Ethereum based Blockchain Technology to achieve Confidentiality, Integrity and Access control in IoT-Generated Healthcare Records*

Ochchhav Patel[1], Dr Hiren Patel[2]

LDRP-ITR, Kadi Sarva Vishwavidyalaya, Gandhinagar, Gujarat-382015[b,]*

[a] *Kadi Sarva Vishwavidyalaya, Gandhinagar, 382015, India*
[b] *Vidush Somany-ITR, Kadi-382715, Kadi Sarva Vishwavidyalaya, Gandhinagar, India*

Abstract

The Internet of Things (IoT) is a network of active and passive objects that interact with each other for information exchange. Due to the immense acceptance of the concept, the IoT utility rate has increased exponentially in recent years. Being an open (and sometimes not-physically-observed) network, the issue of data privacy and security becomes a severe concern on account of the presence of untrusted and malicious users on the network. Most of the existing security approaches are centralized in nature, which leads to bottlenecks and obscurity in public verifiability. Due to its functionality, blockchain technology could be a solution to these problems, owing to its distributed immutable ledger that is cryptographically secured. In this research, we intend to address the security issues in terms of confidentiality, integrity, and access control mechanisms in the IoT for a healthcare system where the data files of a particular patient are encrypted and stored on the blockchain storage in a distributed fashion and accessed through smart contracts. We have observed the efficiency and time complexity of IoT based medical health care system with the utilization of kovan, binance smart chain, rinkeby, and matic blockchain networks. The authors

*Fully documented templates are available in the elsarticle package on CTAN.

*Ochchhav Patel
Email address: ochchhav_ce@ldrp.ac.in (LDRP-ITR, Kadi Sarva Vishwavidyalaya, Gandhinagar, Gujarat-382015)

[1]

propose a secure model for IoT based healthcare systems with the incorporation of the blockchain network.

Keywords: `Blockchain`, Internet of Things, Security, IPFS, Medical Healthcare

1. Introduction

In the modern era of advancement in technology, one of the most promising technologies that aims to enhance the quality of human life could be the Internet of Things (IoT). In many real-life problems and challenges that are now essential for humans to sustain, the IoT plays a massive role. Such use-cases are healthcare, automotive industries, agriculture, education, and many cross-cutting business applications. The core strength of the IoT idea is the high impact it will have on several aspects of everyday life and the behaviour of potential users. Since the working mechanisms of IoT applications vary due to the heterogeneity nature of IoT devices, addressing IoT security has become a challenging task. The individual user who visualizes the ground-level effect suggests that the IoT introduction will be visible in both working and domestic fields. HaddadPajouh [1], assisted living, healthcare, and enhanced learning are some of the only widely known possible application scenarios in which the newly driven enhanced paradigm will play a leading role in the upcoming years to come. There are a lot of challenging and important issues that need to be taken into consideration, and the technological, as well as social, knots have to be untied, formally accepting the idea of IoT widely. With the arrival of the IoT, it also aspires to solve numerous new problems surrounding its networking aspects. As a matter of fact, wherever the use of IoT is acknowledged, it will surely be characterized by the limited available resources in both computation and energy capacity [2]. As far as the rational viewpoint is concerned, an IoT system can be considered as a collection of modern smart devices that interact in a collaborative team that is often bonded to fulfil a communal goal. On the technological front, IoT deployed instruments to upgrade various processing and

communication architectures, methodologies, and modern technologies used in strategies that are committed to achieving their objectives. An adaptation to different environments and being able to self-heal in IoT has a very important role to play in infrastructures that may be able to survive the normal and unexpected changes in the target environment. As things currently stand, privacy and security concerns should be prioritized in a network.

In the IoT, sensors, physical objects, gateways, machines, and networks are very important components. If an IoT network is well customized, it has the potential to grow expeditiously and produce results in the variety, rapidity, and overall volume of the collected data. This volumetric is responsible and essential for opening opportunities for paramount value and the generation of revenue from resources. Although, the primary challenge for the IoT environment modules is probably how to analyze the huge volume of hefty information from all the legitimate sources and to take the required action in a given authentic-time. Due to the increase of interconnected objects and data traffic, there is a requirement and necessity for standardization and analytic techniques. IoT systems require a common analytic platform to support big data, which can also be provided as a service to IoT applications.There are various data mining methods such as machine learning, artificial intelligence, and other decision-making algorithms [3]. These methods enable computational progressions to discover patterns in very largely defined datasets. Due to substantial cost, all these techniques can be essential in organizing raw data as well as extracting usable information and knowledge from it, but due to their substantial cost, they also become a limitation. Cloud technology is used to store and handle data. With the amount of data being used in the industry today, it seems that cloud technology is the only way to handle such large data. There are multiple cloud platforms available on the market with a variety of storage capacity, computational capabilities, differences in application protocols, interoperability, advertising models, and gateway support etc. Although it has some advantages and some disadvantages, it needs to be considered. Network delays, reliability, bandwidth, congestion, and availability are some of the issues that can occur

while transferring large amounts of data from devices such as sensors and smartphones to the cloud infrastructure. In addition, there are various other issues that can play a vital role in deploying the cloud computing [4]. synchronization and standardization between different cloud vendors, maintaining the balance and correspondence between IoT requirements and cloud service environments.

The ability of multiple devices and systems to interoperate with the deployed hardware and software is called interoperability. There are numerous standards and modern technologies that are currently being used for IoT development, apart from so many solutions from various vendors, which leads to the massive heterogeneity that causes interoperability issues. All the layers of IoT interoperability [5] are considered thoroughly. A well-layered framework with high standardized architecture is used to overcome this issue. Communication infrastructure and protocols are usually associated with technical interoperability. It is an important part of an IoT system to provide interoperability over heterogeneous devices, networks, and an assortment of communication protocols such as CoAP, IPv6, 6LoWPAN, IPv4, Wi-Fi, and Bluetooth. IEEE 1905.1 standard [6] was designed for interoperability support and provides a common interface that is an abstraction layer to fleece diversity of MAC widely positioned in-home networking technologies. The solutions to interoperability problems are usually based on APIs [4], implementation of gateways [7] [8] integrating smart resource-constrained objects into the internet using virtual networks [9].

In IoT, for the automatic adaptation between various application protocols, there are several API-based resolutions available for interoperability. According to the protocols in use, IoT devices can be divided into two categories based on the support door TCP/IP protocol suite. IoT applications that support the use of MQTT-SN, MQTT, CoAP, and some other protocols also support the use of TCP/IP smoothly. Though there are still some applications without the support as stated above, the issue of interoperability comes into the picture. There is a need for communication compatibility in a heterogeneous environment, for new protocols always arise with the advancement of technology. We have the luxury of implementing APIs in different software and on different cloud platforms.

Open APIs, which are necessary for application interoperability and which are provided by some operating systems like Contiki, TinyOS, Riot OS, LiteOS, etc., also enable modular designs.

The reliability of the communication system can be defined by the performance of the radio transceiver and communications microcontroller. Users can expect different levels of reliability, so approaches to designing an IoT system can be different at the various users' as well as applications' level. Transmission Control Protocol in computer networking, which is used on the internet, is very reliable, whereas on the other side user datagram protocol is unreliable as no guarantee of delivery of data. Hence, it's safe to say that the use of UDP is advised where the loss of some data may be tolerated due to large data sets. To enhance and upgrade the availability of the computer networks providing redundancy of data, the other standard protocols are the hot standby router protocol, the virtual router redundancy protocol, and the gateway load balancing protocol used [3].

The diversity of technologies and standards is one of the major identified challenges in the development of IoT applications. The development and progress of IoT will depend on a larger basis on the standardization [5] of IoT architecture and upgraded communication technologies where IoT open standards can play a massive role and be one of the key factors for IoT development [4]. This type of standard is an important enabler for innovation because of its availability to the public. To make a framework for IoT standards, the major standardization bodies working in this direction are ETSI, ITU, IEEE, OneM2M, and NIST to provide open standards & architectures, seamless connectivity, and interoperability. In the deployment of IoT applications, security and discretion issues are recognized as key challenges because there are plentiful examples of susceptibilities, threats, and various kinds of risks [10].

It has been predicted by several security experts that IoT is one of the most susceptible technologies and they still expect more targeted outbreaks on currently existing and developing infrastructure, such as a denial of service attack, data loss, and various kinds of ransomware for various IoT applications. IoT sys-

tems should be framed within an open IoT architecture and a set of standards to enable the integration of various technologies and support full interoperability. To ensure service continuity, the IoT architecture needs to provide interoperability and support full mobility. Accordingly, one of the main challenges for IoT systems is to use an open, integrated, and standardized architecture with separated application logic and hardware infrastructure [3]. There are many other challenges in IoT networks, such as scalability to handle the network even if the amount of work increases, unique identification of IoT devices in a network, and self-configuration also. Cloud services are provided under the centralized control of one reliable entity. Hence, the cloud is vulnerable to a single point of failure concerning security and privacy issues, including data manipulation and the availability of cloud services. Regarding data manipulation, the cloud service provider has to be a trusted party as it has control over the data stored in the cloud and related services. Therefore, the cloud provider can manipulate user data. Blockchain, on the other hand, is orchestrated in such a way that all miners and full nodes in the blockchain network maintain the same copy of the blockchain state and trust is distributed among all network nodes [11]. Hence, if one device's blockchain data is altered, the system will reject it, and the blockchain state will remain untampered.

Bitcoin is a well-known blockchain based cryptocurrency that uses the core mechanism of blockchain. A blockchain is a public ledger where all the transactions are stored in a chain of blocks. The chain continuously grows when new blocks are joined to it. Blockchain technology has some key characteristics, such as immutability, decentralised network, persistency, and anonymity. In blockchain, some core technologies, such as distributed consensus, digital signature-based asymmetric cryptography, and cryptographic hash, enable a decentralized environment[12].The structure of a block in a blockchain where the first block of a blockchain is called a "genesis block," which has no paternal block. A block consists of the block header and the body of the block, where the block header includes the block version, merkle tree, timestamp, nonce, parent block, and nBits. The Transaction Counter and the number of transactions can

be found in the structure of the block body. In a blockchain-based decentralized organization, people and machines can coordinate through a set of intended smart contracts, without the need for the involvement of traditional business entities [13]. In commercial governance, distributed decision-making power with multiple signature technologies is used to restrict action until all relevant parties do not agree to a transaction. Blockchain technology has wide-ranging applications, and can be used in numerous sectors like education, business, healthcare, finance, automation, manufacturing, and another domain also [14].

There are some issues in the IoT industry, such as, how 40 to 50 billion devices connect in upcoming years and how P2P communication is possible between universally distributed IoT nodes. Another issue is determining how to create controls for a large number of decentralized devices. Blockchain is unique in this regard can address all the mentioned issues due to its accumulation of 2160 unique addresses, which offers IoT devices addressability and the blockchain P2P ledger creates a direct connection between each device. Blockchain can directly send or receive data over the network because blockchain provides P2P connectivity [15] for intra device communication. We can say blockchain provides security complexity in IoT applications due to bitcoin, which is the core mechanism of blockchain and has proven over more than ten years that a powerful protection method could present the strongest communication security. There are tremendous advantages to IoT and Blockchain integration, but the combination is not straightforward because of various issues like scalability, consensus, smart contract resource utilization, security & privacy, anonymity, and legal issues [16] are possible in the blockchain-IoT environment. Scalability is an integration issue between IoT and blockchain, where the network size of blockchain increases with an increasing number of connected devices because of its need to store all transactions to validate them. Scalability issues could be a potential bottleneck for the IoT because some current blockchain implementations can only process a few transactions per second [17]. Security is a prime issue when IoT and blockchain integrate, as the severe impact of IoT attacks on the network makes it necessary to secure IoT devices

with blockchain. In the IoT, a large amount of data is generated, processed, and transferred among IoT devices where privacy is a serious concern.

This script is organized as follows: Section- 1 introduces a primer view of IoT with applications, blockchain technology overview, security issues in IoT, and how to address IoT security issues using blockchain and challenges of blockchain with IoT integration. Section 2 discusses background technologies for the medical healthcare system such as IoT and blockchain. Section-3 describes our contribution, workflow, and IoT-blockchain based medical healthcare system. Section 4 discussed experiments and the outcomes of proposed work. Section-5 describes the conclusion of our examined work. Section 6, which is the final section, is a future direction for an innovative researcher.

2. Related Work

Different architectures and algorithms have been proposed to provide authentication for accessing IoT Data. By Alam in[18], mHealth is a blockchain-IoT predicated mobile health fortified a system where it provides a unique identity to every connected contrivance in a network to offer data storage and sharing securely and transparently. In IoT, generally a single password mechanism is utilized for authentication and sanction, but those kinds of mechanisms are vulnerably susceptible to attacks. They have proposed a utilizer and contrivance authentication-predicated technique [19]. Every device in the system is considered a distinct node, and they are interconnected by network technologies. There are two types of users: the first is a privileged user, and the second one is an ordinary user that can read the data from the system. Every device in a system is identified by RFID identification. Continuous medical information and streaming data of the patients are kept in a cloud central repository with their meta-data such as CCR details, which are stored in the gateway server. The requested users interact with the gateway server through their user device ID and access the essential data by providing authentication details. As we know, it may cause a delay in a patient's treatment progress or compromise the

patient's life if there is a security and privacy problem with medical data.

Researchers Jayabalan and her team in [20] have been using the blockchain platform to provide secure management and examination of healthcare data. They have utilized the advertising security and privacy properties in that proposed model, predicated on the innovative cryptographic method and proposed solution, to truncate sundry attacks such as denial of service, modification attacks, or provide more secure transactions for IoT applications over the blockchain network. The Internet of Medical Things (IoMT) requires enormous infrastructure for storage and processing of a substantial volume of medical data. The need for IoMT [21] applications and platforms on a centralized cloud is cooperating with security, so an IoMT system with blockchain data structure provides better security and privacy than a central data storage repository. A small amount of data could be stored in blocks. In the IoMT system, a large amount of data is stored in a decentralized storage platform, and on the blockchain would be hash references for that stored data. A reliable and secure healthcare architecture has been proposed by the authors [22] using the ECC algorithm over the CoAP protocol. The proposed approach provides an effective authentication mechanism with high security.

Griggs[23] proposed blockchain-based smart contracts to enable secure analysis and management of medical sensors in the IoT healthcare system. They have used a private blockchain, based on the ethereum protocol, where the sensors communicate with IoT devices that call smart contracts and write records of all actions on the blockchain. In [24], researchers have mentioned the Oracle [24] is the smart device, which communicates directly to the smart contracts and that could assess the provided data and issue alerts to the patient as well as a healthcare provider. Blockchain provides reliability in multiple sectors such as healthcare, banking, smart homes, information storage management, automation, and security. In keenly intellective healthcare, the prime concern is security and privacy of patient data due to the interoperability of multiple participants in the process. One of the modules deals with the process of fetching and sensing the data from the wearable contrivances and the biosensors that

are either worn by the patients or that are present in the environment in which patients are monitored. In the proposed work, they have used two blockchain networks; specifically, the first is the personal health care blockchain and the second one is the external record management blockchain, [25] where the introduced methodology overcomes the security and privacy issues of the data that is being generated in the conventional healthcare system. IoT and blockchain are the most promising and upcoming technologies. The new abstract model based on blockchain and IoT could offer solutions for numerous problems. Each patient or doctor could access their data via a dashboard connected to the blockchain server using the REST API [26]. The patient's record history could be stored on the distributed storage [27], which can be linked to the blockchain with a hash value. Blockchain technology is an evolving and upcoming technology that enables data sharing in a transactional and decentralized fashion. In the healthcare domain, blockchain can provide a balance between privacy and accessibility of electronic health records.

3. Author's Proposed Contribution

As we know, the Internet of Things (IoT) is the sort of web with diverse appliances or things that are embedded with network connectivity and permit these things to create and interchange data. IoT application disciplines are smart residences, healthcare, smart cities, agribusiness, education, etc., where applications are deployed by various sensors or other IoT equipment. If we consider the healthcare scenario in the IoT, it deals with IoT protocols and interacting technologies. The perception layer is responsible for ordering data and transmitting it to the network layer. Various kinds of detectors are available and estimate significant physical quantities such as human temperature, pulse rate, oxygen level, ECG report, etc., Another function of the perception layer is to enable gadgets to collaborate with other gadgets connected to short-range networks. The network layer is accountable for managing the communication and transmitting the piled data from the perception layer to the storage servers

via gateways. The application layer manages the gathered data and processed information is send to the applications or end users' community.

3.1. Proposed Model

In our proposed model, IoT data will be generated by various types of medical sensors and IoT wearable gadgets, and the patient's entire developed data will be exaggerated and filtered as needed before being stored on blockchain storage (IPFS). In the mentioned framework only authenticated users can access data via a blockchain network. IoT-based healthcare applications correspond with the layered architecture of IoT where the first level, which includes sensors or medical gadgets, functions as units for data procurement such as pulse rate, oximeter, and human body temperature. The second level includes communication and the services that collect data from the first layer and deliver it to the next layer. The third layer is for data processing and accepting results. Medical researchers store the patient's data for clinical as well as research objectives, so the healthcare system should demand more cautiousness about data because it concerns the life of the patient.

The architecture of an IoT-based healthcare system where the first module is a unique identification of the patient will be provided by RFID. There are multiple varieties of medical sensors and wearable devices that collect information from the patient's body to support diagnoses or cure processes. The next module is the health gateway, which acts as a communicator or middle layer between IoT devices and the network, where data will be generated from the medical sensors and transferred to the IoT platform. The collected data will be processed on the IoT node and sent to the blockchain storage IPFS. The third component of the architecture is the application layer, where authenticated users can access the patient's data via the blockchain network with the involvement of the RSA algorithm. In a medical-healthcare system, users are divided into mainly two categories: primary users, including doctors, nurses, and nearby relatives, and secondary as regular users including medical insurance companies, researchers, and drug inventors. Whenever the end-user desires

to access the patient's data, he must endure an authentication procedure.

Internet security matters are extremely serious for healthcare systems that have been overcome using trusted authenticated mechanisms. IoT security is the technology area safeguarding interconnected devices and networks in the internet of things. In the IoT network, data communication can be secured by the cryptographic mechanism by using symmetric or asymmetric encryption algorithms.

3.2. Proposed Work

As we ken the Internet of Things is terrorized by weak connectivity, poor scalability, absent trust, cracked security, and a broken business model. IoT's main issues are node addressing, node identification, device heterogeneity, security, and energy constraint [5]. We are mainly focusing on security in terms of confidentiality, data integrity, and access control mechanisms. IoT data will be engendered from the authentic environment and stored in the blockchain storage IPFS, then only authenticated users will access the data through the blockchain network. The live medical data progenitor-like various kinds of medical sensors or wearable IoT contrivances have engendered a significant amplitude of live medical data for patients. Engendered data from the data progenitor, such as pulse rate of patients, the oxygen level in a patient's body, the temperature of the human body, etc. will be stored in a file. The patient's engendered data is stored utilizing a unique file denominating convention that is provided by the RFID device.

There are various peer-to-peer file systems such as distributed hash tables, block exchanges (bit torrent), version control, self-certified file systems, and IPFS that are used as file storage systems. IPFS is a peer-to-peer distributed file system, where no nodes are confidential. IPFS nodes store IPFS objects in local storage. All IPFS nodes connect and transfer objects among them. Files and other data structures are represented by these objects. The data file for the patients will be generated in the .json file format. In our implementation,

we used the AES-CBC cryptographic algorithm. Before data is transmitted to the blockchain storage, data will be converted into an encrypted format by the AES-CBC cryptographic algorithm. The AES-CBC algorithm is utilised for the encryption and decryption of data files, and it is a round-predicated algorithm. In AES-CBC algorithm, there are three types of keys utilized: 128 bits, 192 bits, and 256 bits. There are four steps to engender a new key where the first step is the sub byte and the remains are rotate word, round constant, and combine the round key. For transformation of plain text to cipher text the sub bytes, shift rows, mix columns, and integrate round key approaches are utilized. This ciphertext will be converted into plain text that is thoroughly inverted process encryption. After encryption of the data file, that file will be sent to the IPFS storage. Here, table 1 shows the terminologies used in implementation.

Table 1: Terminology Table

Notation	Description
K_{sym}	Symmetric Key
P_D	Patient Data File
$(P_D)'$	Encrypted Patient Data File
$(E_{K_{AES}})$	Encryption using Key Value of AES
$IPFS$	InterPlanetary File System
$H(P_D)'$	Hash of Encrypted Data File
$(K_{AES})'$	Encrypted Key value of AES
$(Pu_{Receiver})$	Receiver's Public key
$(Pr_{Receivers})$	Receiver's Private key
$(E_{Pr_{Receiver}})$	Encryption using Receiver's Private key
$(E_{Pu_{Receiver}})$	Encryption using Receiver's Public Key
$(D_{K_{AES}})$	Decrypted Key of AES
$(Hash_{IPFS})$	Hash of stored file that is derived from the IPFS

Algorithm 1 Data Encryption and Decryption using AES-CBC Algorithm

Function Encryption (Filtered_Data_File) ▷ Patient Data File
IF
Data conservation is required **then**
Generate a Symmetric Key,
$(P_D)' \leftarrow Encrypt_{Sym}(P_D, Key, IV)$
$(P_D) \leftarrow Decrypt_Sym((P_D)', InvKey, InvIV)$
Else
Do Nothing
End IF
End Function

In encryption algorithm, we encrypt the data file (P_D) by using the symmetric key (K_{sym}) and initial vector IV. After the use of symmetric key and initial vector (IV) it will be generate ciphertext $(P_D)'$. After data file encryption, that symmetric key (K_{sym}) will be encrypted by receiver's public key($Pu_{Receiver}$) and stored on blockchain platform for further purpose. We will be use the receiver's public key ($Pu_{Receiver}$) for decrypt the symmetric key (K_{sym}) for decryption of original data file (P_D). The Encrypted file$(P_D)'$ with a unique id will be stored in blockchain storage (IPFS). IPFS nodes store the IPFS object in local storage where every IPFS node can communicate with each other and transfer objects among all the IPFS nodes in a network. The acknowledgement of the submitted file will be received from the IPFS in form of a hash value. IPFS storage is withal more public, so confidentiality of data is required. This could be a contravention for certain types of data storage which exposes private data. IPFS can provide a proof of authenticity to the owner of that content. It seems IPFS distributes expeditious and secure fault tolerant file storage for content. As IPFS evolves, it could utilize a privacy layer that can hide personal data that is withal encrypted at rest, so there would be no contravention of exposing anything confidential.

During the entire process, a unique id will be developed from the RFID device for the patient data file (P_D), based on that id, data of the particular patient will be stored in the file. The data architect will develop medical data and send it to the IoT platform, whatever data generated will be stored in a file having the unique id of the patient. Data file $(P_D)'$ that is gathered at the IoT platform will be sent to the IPFS storage.

Algorithm 2 Data Decryption on Receiver side

1: **Input**:Encrypted File $(P_D)', Encrypted(K_{AES})'$
2: **Output** :Decrypted Data File(P_D)
3: **Function** Decryption$((P_D)', (K_{AES})', K_{Sym})$
4: $(P_D) \leftarrow Decryption_{Asym}((K_{AES})', E_{Pr_{Receiver}})$
5: $P_D \leftarrow Decryption_{Sym}((P_D)', K_{Sym})$
6: **End Function**

This file is encrypted using AES symmetric key (K_{sym}) and that key is also encrypted by receiver's public key ($Pu_{Receiver}$). The encrypted symmetric key $(K_{AES})'$ will be stored on blockchain platform. The retrieved file from the IPFS will be in encrypted format so it should require decryption process.

Whenever end users such as doctors, nurses and relatives want to access data file of a particular patient, then they would require to pass an authentication process. Authenticated mechanism of the user succeeds the security mechanism. Here smart contract will find hash value of requested file from the Blockchain and send the response in form of the hash value of that file to the primary validated user. The validated user will be gone to the IPFS storage with the hash value and return with the intended file with the matching of the hash value.

Algorithm 3 Interplanetary File System for Distributed Storage

Function IPFS
Patient's Data File (P_D) send to the IPFS for Data Storage
Input Parameters: (IPFS, $Hash_{IPFS}$) ▷ P_D is the Data File that is Requested by Patient to Store on IPFS
Output : $H(P_D)'$
Step 1 - Data Storage Request
Source Node (SN) sends Request to IPFS
IF
Ethereum address of source node exists in Blockchain
Hash of Data file ($Hash_{IPFS}$) is calculated
IPFS divides the data in small chunks
Step 2 - Data Acquirement Request
SN requests the data from IPFS
IF
($Hash_{IPFS}$) is present on IPFS server
then
IPFS aggregates the data
IPFS sends Protected Data File $(P_D)'$ to the SN
ELSE
Message(The data is not present)
End IF
ELSE
SN is a malicious node
End IF
End Function

4. Implementation

Our Experimentation work has been divided into two-phase, first phase is related to IoT implementation where we have used hardware as an RFID reader, tags, medical sensors and raspberry pi. In the second phase we have used metamask, ethereum platform, IPFS as distributed storage and solidity as a programing language in blockchain side implementation. In our implementation we have integrated two technologies and stated how medical data generated and secured in the IoT environment. Also specified how to store that data at IPFS storage and how to retrieved by the blockchain network. RFID device generated the file having unique id of the patient. The generated data filtered as per requirement and that file is encrypted using the cryptographic method. Raspberry pi can interface with various sensor and RIFD tag using inbuilt python library. We have installed the raspbian operating system using berryboot os that can work as a universal operating system and provide a platform to install any rasbpbian operating system. Also Raspberry pi integrates with RFID RC522 chip using python library such as MFRC522.py which is used to read and write data from/to the RFID tags.

IPFS storage generate the hash value of particular data file of the patient and send back to IoT platform. These generated hash value $H(P_D)'$ is send to the blockchain network for future reference. First, we encrypted that data file on IoT platform using python objcrypt library in the form of AES-CBC encryption method. We stored encrypted content into a file named the same as the ID of the RFID tag then after upload the encrypted file to the IPFS storage. IPFS storage return fixed-length hash value ($Hash_{IPFS}$) of stored file.

4.1. Mathematical Derivation of Implementation

Here Patient data file (P_D) is encrypted using symmetric key (K_{AES}). The encrypted data file $(P_D)'$ send to IPFS storage and as an acknowledgement IPFS return hash value $H(P_D)'$ for stored file. There are two values stored on blockchain, one of them is hash value $H(P_D)'$ of protected file (P_D) and

another that is (K_{AES}). The symmetric key (K_{AES}) is encrypted using public key $(Pu_{Receiver})$ of receiver. Here encrypted symmetric key $(K_{AES})'$ stored on blockchain network. If any one want access data file (P_D), they have to come on blockchain platform and use the $(H(P_D))'$ and (K_{AES}). Using hash value $(H(P_D))'$ of data file, receiver can retrieve the data file in protected mode due to file encryption method. Receiver can decrypt that file using symmetric key (K_{AES}) but that key is also encrypted using receivers public key. The key $(K_{AES})'$ is decrypted using receiver's private key$(Pr_{Receiver})$ and using that key, protected file$(P_D)'$ is decrypted and convert into original data file (P_D). Following steps are indicate life cycle of entire process to sending and receiving data file (P_D) from data origin to data consumer.

Step 1. $(P_D) \xrightarrow{E_{K_{AES}}{}^{(P_D)}} (P_D)'$

Step 2. $(P_D)' \xrightarrow{Send\ to} IPFS$

Step 3. $IPFS \xrightarrow{Send\ Acknowledgement} H(P_D)'$

Step 4. H$(P_D)' \xrightarrow{Store\ on\ the\ Blockchain\ Network} Blockchain$

Step 5. $(K_{AES}) \xrightarrow{E_{Pu_{Receiver}}} (K_{AES})'$

Step 6. $(K_{AES})' \xrightarrow{Encrypted\ Key\ Store\ to} Blockchain$

Step 7. $User_{Receiver} \xrightarrow{Send\ Request\ to\ Blockchain\ Hash} H(P_D)' and\ (K_{AES})'$

Step 8. $(K_{AES})' \xrightarrow{Key\ Decryption\ using\ E_{Pr_{Receiver}}} (K_{AES})$

Step 9. $(P_D)' \xrightarrow{File\ Decryption\ using\ D_{K_{AES}}} (P_D)$

4.2. Model Implementation

In our implementation we have used smart contract which is written in ethereum solidity programming language for IoT based healthcare system for achieving data confidentiality, integrity, and access control mechanism. The fig.

1. shows cryptographic process where we have used blockchain-based authenticated mechanism to access the data file of the patient from the distributed storage. All the medical sensors have been attached to the patient's body and generated data stored in a unique file that is engendered by the RFID device.

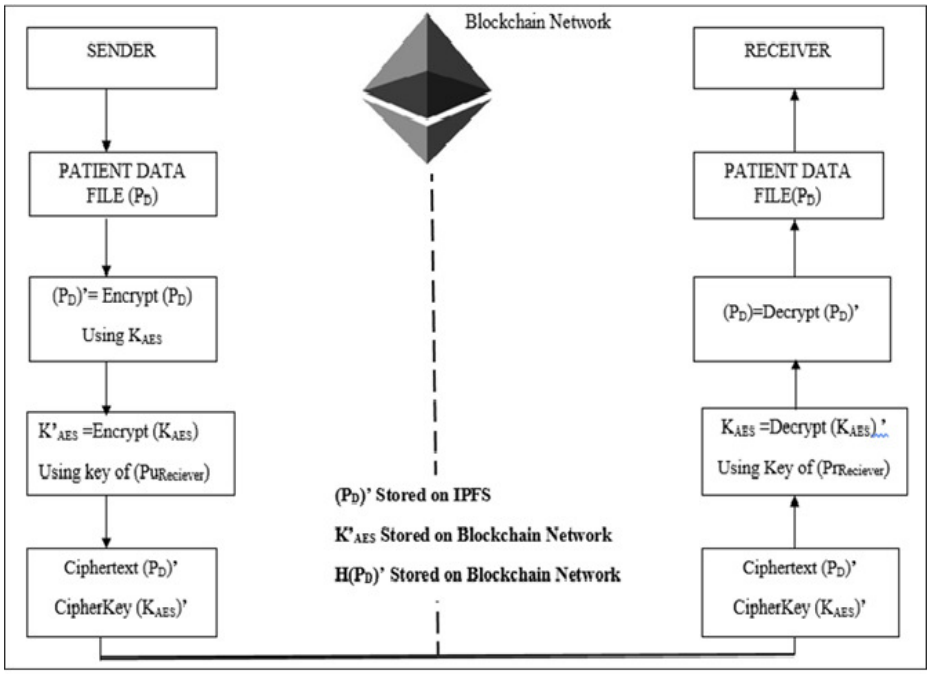

Figure 1: Cryptographic process in proposed model

The data file is encrypted using AES-CBC (Cipher block chaining) cryptographic algorithm and that encrypted file stored on IPFS storage. Due to the blockchain-based mechanism only authenticated users can access the patient's data file from the data storage so prevent such kind of attacks in a network.

4.3. File Sending and Receiving via Blockchain Network

The data file (P_D) of the patient is encrypted using symmetric key and that file converted into protected mode $(P_D)'$. The data file $(P_D)'$ is send to IPFS storage and as an acknowledgement receiver received the one hash value for that stored file. If receivers want to retrieve the data file (P_D) from the IPFS then

they have to used stored hash value of that file.

Also, same symmetric key must use for the decryption process to convert the protected file $(P_D)'$ to original data file (P_D). The blockchain platform is used for sending and receiving data files, where we have invented decentralized file sharing platform. The sender should require the wallet address of the receiver entity and select the data file as per the sending requirement to send the data file to a specific destination address.

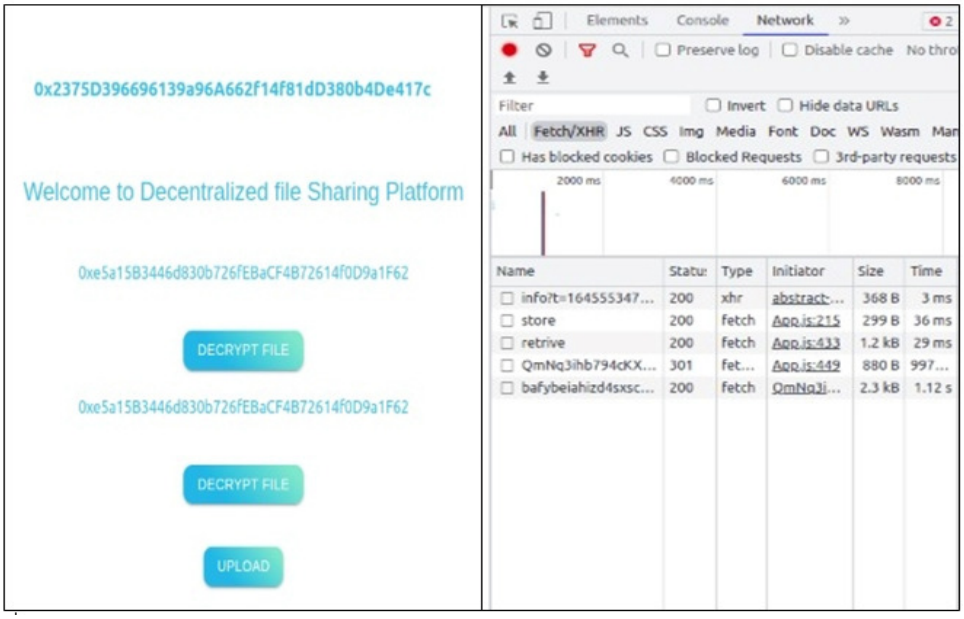

Figure 2: Platform that shows received data file with sender address

The data file is encrypted using an encryption algorithm and that file is stored on the IPFS platform. IPFS storage returns the hash value for that stored file. The retrieved hash value and symmetric key are stored on the blockchain platform. The symmetric key is encrypted by receiver's public key and hash value of protected data file $(P_D)'$ from the IPFS are also stored on blockchain. If receiver want to receive the original data file from the IPFS then he must go on blockchain platform and use the hash value of stored file and private key of receiver for data file decryption as shown in fig.2.

5. Blockchain Network Latency

Blockchain technology presents new tools for authentication and authorization in the digital world that prevents the demand for a kind of unified administrator. As an outcome, it empowers the creation of new digital relationships. Blockchain technology uses a smart contract protocol or rule which is immutable, which means once it is deployed it stays endless. In case a revised version of the present contract is created, due to a production bug, then the manual transfer of stored data is required, which is an awkward process.

In Blockchain, performance measurement is challenging as it is very complex to duplicate a creation-like environment for performance testing. It needs to be tested for network latency based on block size, network type, expected transaction size, how long a query takes to return results with the technical authentication protocol.

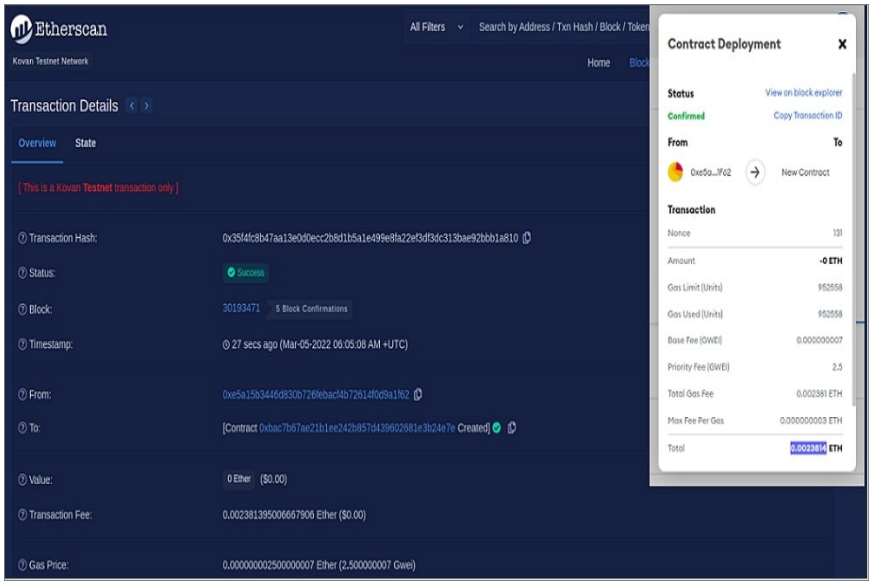

Figure 3: Required gas value for smart contract development using kovan network

We have implemented the transactions on various blockchain test networks and estimated the required gas value for smart contract deployment on the blockchain network. Also, we have measured the required gas amount for up-

loading the hash of the protected data files and encrypted AES key on the blockchain network. We have used Kovan, Rinkeby, BSC, and Matic Blockchain networks for transactions.

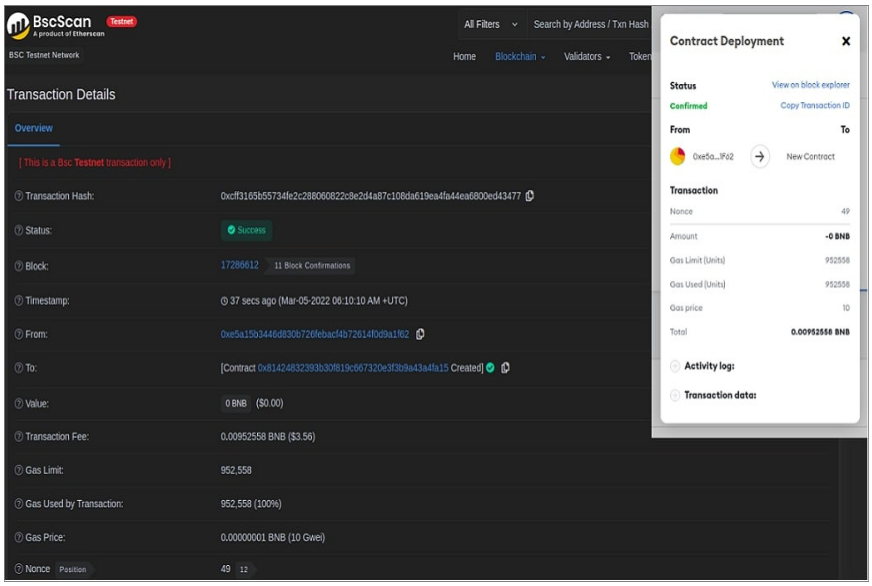

Figure 4: Required gas value for smart contract development using binance smart chain network

480

Here fig. 3,4,5 and 6 indicate the required gas value for smart contract deployment on blockchain network. The Fig.7 shows a comparison among various blockchain networks for the required gas during smart contract deployment on the blockchain network.

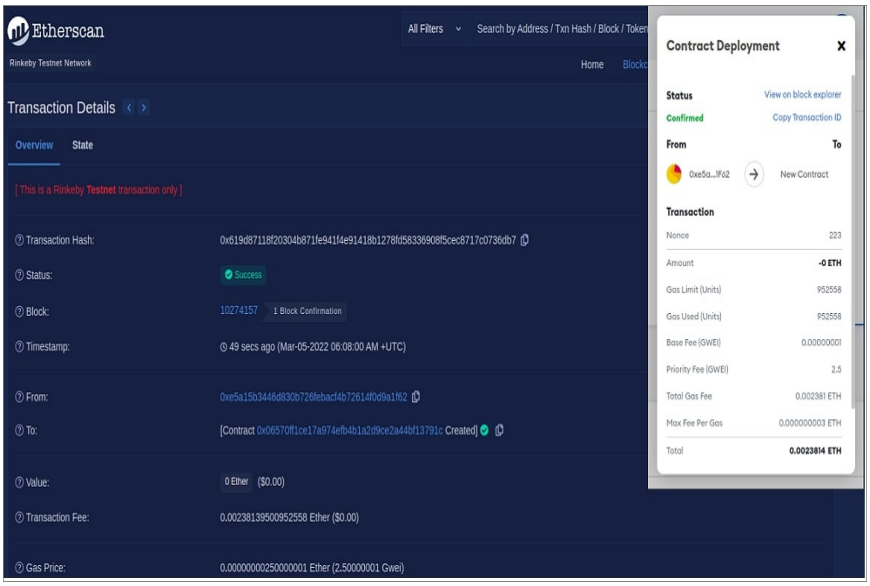

Figure 5: Required gas value for smart contract development using rinkeby network

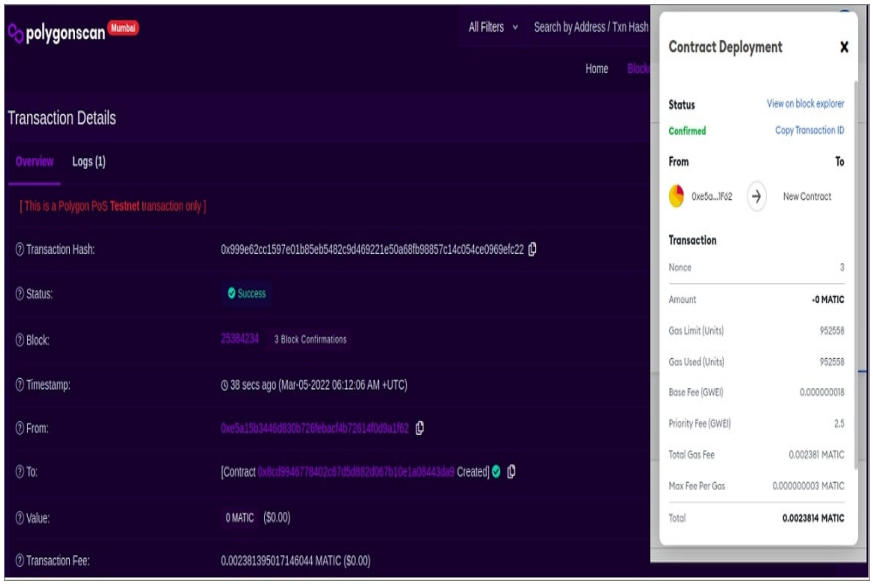

Figure 6: Required gas value for smart contract development using matic network

We conclude and noted, the matic network takes less amount of gas value for smart contract deployment. The kovan and rinkeby test networks on ethereum

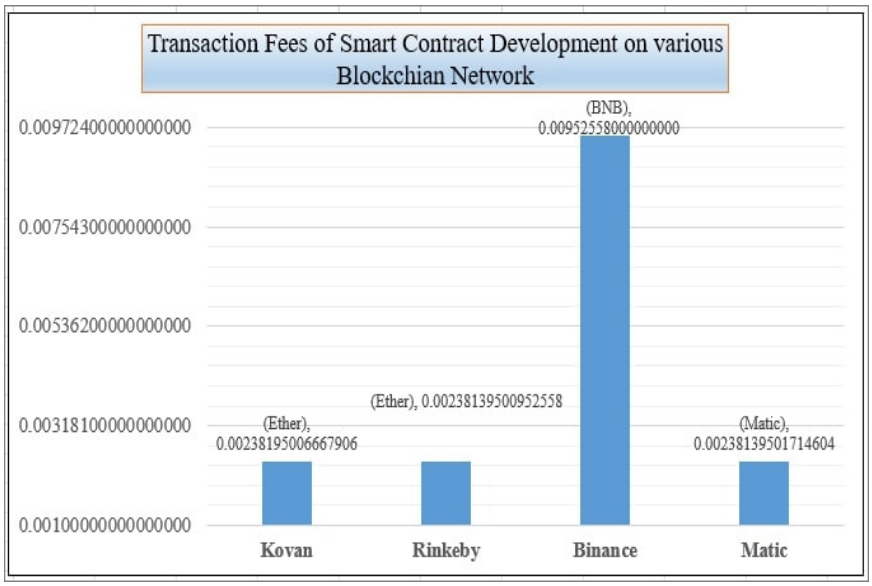

Figure 7: Comparisons of blockchain networks with transaction fees for smart deployment

consumed more gas value than binanace and matic networks. It depends on the network and requirements also, if you pay the lower price, your transaction will take much longer time to execution.

6. Results and Discussion

There are three main security necessities that need to be addressed by any model developer: confidentiality, integrity, and availability. Confidentiality makes sure that only authorized users can access the system. Integrity is responsible for messages sent to the destination without any modification, and availability means data is always available to the users when needed.

6.1. Comparative analysis of proposed framework with existing Blockchain Techniques

It is a comparative analysis of the proposed performance with the existing blockchain techniques in terms of data integrity, access availability, data security, confidentiality, and scalability. The proposed framework is compared against the existing blockchain-based implementations such as [28, 29, 30]. From Table 2, it is obvious that the proposed system satisfies the drawbacks of existing systems in terms of data confidentiality, access control, data integrity, and scalability.

Table 2: Comparative analysis of proposed framework with existing blockchain techniques

Scheme	**Confidentiality**	**Data Integrity**	**Data Availability**	**Data Security**	**Scalability**
Blochi [31]	Yes	Yes	Yes	No	No
Wang & Song[30]	Yes	Yes	Yes	Yes	No
Medchain [29]	Yes	Yes	Yes	Yes	No
Proposed framework	Yes	Yes	Yes	Yes	Yes

Confidentiality: In this implementation, the patient data file will be stored in the IPFS after the cryptographic process. Here, the AES-CBC algorithm is used for file encryption and that symmetric key is encrypted using the receiver's public key.

Data Integrity: Data integrity means stored data is immutable and permanent. It cannot be modified or deleted. In a blockchain, the data is stored as hash values in each block, and each block stores the hash value of the previous block in this blockchain framework. The confidence in this blockchain framework is based on the consensus mechanism, digital signature, and the designed cryptographic algorithm in spite of relying on a third-party provider. All the blocks are associated, any alteration in the original data will affect in a change in its hash value, and it is computationally difficult to tamper with the record, such that the non-tampering of the patient data is also explicitly guaranteed. The original data is stored in IPFS storage after performing a special cryptographic process.

Scalability: The proposed framework preserves most of the security requirements and provides cryptographic storage of data in IPFS thereby resolves the scalability issue in the existing techniques. The scalability of the proposed system has demonstrated and proved that the system is capable of processing large datasets at low latency.

Data Security: Data security is a vital task in our implementation as the patient data is cryptographically stored on IPFS. This blockchain framework stores only a hash of the encrypted data on the blockchain network, and the actual massive data is stored after encryption on the IoT Platform. This system is a patient centric approach that provides authenticated access permissioned by the patient and guarantees the security of the patient data. Also, the smart contracts functionality combines with blockchain solutions to embrace high-level encryption and ensure patient confidentiality in their health care information. In addition, the data stored on IPFS is encrypted using a special AES-CBS cryptographic algorithm to establish vigorous blockchain data security solutions.

We consider the security margin of the model under various threats also.

DoS Attack:

In a DoS attack, attackers try to foil trustworthy users from accessing the services on the network. In such cases, the enemy can launch fraudulent trans-

actions and can expand traffic in the network. However, in our system, random users cannot join the network and access the services without proof of authority. To access the file, users have to get the hash of a particular file and a symmetric key value from the blockchain network. Also, users have to come onto the blockchain network to get the required key value from the blockchain wallet platform. Here, the symmetric key is encrypted using the receiver's public key and that key will be decrypted using the receiver's private key only. None of the users can opt original data file without use of hash value and decrypted key , therefore our system is safe against such kind of attacks.

Mining Attack:

In our system, for accessing data files from the storage network (IPFS), users have to use the hash value of that file. If a user gets the hash value and recovers the patient data file (Pd) from the IPFS storage, even though the user cannot opt the actual file due to the use of the cryptographic algorithm. To avoid the risk of a 51% attack, the blockchain can use the Proof of Stake (PoS) consensus mechanism, which is a more secure agreement than PoW. In our implementation, we have used various blockchain networks and measured the latency of each blockchain network with data transfer processes on IPFS storage. We have tested the binance network also for sending and receiving data files, which works on PoS.

Storage Attack:

As we know, if an intruder attacks the cloud storage, he can modify, remove, or enhance the data in the cloud. In our implemented model, we are using cryptographic methods to encrypt the data file. The encrypted data file is stored on the IPFS distributed platform and it returns an acknowledgement in the form of a hash value for that file. The hash value of the data block is stored in the blockchain, therefore changes in the data file can be easily detected. However, in our model, if any user wants to store or manage data over the IPFS platform, he needs to have a hash of the original hash file with the symmetric key of AES-CBC.

7. Conclusion

Due to issues such as being unattended, heterogeneous, and resource-constrained, security and privacy have become one of the most significant issues in the IoT environment. In this research, we aim to demonstrate the usage of blockchain technology in the healthcare system in diverse situations, from data sharing to the development of clinical research or diagnosis aid in patient health. Patient data is generated by various IoT sensors and secured through cryptographic methods. The encrypted data could be stored on blockchain storage (IPFS). The authors propose a secure model for IoT based healthcare systems that claims to offer reliability and security.

8. Future Work

In our approach, we have used the IoT device Raspberry Pi to generate IoT data and applied a cryptographic algorithm for data encryption on the IoT platform instead of an innovative researcher can use progressive IoT tools to support advanced encryption algorithms. The data that is already encrypted is stored in IPFS blockchain storage, which can be essentially helpful for decentralized file storage for any sort of peer-to-peer transmission. In our proposed work, we have used the ethereum solidity programming language for writing a smart contract. Instead of the ethereum platform, hyperledger fabric, or any other platform, can be used for writing an agreement between entities in the system.

References

[1] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, H. Karimipour, A survey on internet of things security: Requirements, challenges, and solutions, Internet of Things (2019) 100129.

[2] H. Shin, H. K. Lee, H.-Y. Cha, S. W. Heo, H. Kim, Iot security issues and light weight block cipher (2019) 381–384.

[3] A. Čolaković, M. Hadžialić, Internet of things (iot): A review of enabling technologies, challenges, and open research issues, Computer Networks 144 (2018) 17–39.

[4] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: A survey on enabling technologies, protocols, and applications, IEEE communications surveys & tutorials 17 (4) (2015) 2347–2376.

[5] S. L. Keoh, S. S. Kumar, H. Tschofenig, Securing the internet of things: A standardization perspective, IEEE Internet of things Journal 1 (3) (2014) 265–275.

[6] A. Kortebi, O. Bouchet, A. Mengi, H. Lucht, M. Brzozowski, O. Maye, P. Celeda, J. Pazdera, Convergent and reliable hybrid home networks (2016) 112–114.

[7] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, M. Mohammadi, Toward better horizontal integration among iot services, IEEE Communications Magazine 53 (9) (2015) 72–79.

[8] S. Guoqiang, C. Yanming, Z. Chao, Z. Yanxu, Design and implementation of a smart iot gateway (2013) 720–723.

[9] I. Ishaq, J. Hoebeke, I. Moerman, P. Demeester, Internet of things virtual networks: Bringing network virtualization to resource-constrained devices (2012) 293–300.

[10] L. Da Xu, W. He, S. Li, Internet of things in industries: A survey, IEEE Transactions on industrial informatics 10 (4) (2014) 2233–2243.

[11] I. Makhdoom, M. Abolhasan, H. Abbas, W. Ni, Blockchain's adoption in iot: The challenges, and a way forward, Journal of Network and Computer Applications 125 (2019) 251–279.

[12] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: A survey, International Journal of Web and Grid Services 14 (4) (2018) 352–375.

[13] A. Wright, P. De Filippi, Decentralized blockchain technology and the rise of lex cryptographia, Available at SSRN 2580664.

[14] N. M. Kumar, P. K. Mallick, Blockchain technology for security issues and challenges in iot, Procedia Computer Science 132 (2018) 1815–1823.

[15] J. A. D. Donet, C. Pérez-Sola, J. Herrera-Joancomartí, The bitcoin p2p network (2014) 87–102.

[16] M. Maroufi, R. Abdolee, B. M. Tazekand, On the convergence of blockchain and internet of things (iot) technologies, arXiv preprint arXiv:1904.01936.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: Architecture, consensus, and future trends (2017) 557–564.

[18] T. Alam, mhealth communication framework using blockchain and iot technologies, International Journal of Scientific & Technology Research 9 (6).

[19] R. S. Joshitta, A neoteric authentication scheme for iot healthcare system, International Journal of Engineering Sciences & Research Technology 5 (12).

[20] J. Jayabalan, N. Jeyanthi, Scalable blockchain model using off-chain ipfs storage for healthcare data security and privacy, Journal of Parallel and Distributed Computing.

[21] N. Dilawar, M. Rizwan, F. Ahmad, S. Akram, Blockchain: Securing internet of medical things (iomt), Int J Adv Comput Sci Appl 10 (1).

[22] M. A. Azzawi, R. Hassan, K. A. A. Bakar, A review on internet of things (iot) in healthcare, International Journal of Applied Engineering Research 11 (20) (2016) 10216–10221.

[23] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, T. Hayajneh, Healthcare blockchain system using smart contracts for secure automated remote patient monitoring, Journal of medical systems 42 (7) (2018) 130.

[24] D. Rogers, A visit to the oracle: Reviewing the state of construction industry digitalisation, Construction Research and Innovation 10 (1) (2019) 11–14.

[25] S. Chakraborty, S. Aich, H.-C. Kim, A secure healthcare system design framework using blockchain technology (2019) 260–264.

[26] T. Dey, S. Jaiswal, S. Sunderkrishnan, N. Katre, Healthsense: A medical use case of internet of things and blockchain (2017) 486–491.

[27] J. Benet, Ipfs-content addressed, versioned, p2p file system, arXiv preprint arXiv:1407.3561.

[28] B. Shen, J. Guo, Y. Yang, Medchain: Efficient healthcare data sharing via blockchain, Applied sciences 9 (6) (2019) 1207.

[29] H. Wang, Y. Song, Secure cloud-based ehr system using attribute-based cryptosystem and blockchain, Journal of medical systems 42 (8) (2018) 1–9.

[30] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, J. He, Blochie: a blockchain-based platform for healthcare information exchange (2018) 49–56.