryptography, which generates a pair of keys. Secp256k1 is the elliptic curve employed by Ethereum.

3.2.5 IPFS

A distributed peer-to-peer file system is IPFS (Interplanetary File System). The innovation with IPFS is that content-based

addressing has taken the place of location-based addressing. In other words, we need the hash of the data rather than the address where it is stored in order to search for it. A distinct hash is created for each file that is delivered to the IPFS for storage [21]. So, all you have to do to find this file is search up its hash. IoT data is generated in an authentic environment and stored in IPFS storage so that authorized users can access it via the blockchain network. We have experimented with data file encryption using the AES-CBC cryptographic technique. The security of health data in terms of confidentiality, data integrity, and access control mechanisms is the main focus of this study. We have covered reply attacks, masquerade attacks, modification attacks, message tampering, eavesdropping, and brute force assaults in our research.

As we know, lack of trust, inadequate connectivity, weak security, and scalability plague the Internet of Things. The IoT also has other problems, such as device heterogeneity, energy limits, node addressing, and node identification. Temperature, oxygen saturation, pulse rate, and other data created by the data generator are among those that are kept in a file.

Table 1: Types of Attacks

CIA Triad	Types of Attacks
Confidentiality	1. Snooping 2. Traffic Analysis 3. Eavesdropping 4. Brute Force
Integrity	1. Modification 2. Masquerading 3. Replying 4. Repudiation 5. Message Tempering
Availability	1. Denial of Service 2. Session Hijacking 3. Jamming

The data is saved using a particular file naming scheme provided by the RFID chip. The patient data file will be produced using the JSON file format. In order to steal information and amass it for financial advantage, outside hackers gain access to patient and medical systems. They could, for instance, make false claims to health insurance using patient personal information. Hackers that demand a ransom from healthcare businesses in exchange for recovering patient data systems constitute another sort of external theft. Curiosity is another problem with healthcare data security. The remaining instances of insider abuse are brought on by unintentional behaviours like human mistakes, such as putting false information into a healthcare database or clicking on a phishing email. Numerous assault kinds are shown in Table 1 in this article.

Table 2: Acronyms

Notation	Description
IPFS	InterPlanetary File System
D_P	Patient's Data File
D'_P	Patient's Encrypted Data file
K	Shared Secret Symmetric Key
K'	Encrypted Symmetric Key
H_D	Hash of Patient's Datafile (D'P)
PU_R	Public Key of Receiver
PR_R	Private Key of Receiver
E_K	Encryption Using Receiver's Public Key
D_K	Decryption Using Receiver's Private Key

AES-CBC Advanced Encryption Standard- Cipher-Block Chaining

Algorithm 1: Data Encryption

1: Function Encryption: Input- Data File D_p, Output- Encrypted file D'_P

2: Select the encryption algorithm (E.g., AES-CBC)

3: Collect a symmetric key K

4: Generate a random initial vector IV

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

6: Return the encrypted file (D'_p) on IPFS storage and K' on blockchain

Utilizing the symmetric key (K) and initial vector IV in the encryption procedure, we encrypt the data file (D_p). According to algorithm 1, after using a symmetric key and an initial vector (IV), ciphertext (D'_p) will be generated. After data file has been encrypted, the symmetric key (K) is decrypt using the recipient's public key (PU_R) and saved on the blockchain platform for further use. On IPFS storage, the encrypted file (D'_p) will be kept. A hash value serving as an acknowledgement of the supplied file will be received from IPFS. As seen in algorithm 2, the receiver's private key (PR_R) has been used to decrypt the symmetric key (K') for the original data file (D_p). Since IPFS storage is now more widely accessible, data confidentiality is necessary. This can be a breach of specific data storage policies that reveal sensitive data. The owner of that content may request authenticity confirmation from IPFS. It appears that IPFS provides quick and reliable fault-tolerant file storage for content. As IPFS develops, it might make use of a privacy layer to conceal personally identifiable information that is also encrypted at rest, ensuring that no sensitive information is revealed. The data file (D_p), is encrypted with an AES symmetric key (K). Here, the symmetric key (K) is encrypted using the receiver's public key (PU_R) of the RSA method to produce the encrypted key (K').

Algorithm 2: Receiver-side data decryption

1: Input: (Encrypted File (D'_P), K', H_D)
:: Symmetric key encryption using receiver's public key (PU_R)
2: Output: Decrypted Data File (D_P)
3: Function Decryption ((D'_P), K', E_K)
4: (K) ← DecryptionAsym , (E_K ,PR_R) :: Key Decryption using Receiver's Private Key (PR_R)
5: DPatient ← D_K (D'_P, K)
6: End Function

Algorithm 3: Uploading documents to the Interplanetary File System and storing hashes on Blockchain

1. Function Upload (D'_P): Encrypted Patient's Data File
2. for each Datafile
3. do
4. Retrieve (D_P) Patient_Datafile and encrypt it using Symmetric key K (AES)
5. K'= E_K (K, PU_R)
6. Send (D'_P) Patient_Datafile to IPFS
7. IPFS stores (D'_P) Datafile and assigns a hash value to it.
8. A hash value is returned from IPFS as an acknowledgement of a stored file (D'_P)
9. IPFS hash value is sent to Blockchain
10. Encrypted Key K' is sent to Blockchain
11. Function Storage (IPFSHash, K'):
12. for each IPFSHash and K' do
13. Web3 is invoked to execute smart contracts.
14. Metamask displays request to approve transaction payment
15. Payment is approved: IPFSHash and K' are stored on Ethereum

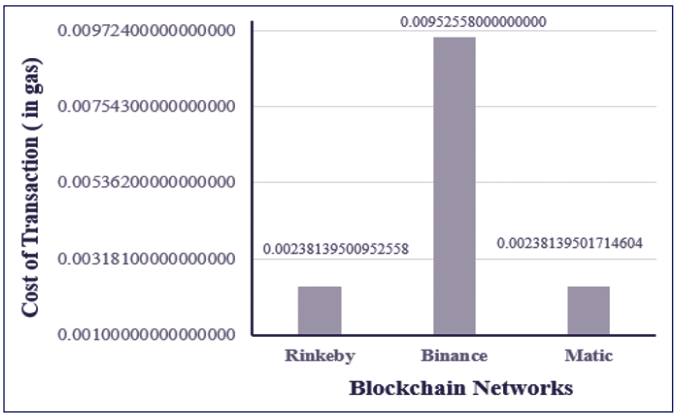
The source node requested to IPFS, to store its processed data file on that platform. For data file encryption, a receiver's public key (PU_R) is used. After the use of that bundle, a data file is received on the IPFS platform, and its hash value is computed. The calculated hash value (H_D) will be sent to the source node as the ID of that data file. In IPFS, a copy of a requested file is cached on the requester's node. There will be more cached copies of the datafile as more users seek it. Any node or group of nodes that has the file on it can respond to subsequent requests for it. Numerous nodes increasingly split out the responsibility for providing the requested data and completing the request. It necessitates a new kind of Web address. The decentralized web employs content-based routing technologies like IPFS instead of address-based routing, which requires you to know the exact location of the data and supply a precise URL to that data [11]. You should encrypt a file before importing it if you need to keep the content confined to a small group of people but yet want it to be available to others. However, imported files are voluntarily not encrypted by default, despite the fact that data transit is encrypted in both directions. In our implementation, when an encrypted data file (D'_P) is delivered to the IPFS platform, we use the AES-CBC (symmetric) algorithm to encrypt it. After the successful execution of the smart contract with the involvement of Web3, the hash value (H_D) and encrypted key (K') will be stored on Ethereum, which is illustrated in Algorithm 3.

4. LATENCY OF THE BLOCKCHAIN NETWORK

Blockchain technology offers new digital capabilities for authentication and permission that eliminate the need for some sort of centralised administration. As a result, it allows for the formation of new digital relationships. The immutable smart contract protocol or rule used by blockchain technology implies that once it is implemented, it cannot be changed [9]. As it is exceedingly difficult to replicate a creation-like environment for performance testing, performance assessment in blockchain is difficult. The technical authentication protocol has to be evaluated for network latency depending on block size, network type, estimated transaction size, and how long it takes a query to return results. We have tested the transactions on various blockchain networks and determined how much gas is required to deploy smart contracts on the blockchain network. We also computed the amount (in USD) of gas required to upload the AES encrypted key (K') and hash (HD) of encrypted data files to the blockchain network. For transactions, we have utilized the blockchain networks of Rinkeby, BSC, and Matic.

We come to a conclusion and note that deploying smart contracts on the MATIC network requires less gas. On Ethereum, the Kovan and Rinkeby networks consumed more gas than the Binance and Matic networks in assessments of gas requirements. If you pay a lower cost, your transaction may likely go much more slowly, depending on the network and other parameters. We come to a conclusion and note that deploying smart contracts on the MATIC network requires less gas value. On Ethereum, the Kovan and Rinkeby networks consumed more gas than the Binance and Matic networks in assessments of gas requirements. If you pay a lower cost, your transaction may likely go much more slowly, depending on the network and other parameters. The comparison of various blockchain networks for the amount of gas used during the deployment of smart contracts on the blockchain network is shown in Fig. 1. The actual cost of deploying a smart contract on the blockchain network is shown in Fig. 2, which also shows the conversion of the gas value into USD ($).

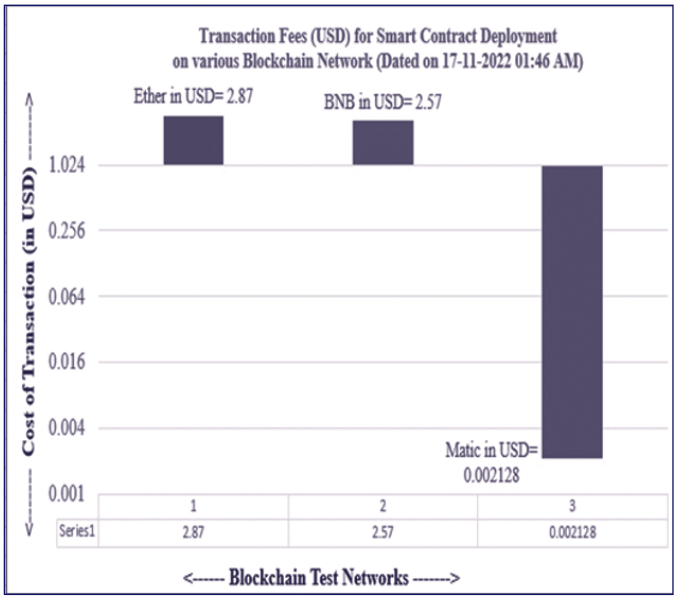
Fig. 1. Required gas value for smart contract deployment on a blockchain network



5. IMPLEMENTATION

The two phases of our experimentation are as follows: In the initial stage of IoT deployment, Raspberry Pi, tags, and medical sensors have been used. The second phase involved developing the blockchain side using the Ethereum platform, Solidity as the programming language, Metamask (a blockchain wallet), and IPFS for distributed storage. We successfully integrated two technologies in this execution, outlining how

Fig. 2. Required USD ($) for smart contract deployment on a blockchain network (conversion of gas to USD)

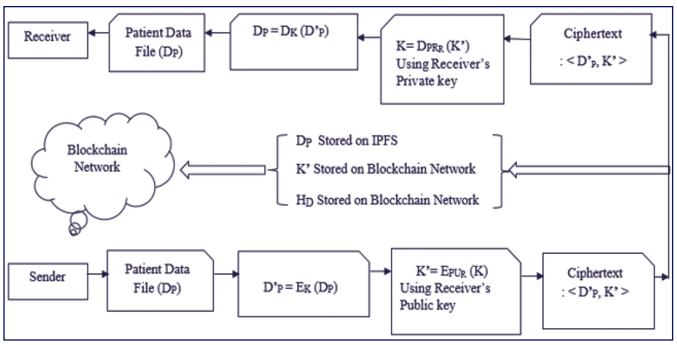


medical data is produced and safeguarded in the context of the Internet of Things. It also included instructions on how to store that data on IPFS storage and how the blockchain network may use it. The RFID gadget created a file with the patient's individual ID. The output data is subsequently filtered 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 is 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. The hash value of a specific data file for the patient is generated by IPFS storage and sent back to the IoT platform. First, we use the Python.objcrypt module to encrypt that data file using the AES-CBC encryption algorithm on the IoT platform. We upload the encrypted file to IPFS storage. A fixed-length hash value (H_D) of the stored file is returned by IPFS storage. For later use, the retrieved hash value (H_D) is stored on the blockchain network.

5.1 File encryption and decryption using a mathematical derivation

Here, a symmetric key (K) is used to encrypt the patient's data file (D_p). When the encrypted data file (D'_p) is transmitted to IPFS storage, IPFS responds with the hash value (H_D) for the stored file as an acknowledgement. The hash value (H_D) of the protected file (D'_p) is one of the values saved on the blockchain, and the other value is (K'). The receiver's public key (PR_R) is used to encrypt the symmetric key (K), and that encrypted symmetric key (K') stored on the blockchain network. Anyone wishing to view a data file (D_p) must visit the blockchain platform and utilize the H_D and

Fig. 3. Cryptographic process of proposed work



K'. Due to the file encryption approach, the receiver can access the data file in protected mode by using the hash value (H_D) of the data file. A symmetric key (K) that the receiver can use to decrypt the file is simultaneously used to encrypt it with the receiver's public key. The protected file (D'_p) is decrypted and transformed back into the original data file (D_p) once the key (K') is decrypted using the receiver's private key (PR_R). The following steps show how the overall transmission and reception of data files (D_p) from the data origin to the data consumer take place.

The following steps show how the entire receiving and transmission of data files (D_p) from the data origin to the data consumer takes place.

Step 1: The patient's data file (D_p) is encrypted using the symmetric key K, and that file is converted into a protected data file (D'_p).

Step 2: The encryption process E_K is performed

using the recipient's public key (PR_R), which is used to transform the symmetric key (K) into the

Step 3: A protected data file (D'_p) is sent to IPFS file storage.

Step 4: IPFS sends the fixed-value hash (H_D) as an acknowledgement to the source platform.

Step 5: Retrieved hash value is stored into a blockchain platform

Step 6: Another entity, K', is also stored on the blockchain platform.

Step 7: The user can send the request to IPFS via blockchain for the data file (D_p).

Step 8: IPFS sends the reply (data file D'_p) based on the matched hash (H_D).

Step 9: The decryption process DK is performed using the receiver's private key PRR, and that encrypted key (K') is converted into its original form K.

Step 10: Using a symmetric key (K), a protected data file (D'P) is converted to an original data file (DP).

encrypted form (K').

5.2 Implementing a Model

In order to establish data confidentiality, integrity, and access control measures, we employed smart contracts, which are implemented in the Ethereum Solidity programming language, for IoT-based healthcare systems. All of the medical sensors have been fastened to the patient's body, and the data they produce is saved in a special file that the RFID device generates. Fig. 3 illustrates the cryptographic procedure we used to obtain the patient data file from the distributed storage using a blockchain-based authenticated mechanism. The data file is encrypted using the AES-CBC cryptographic method and stored on an IPFS server. Due to the blockchain-based technology, only authorized users are able to access the patient's data file from the data store and preventing network attack.

Fig. 4. Platform that shows the received data file with the sender's address

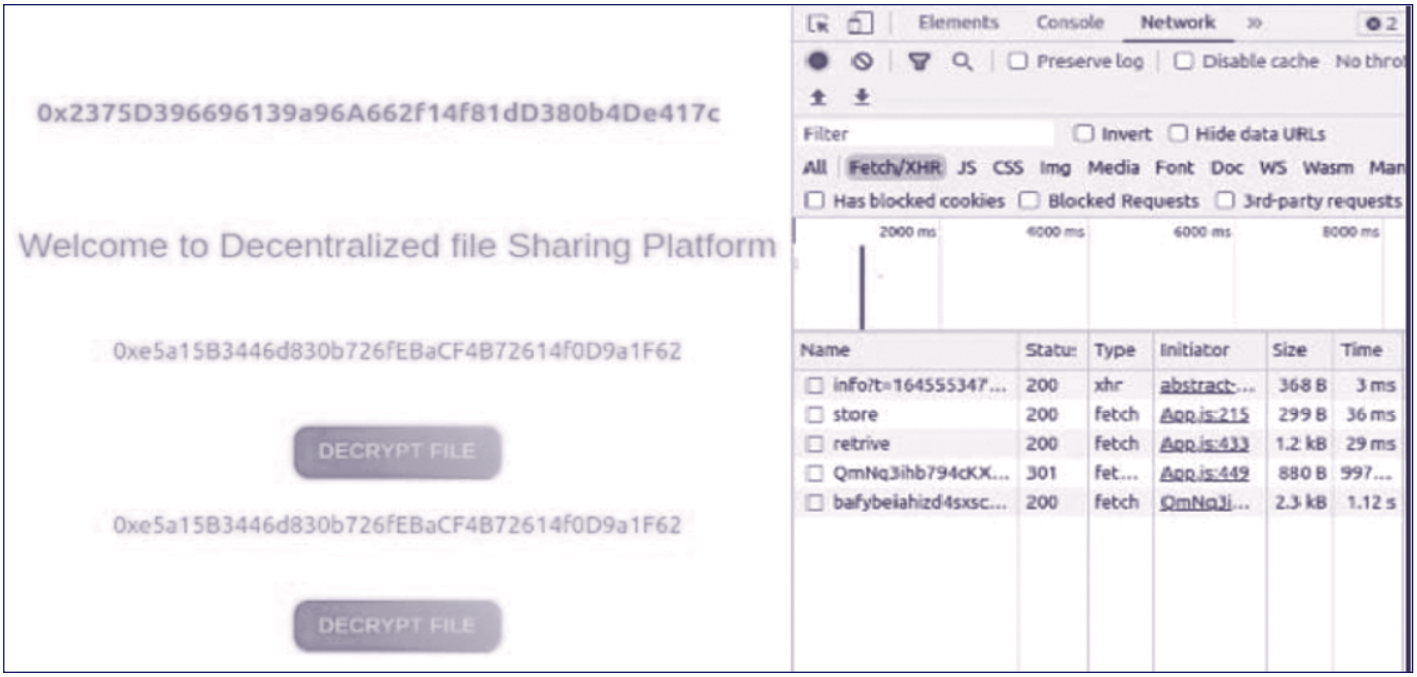
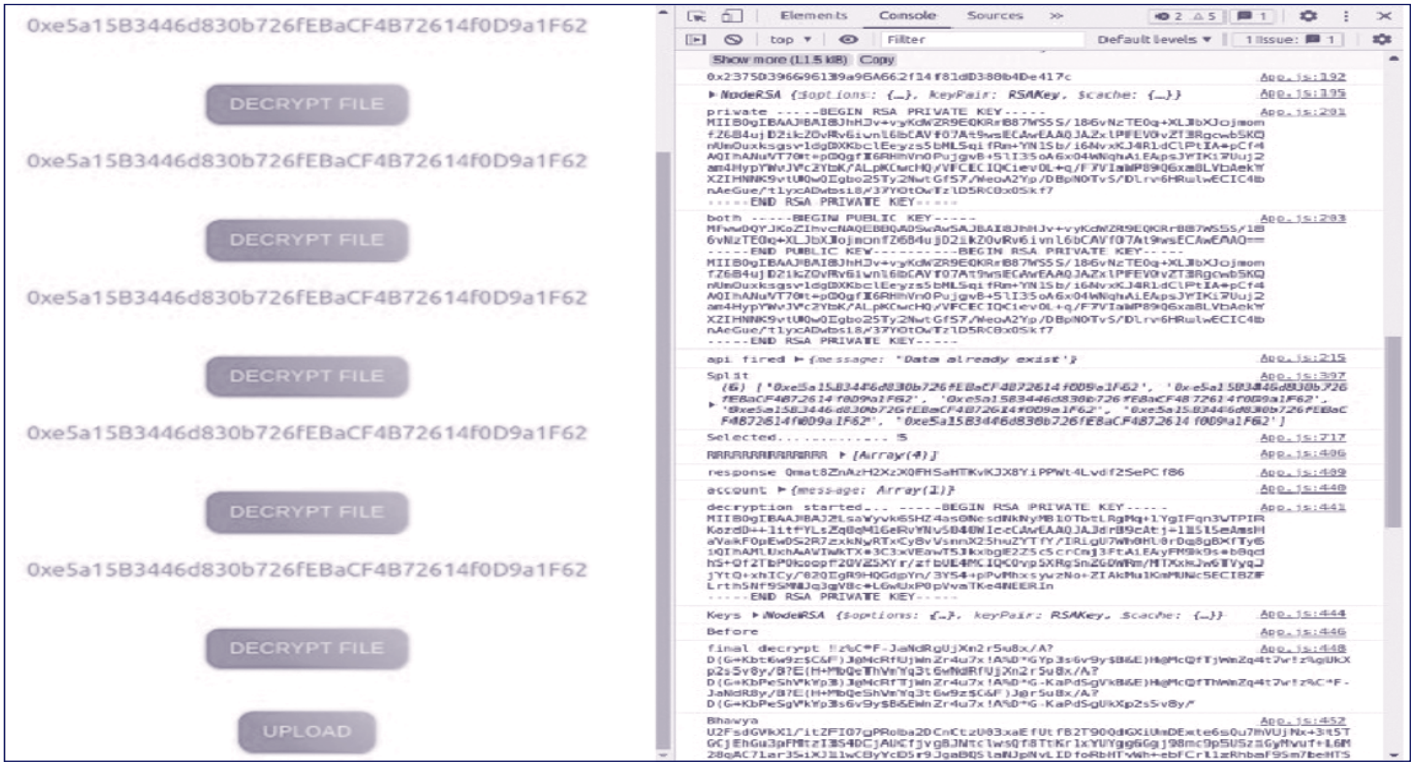


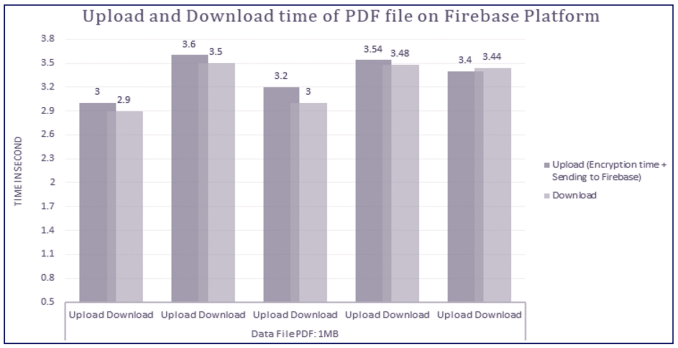
Fig. 5. Data file decryption using private key (PR_R) and symmetric key (K)



5.3 File Sending and Receiving via Blockchain Network

The data file (D_p) is secured with a cryptographic technique (AES) and kept on the IPFS platform. The receiver's public key (PU_R) encrypts the symmetric key (K). IPFS storage returns the hash value (H_D) for the corresponding file that was stored. The blockchain platform stores the hash value (H_D) and encrypted symmetric key (K') that have been obtained. As shown in Fig.4. the recipient must visit the blockchain platform, and use their private key

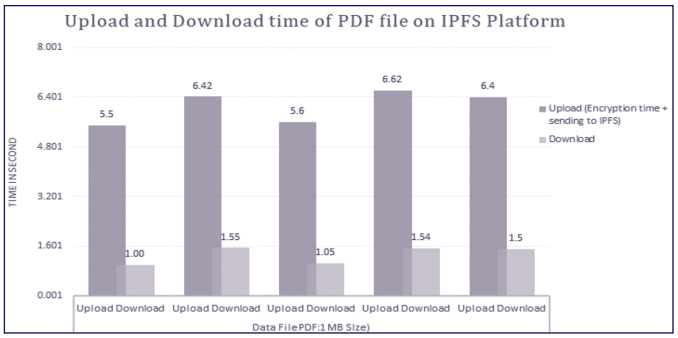
Fig. 6. Upload-Download interval for. json data file on Firebase platform.



(PR_R), and the hash value (H_D) of the saved data file to decrypt it in order to obtain the original data file (D_p) from IPFS.

As everyone knows, an RSA (Rivest-Shamir-Adleman) key pair consists of a private key and a

Fig. 7. Upload-Download interval for. json data file on IPFS platform.



public key. Digital signatures are created using the RSA private key, but the RSA public key is used to verify them. The RSA public key can also be used to encrypt DES or AES data keys, and the RSA private

key can be used to recover the keys. Platform used

by the recipient, from which the recipient can download and upload data files to the IPFS platform. In our implementation, the symmetric key (K) used to encrypt the patient's data file (D_p) using AES is encrypted using the sender's public key (PU_R). The encrypted file (D'_p) is converted into the original file (D_p) using the user's private key (PR_R), as shown in Figure 5.

During testing, it has been discovered that our system supports the submission of files in the JSON, PDF, and picture data file formats. Figure 5 illustrates how to encrypt the patient›s data file (D_p) using symmetric key (K), which is encrypted using the recipient's public key (PU_R). The receiving end uses a hash value (H_D) to obtain the data file from the IPFS. The retrieved data file (D'_p) is encrypted; as a result, the symmetric key is decrypted with the receiver's private key, and the obtained data file is then transformed back into the original data file (D_p) using that symmetric key (K_S).

6. RESULTS

We initially tested our implementation on Ganache, and then we simulated main net behaviour using Kovan, Rinkeby, Binance, and the Matic network. There is a single instance of the Ganache platform that mimics the blockchain network. The interface for adding and viewing records is built using ReactJS, and the backend is built using JavaScript. The patients' cryptographic keys have also been kept in MongoDB. In order to replicate a blockchain network, we employed the Ethereum platform with Solidity as our test blockchain.

The blockchain is additionally communicated with via Web3-JS. In order to test the IPFS network, we employed INFURA, which provides dependable, safe, and scalable access to the IPFS gateway. We examined the upload and download speeds of data files for our solution using Firebase and IPFS. The file (. JSON, 160 kB) was utilized five times on both an IPFS distributed database and a Firebase centralized database, and the upload and download times were recorded. Figures 6 and 7 show the Firebase platform's results for file upload and download times as well as the IPFS platform's time. How rapidly data files may be recovered via IPFS depends on a variety of factors, including the number of systems storing the records, the location of the nearest system possessing the record, the number of systems storing the records, and other factors.

Analysis of the proposed framework in comparison to current blockchain technologies. Confidentiality, integrity, and availability are the three main security considerations that must be taken into account by any model developer. Encrypting data makes guarantee that only authorized users can access the system. Both availability and integrity guarantee that messages are sent to their intended recipients without being changed, and both ensure that users can always access the data they require.

It is a comparison of the proposed work's confidentiality, data integrity, and access control features with those of the current blockchain approaches. The suggested architecture has been evaluated with current blockchain-based implementations, like [15], [18],[21],[22] and [27]. In terms of data confidentiality, access control, data integrity, and scalability, it is evident that the proposed system addresses the shortcomings of the current systems.

The patient data in our system is stored on IPFS using cryptography techniques, so data security is a crucial responsibility. The actual, enormous data is saved after encryption on the IPFS storage, while this blockchain architecture just keeps a hash of the transaction on the blockchain network. This solution, which takes a patient-centric approach, ensures the protection of patient data and offers authorized access with patient authorization. Additionally, the blockchain

solutions' smart contracts feature combines to support high-level encryption and guarantee patient anonymity in their medical records. To create strong blockchain data security solutions, the data saved on IPFS is also encrypted using a unique AES-CBS cryptographic method.

The patient data file (D_p) is encrypted using the cryptographic method before being saved to IPFS. Here, the AES-CBC encryption method is used to protect the file contents by encrypting the symmetric key (K) with the recipient's public key (PR_R). Eavesdropping attacks occur when a hacker intercepts, deletes, or modifies data that is being sent between two devices. Snooping, also known as eavesdropping, accesses data exchanged between workstations using open network connections. A hacking method known as a "brute force attack" uses trial and error to crack encryption keys, passwords, and login information. It's a simple but effective way to gain unauthorized access to user accounts. Our research has explored the use of brute force attacks, snooping, and eavesdropping.

Table 3: Analysis of the proposed framework in comparison to current blockchain technologies

Scheme	Blockchain Platform	Confidentiality	Data Integrity	Scalability
Medchain [15]	Consortium Blockchain	Yes	Yes	No
Blochi [18]	Private Blockchain	No	Yes	No
Wang & Song [21]	Private Blockchain	Yes	Yes	No
SmartMedChain [22]	Private Hyperledger	Yes	Yes	No
Healthchain [27]	Consortium Blockchain	Yes	Yes	Yes
Proposed Work	Public Ethereum	Yes	Yes	Yes

Data integrity refers to the permanent and unchangeable storage of data. It cannot be changed or eliminated. Each block in a blockchain holds the hash value of the preceding block in addition to the data, which is saved as hash values in each block. Despite relying on a third-party provider, the consensus method, digital signature, and built-in cryptographic algorithm form the foundation of this blockchain framework's confidence. Since all the blocks are connected, any modification to the original data will affect its hash value, and since altering the record is computationally challenging, the non-tampering of the patient data is also expressly guaranteed. The original data is saved in IPFS storage once a unique cryptographic procedure has been carried out. We also explored a modification and response attack, which may be prevented by being aware of how encryption works. When cryptography is used, the communication is usually encrypted. On the receiving end, the message is unlocked using the decryption technique. To guard against such attacks, the sender and recipient are obliged to select a session key at random. This session key represents a code type that will be valid for just one interaction between sender and recipient. It is impossible to set up this code again. Timestamps are another tool that can be used. A timestamp that has passed its expiration date cannot be cracked by hackers because timestamps have a lifespan.

The suggested framework offers encrypted data storage in IPFS while maintaining the majority of security requirements and addressing the scalability issue in the current approaches. The scalability of the suggested approach has shown that it is capable of processing massive data sets quickly.

7. CONCLUSION

Numerous issues cause performance degradation for the IoT environment. A few of such issues are unattended, resource-constrained, heterogeneous devices, sometimes resulting in security, privacy, and reliability concerns. During our research, it has been our prioritized motive to showcase and avail the usage of blockchain technology, specifically in the healthcare system, in diverse situations. The diverse can include a variety of steps such as data sharing, clinical research development, or patient health diagnosis. Numerous IoT sensors and cryptographic models are used to generate patients' data and secure the same data. IPFS storage can be used to store encrypted data. In this research work, an Ethereum based, blockchain framework has been implemented for securing data storage and providing efficient access control between stakeholders like patients, doctors, pharmacists, and other participants through encryption techniques and access control mechanisms. With the upsurge in health data every year, we look forward to enhancing this framework with rigorous simulations in scalability and comparing it with other blockchain configurations that will invite further attention in future research tasks.

8. FUTURE WORK

For performing the current prototype implementation, the IoT device raspberry pi has been used to generate IoT data and apply a cryptographic algorithm that has been used for various methodologies in data encryption on the IoT platform. Innovative researchers may use progressive IoT tools to support advanced encryption algorithms. There is a constant rise in advanced encryption algorithm usage, which will motivate researchers to use progressive IoT tools, which are well-equipped for advanced encryption. IPFS storage, which is certainly needed for decentralized file storage for various types of peer-to-peer transmission of data, is used to store the encrypted data. In our research for a smart contract, the Ethereum-based solidity programming language has been used. Various other platforms like Hyperledger can be utilized for penning an agreement between entities in the system instead of the Ethereum platform.

REFERENCES

1. *Sethi, P., & Sarangi, S. R. (2017). Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017.*
2. *Dhanvijay, M. M., & Patil, S. C. (2019). Internet of Things: A survey of enabling technologies in healthcare and its applications. Computer Networks, 153, 113-131.*
3. *Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 17(2s), 1-17.*

4. *Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The internet of things for health care: a comprehensive survey. IEEE access, 3, 678-708.*
5. *Restuccia, F., Kanhere, S. D., Melodia, T., & Das, S. K. (2019). Blockchain for the internet of things: Present and future. arXiv preprint arXiv:1903.07448.*
6. *Ahmad, L., Khanji, S., Iqbal, F., & Kamoun, F. (2020, August). Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In Proceedings of the 15th international conference on availability, reliability and security (pp. 1-8).*
7. *Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., & Li, Y. (2020). Performance analysis and comparison of PoW, PoS and DAG based blockchains. Digital Communications and Networks, 6(4), 480-485.*
8. *Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. Ict Express, 7(2), 229-233.*
9. *Qashlan, A., Nanda, P., He, X., & Mohanty, M. (2021). Privacy-preserving mechanism in smart home using blockchain. IEEE Access, 9, 103651-103669.*
10. *Asghari, P., Rahmani, A. M., & Javadi, H. H. S. (2019). Internet of Things applications: A systematic review. Computer Networks, 148, 241-261.*
11. *Chenthara, S., Ahmed, K., Wang, H., Whittaker, F., & Chen, Z. (2020). Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. Plos one, 15(12), e0243043.*
12. *H. Wu, A. D. Dwivedi, G. Srivastava, Security and privacy of patient information in medical systems based on blockchain technology, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 17 (2s) (2021) 1–17.*
13. *Wu, H., Dwivedi, A. D., & Srivastava, G. (2021). Security and privacy of patient information in medical systems based on blockchain technology. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), 17(2s), 1-17.*
14. *Griggs KN , Ossipova O , Kohlios CP , Baccarini AN , Howson EA , Hayajneh T . Healthcare blockchain system using smart contracts for secure automated re- mote patient monitoring. J Med Syst Jul. 2018;42(7):130.*
15. *Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient healthcare data sharing via blockchain. Applied sciences, 9(6), 1207.*
16. *Dilawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019). Blockchain: securing internet of medical things (IoMT). International Journal of Advanced Computer Science and Applications, 10(1).*
17. *Rogers, D. (2019). A visit to the Oracle: Reviewing the state of construction industry digitalisation. Construction Research and Innovation, 10(1), 11-14.*
18. *Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018, June). Blochie: a blockchain-based platform for healthcare information exchange. In 2018 ieee international conference on smart computing (smartcomp) (pp. 49-56). IEEE.*
19. *Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326.*
20. *Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. Computers & Security, 78, 126-142.*
21. *H. Wang and Y. Song, "Secure cloud-based ehr system using attribute-based cryptosystem and blockchain," Journal of medical systems, vol. 42, no. 8, pp. 1–9, 2018.Wang, H., & Song, Y. (2018). Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. Journal of medical systems, 42(8), 1-9.*
22. *El Majdoubi, D., El Bakkali, H., & Sadki, S. (2021). SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework. Journal of Healthcare Engineering, 2021.*
23. *Zhao, C. W., Jegatheesan, J., & Loon, S. C. (2015). Exploring iot application using raspberry pi. International Journal of Computer Networks and Applications, 2(1), 27-34.*
24. *Abad, E., Palacio, F., Nuin, M., De Zarate, A. G., Juarros, A., Gómez, J. M., & Marco, S. (2009). RFID smart tag for traceability and cold chain monitoring of foods: Demonstration in an intercontinental fresh fish logistic chain. Journal of food engineering, 93(4), 394-399.*
25. *Hassen, H. B., Ayari, N., & Hamdi, B. (2020). A home hospitalization system based on the Internet of things, Fog computing and cloud computing. Informatics in Medicine Unlocked, 20, 100368.*
26. *Ethereum - Wikipedia. (2015, July 30). Ethereum - Wikipedia. Retrieved November 12, 2022, from https://en.wikipedia.org/wiki/Ethereum*
27. *Xu, J., Xue, K., Li, S., Tian, H., Hong, J., Hong, P., & Yu, N. (2019). Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet of Things Journal, 6(5), 8770-8781.*