International Journal of

INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

IBLOSH: IOT-Enabled Blockchain-Based Data Security Framework for Healthcare System

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

Submitted: 27/04/2023 **Revised**: 28/06/2023 **Accepted**: 05/07/2023

Abstract: As Usage of Internet of Things (IoT) sensors and wearable devices has augmented in recent years in the healthcare domain to accumulate real-time data from patients and pass it over to the medical staff for further analysis, processing, and storage. Centralized computation, processing, and storage are subject to many concerns, including single points of failure, distrust among communicating stakeholders, and data security. Blockchain could be a preeminent alternative to address these issues with its inherent qualities such as decentralization, distributed, immutability, unanimity, security, and transparency. Hence, researchers have started integrating IoT and Blockchain for the medical industry to offer a secure e-healthcare mechanism. In this research, we introduce IBLOSH, an IoT-enabled Blockchain-based data security framework for healthcare systems. Our contributions through this research are (a) Depicting a layered architecture for healthcare systems that makes use of IoT and Blockchain (b) Complete methodological proposal of IBLOSH, including its schematic, detailed flow of communication, and its Blockchain perspective (c) Security verification of the said proposal (d) experimentation setup and (e) Results generated through execution of smart contracts. We employ the latest cryptographical options, such as AES for symmetric key encryption, RSA for public key infrastructure, SHA for integrity verification, and the ECDSA digital signature for authenticity. A broad empirical analysis is conducted to assess the IBLOSH's performance, and the outcomes state that the low latency results in improved efficacy.

Keywords: *Internet of Things, Healthcare, Security, Blockchain*

1. Introduction

The Internet of Things (IoT) is a rapidly growing network of interconnected physical devices, vehicles, appliances, and other objects embedded with sensors, software, and connectivity capabilities. IoT has the potential to change a number of areas of our life, including manufacturing, transportation, healthcare, and home automation [1]. IoT offers more efficiency, convenience, and productivity by seamlessly fusing the physical and digital worlds, but it also raises worries about security, privacy, and ethical ramifications. By gathering and analysing data from linked devices, it enables increased operational efficiency and results in resource allocation and enhanced operations. IoT offers a lot of benefits, but it also has its share of drawbacks. Security and privacy issues are serious concerns since the vulnerabilities in IoT devices can result in unwanted access and data leaks. The wide variety of devices and protocols causes problems with interoperability and standardization, which obstruct effective communication. When dealing with the enormous volumes of data produced by IoT devices, data management, scalability and analytics become challenges. For a responsible and reliable IoT ecosystem, ethical and legal issues relating to data ownership, permission, and surveillance must be resolved [2].

IoT applications in the medical field have the potential to transform how healthcare is delivered and enhance the outcomes of overall healthcare ecosystem. IoT systems and devices, including wearable devices, can be used to improve medical process, gather and analyse real-time data, and monitor patients remotely. IoT can also permit telemedicine, which enables patients to obtain medical consultations remotely, obviating the need for in-person visits and enhancing access to healthcare, particularly in remote regions. However, there are issues and challenges associated with IoT deployment in the medical field. The privacy and security of sensitive patient data are among the main issues [3]. Hence, it is essential to implement strong security measures, data encryption, and stringent access limits. Another exertion is the integration and interoperability of multiple IoT systems and devices. To retain patient confidence and ensure responsible use of IoT in the medical industry, additional legislative and ethical factors, including data ownership, permission, and compliance with privacy legislation, need to be addressed [4].

Blockchain technology, being a decentralized, immutable and secure framework, can be utilized to address IoT-related healthcare concerns as mentioned above. Sensitive healthcare data generated by IoT devices can be stored and managed on a secure and decentralized platform [5]. Patient data may be securely stored, retrieved, and shared among authorized parties while maintaining privacy, integrity, and interoperability by employing Blockchain's immutable and transparent characteristics. Additionally, the tamper-resistant audit trail provided by Blockchain technology

[1] *LDRP-ITR, KSV, Sarva Vidyalaya Kelavani Mandal, Gujarat, Gandhinagar- 382015, India*
[2] *VS-ITR, Sarva Vidyalaya Kelavani Mandal, Kadi, 382715, India*
* *Corresponding Author Email: ochchhavpatel@gmail.com*

improves data provenance, allowing for effective tracking of medical device data, regulatory compliance, and accurate and auditable medical records. In general, Blockchain gives IoT-based healthcare systems improved security, privacy, data management, and interoperability, promoting the development of patient-centric and effective healthcare services [6].

In this article, we proposed a framework, IBLOSH, IoT-enabled Blockchain-based data Security framework for Healthcare system which utilizes the modern cryptography options (for instance, AES [7], SHA[7] and RSA [8]) to ensure confidentiality, integrity and authorised communication. These cryptographic algorithms improve the security of healthcare data kept on a Blockchain when they are linked with an Ethereum-based Blockchain platform. The Blockchain's immutable and transparent record-keeping feature protects the accuracy of medical information and the auditability of data access and exchange. Together, AES, SHA, RSA, and Blockchain-based Ethereum technology build trust model and enable cutting-edge applications IoT-based healthcare ecosystems.

The overall structure of this research is as under. We start with the introduction that provides an overview of the IoT, Blockchain, and issues in the healthcare system as the context for the study. The background section delves into the existing literature, highlighting the relevant work and previous research related to IoT-based healthcare, cryptographic algorithms AES and RSA, and Ethereum-based Blockchain platforms. The subsequent section, our contribution, outlines the specific contributions of the paper, emphasizing how the integration of cryptographic options and the Ethereum Blockchain platform in IoT-based healthcare. The experimentation and results section details the methodology employed, including the experimental setup and data collection process. It presents the findings and outcomes of our study, showcasing the effectiveness and impact of the proposed approach. Moving forward, the conclusion and future work section summarizes the key findings, discusses the implications of the research, and identifies potential areas for further investigation and improvement. This section provides insights into the future direction of the research and possible avenues for extending the work.

2. Background

The importance of cyber-security intelligence in the healthcare sector and the use of artificial intelligence (AI) to strengthen security measures are highlighted by Chakraborty, C., et al. (2023) [9]. The suggested system uses a combination of centralized and federated transfer learning mechanisms to detect cyber-attacks targeted exclusively at the healthcare industry. To effectively communicate data between the cloud and healthcare industries, the Edge of Things (EoT) platform is created. It introduces the centralized with Multi-Source Transfer Learning (CMTL) algorithm to identify and categorize diverse threats, including information gathering, malware assaults, infiltration attacks, DDoS attacks, and man-in-the-middle attacks. The usefulness of the suggested system in strengthening cybersecurity in the healthcare sector is highlighted by these findings. The approach proposed by Sharma, P., et al. (2023) [10], maintains security by enforcing regulations through smart contracts within the Blockchain network. Using the Etherscan tool, the researchers ran a number of experimental tests to evaluate the performance of the suggested architecture. Operation cost, latency, and processing time are the main metrics employed in these tests. In terms of latency, throughput, and response time, the effectiveness of the suggested system is also contrasted with that of existing methods. Researchers point out the security flaws in traditional healthcare systems and provide an innovative solution in the form of a distributed, privacy-preserving application built on Blockchain technology. Alruwaill, M. N., et al. (2023) [11], proposed a Blockchain-based smart healthcare system that makes use of IoMT devices for ongoing patient monitoring. In addition to providing additional processing capabilities, the edge device plays a critical role in hashing and encrypting data. The technology protects data privacy within the Blockchain by using a symmetric key, enabling patients to safely communicate their data using smart contracts while prohibiting illegal access by doctors. A verification node and the Blockchain are in charge of signing and certifying patient data in the healthcare provider system using an asymmetric key. To assure the veracity and integrity of the data source, location-based authentication is also handled. The approach proposed by Durga, R., et al. in (2022) [12], consists of two parts: a federated learning model that reduces computational complexity and Blockchain technology that permits data sharing while maintaining anonymity. FLED-Block (Federated Learning Ensembled Deep Five Learning Blockchain Model), the proposed framework, collects data from various medical healthcare centres, develops the model using a hybrid capsule learning network, and makes accurate predictions while protecting data privacy and sharing among authorized individuals. The suggested architecture solves the issues of complexity, data privacy, and cross-border collaboration by fusing Blockchain with federated learning. A 'BIoMT' (Blockchain-based Internet-of-Medical-Things) architecture is proposed by researcher Bhattacharjya, A., and his team in 2022 [13]. It is analysed and discussed how Blockchain technology benefits IoMT (Internet of Medical Things) infrastructures. The difficulties with the current cloud-based IoMT solutions can be solved using the BIoMT architecture that has been outlined. The issue of the primary server failing or other single-point failures may be addressed using a decentralized BIoMT architecture. Additionally, the disclosed PoW consensus process ups the security level of patients' clinical records and enables tamper-free open access to all nodes in the BIoMT network. These features make the BIoMT architecture tamper-proof. Jiang et al. (2018) [14] developed the "BlocHIE" system, a Blockchain-based network for exchanging medical data. They looked into the various specifications for exchanging health data from various sources. In order to meet the criteria of both authenticity and privacy, they created two loosely coupled Blockchains to manage different types of healthcare data and merged off-chain storage and on-chain verification. They integrate off-chain storage and on-chain verification methods into the EMR-Chain to adequately preserve privacy and authentic ability. They also recommended two transaction packaging approaches to increase system efficiency and client fairness. K. Christodoulou et al. (2020) [15] suggested the COVID-19 Pandemics system, which is based on a peer-to-peer network powered by the distributed Interplanetary File System paired with on-chain tagging, in order to offer a secure manner of sharing medical data. Using an open-source variation of the Pretty Good Privacy (PGP) encryption technique, medical data is safely protected. The proposed design employs asymmetric cryptography to encrypt medical data using the recipient's public key. Prior to the data being re-pushed for storage on a peer-to-peer file storage system controlled by an IPFS cluster, encryption takes place at the client side. Public-key cryptography is used by the system to handle each participant's identity information. Even though identity is pseudonymous to safeguard privacy, the smart contract can link users' social security numbers or any other regularly used form of identification with their Ethereum public addresses. The secp256k1 Elliptic Curve Digital Signature Algorithm is used to create an Ethereum public/private key pair. On the Ethereum Blockchain, this pair serves as the authentication technique. According to Wu et al. (2023) [16], the majority of medical data is transmitted via potentially susceptible channels without encryption, placing patients in danger of intrusion and manipulation. Another issue is the ineffective archival and storage of massive amounts of unprocessed medical data on the cloud. This contribution provides a multi-access edge computing and block-chain based approach for sharing medical resources in the near future. Device-to-device communication is used to facilitate efficient and dependable information sharing between various medical devices. Before being processed by the MEC, medical data is encrypted and decoded using ShangMi cryptographic techniques. Blockchain is used to protect data and stop modifications. The method's effectiveness is shown by the simulation results, and its security is established by the security analysis. According to Almaiah et al. (2021) [17], the goal of this study is to present a novel system that uses heuristic, signature, and voting detection techniques to ascertain the most efficient preventative measures that can be taken to identify harmful and security risks associated with Blockchain technology. To identify malicious sensor nodes in this system, the cluster core node combines the capabilities of Blockchain with those of the three detection systems. Additionally, CN uses crucial parameters such as sensor node-hash value, node signature, and voting percentage to identify rogue nodes in WSNs. The overall result statistic from the simulation of the suggested method revealed that 94.9% of malicious messages were successfully recognized and identified.

With the background understanding of the issue with reference to recent work by contemporary researchers, we not illustrate the layered architecture of IoT and Blockchain which includes a variety of physical devices like wearables, actuators, and sensors, as shown in figure 1. These devices play a crucial role in collecting and transmitting real-time healthcare data. Additionally, communication protocols like Zigbee, Wi-Fi, cellular, and Bluetooth are employed to enable seamless connectivity and data exchange between the devices and the healthcare system. Low-power wireless communication is provided by Zigbee, high-speed data transfer is guaranteed by Wi-Fi, extensive coverage is provided by cellular networks, and short-range wireless communications are made possible by Bluetooth. The architecture facilitates the smooth gathering and transfer of healthcare data by combining these physical devices and communication protocols, setting the groundwork for succeeding layers in the IoT-based healthcare system. In order to provide safe and effective communication, the network layer plays a critical role by implementing numerous protocols. Peer-to-peer (P2P) network technology is used at this layer to allow consumers, IoT devices, and medical equipment to communicate directly with one another. A broad address space is ensured

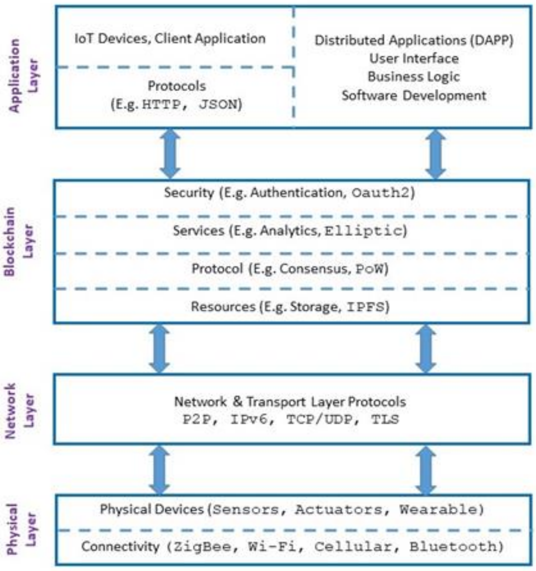

Application Layer
IoT Devices, Client Application
Protocols (E.g. HTTP, JSON)
Distributed Applications (DAPP)
User Interface
Business Logic
Software Development
Blockchain Layer
Security (E.g. Authentication, Oauth2)
Services (E.g. Analytics, Elliptic)
Protocol (E.g. Consensus, PoW)
Resources (E.g. Storage, IPFS)
Network Layer
Network & Transport Layer Protocols
P2P, IPv6, TCP/UDP, TLS
Physical Layer
Physical Devices (Sensors, Actuators, Wearable)
Connectivity (ZigBee, Wi-Fi, Cellular, Bluetooth)

Fig 1. The Layered Architecture of Healthcare with IoT using Blockchain by the use of IPv6, allowing for the rapid growth of linked devices. TCP/UDP protocol implementation also permits dependable data transmission and network node-to-node communication. With the help of the Transport Layer Security (TLS) protocol, which encrypts data as it is transmitted and provides authentication and integrity, the security of healthcare data is improved. By including these protocols, the architecture's network layer makes it possible for connections to be seamless and safe, supporting the trustworthy sharing of medical data.

In the architecture of Healthcare with IoT using Blockchain, the Blockchain layer plays a critical role in ensuring security, providing essential services, implementing protocols, and managing resources. This layer takes advantage of Blockchain technology's built-in advantages to establish trust and immutability in healthcare data. The Blockchain layer protects the security of sensitive information by using cryptographic methods to guard against unwanted access or manipulation. It also makes it possible to use decentralized applications (DApps) and smart contracts to deliver a range of healthcare services, including secure data exchange, interoperability, and patient consent management. The application layer serves as the interface between users and the underlying system. Web-based or mobile user interfaces enable a smooth user experience and simple navigation. The layer also includes the business logic, which includes the guidelines, processes, and algorithms that direct how the healthcare system functions. Additionally, the client apps and the core system communicate and exchange data using the HTTP and JSON protocols, allowing for seamless transmission of data. The components of the application layer function as a unit to deliver a user-centric, effective, and cutting-edge healthcare experience.

3. Our Contribution

We summarize our contribution in figure 2 which shows the schematic of our proposal IBLOSH: IoT-enabled Blockchain-based data Security framework for healthcare system. The system makes use of various IoT sensors to gather data, which is then saved on the IPFS (InterPlanetary File System) platform. The acquired data files are encrypted using the AES symmetric method, which has strong encryption capabilities, to assure data security. For the purpose of retrieval, the IPFS platform creates a hash value for each file that is saved. These hash values are then kept on the IPFS network, guaranteeing the immutability and integrity of the data.

Any authorized user, including a pharmacy, insurance company, physician, or nurse, can access the recorded data in this suggested system by submitting a registration request through the Blockchain network. A safe and open platform for user registration, identity verification, and data access is Blockchain technology. The solution makes use of Blockchain's decentralized structure to guarantee data privacy, authenticity, and auditability. The Blockchain verifies and stores each user's identity and access permissions, allowing for restricted and allowed data retrieval.

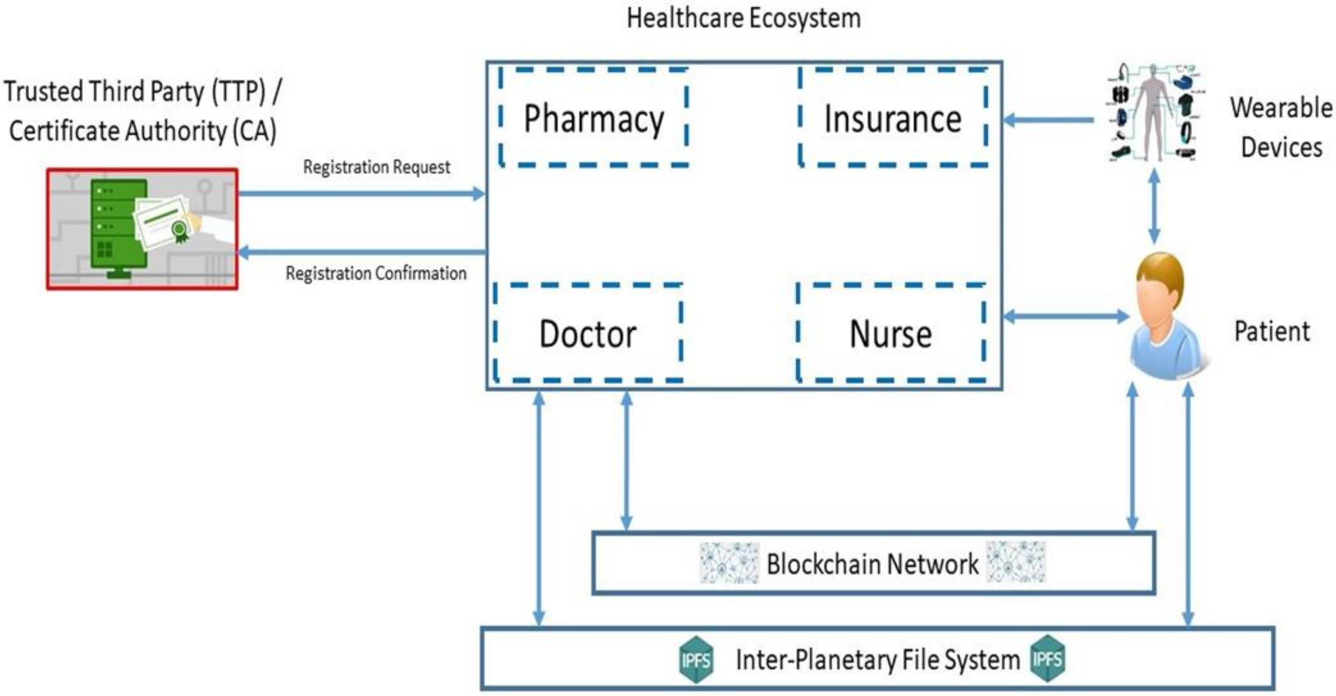


Fig 2. IBLOSH: Schematic Depiction

Overall, this study endeavour intends to develop a strong and secure healthcare system where data can be effectively collected, saved, and accessed by authorized parties while ensuring data privacy and integrity. It does this by combining IoT, IPFS, encryption methods, and Blockchain.

Figure 3 depicts a sequence diagram illustrating the proposed work. In this process, every entity is required to register with the system. Once registered, the Certificate Authority sends an acknowledgement ($ACK_{Positive}$) to the registered person in the form of PID, $P_{RPatient}$, and $P_{UPatient}$. The patient's generated data is stored in a patient data file called DataPatient. To enhance security, the DataPatient file is converted into a protected data file called $Data'_{Patient}$ using the AES (Advanced Encryption Standard) key K. This symmetric key K is encrypted using the receiver's public key. According to the scenario mentioned in the sequence diagram, if Doctor 1 wants to access the data file, they must send a request to the IPFS (Interplanetary File System) platform through Blockchain. The symmetric key K is encrypted using Doctor 1's public key ($P_{UPatient}$). The recipient can then retrieve the data file from IPFS using the hash value H. However, the retrieved data file is in protected mode ($Data'_{Patient}$). To convert the protected data file ($Data'_{Patient}$) back into its original form, the recipient can use the decrypted key K along with their private key ($P_{RDoctor1}$).

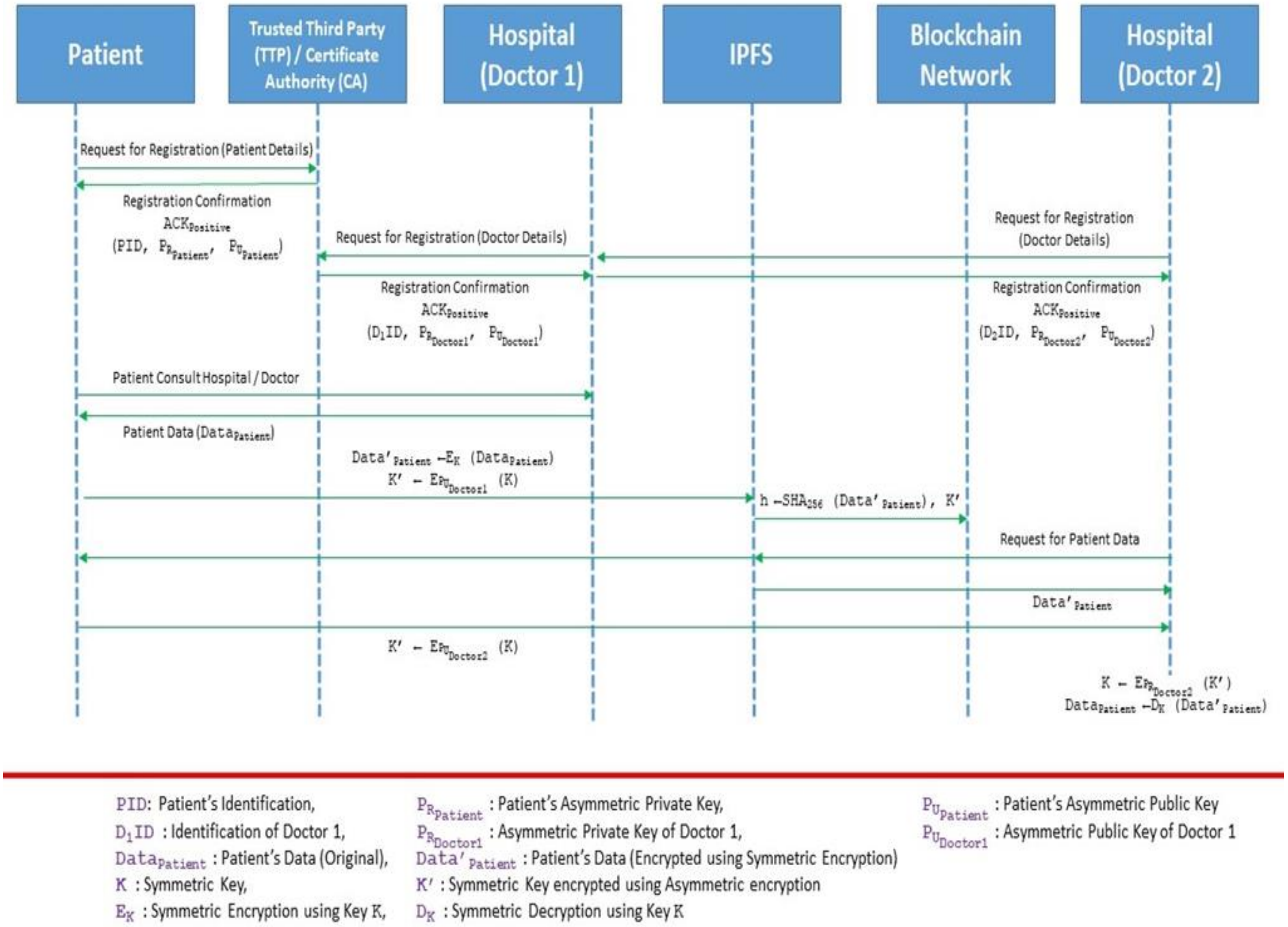
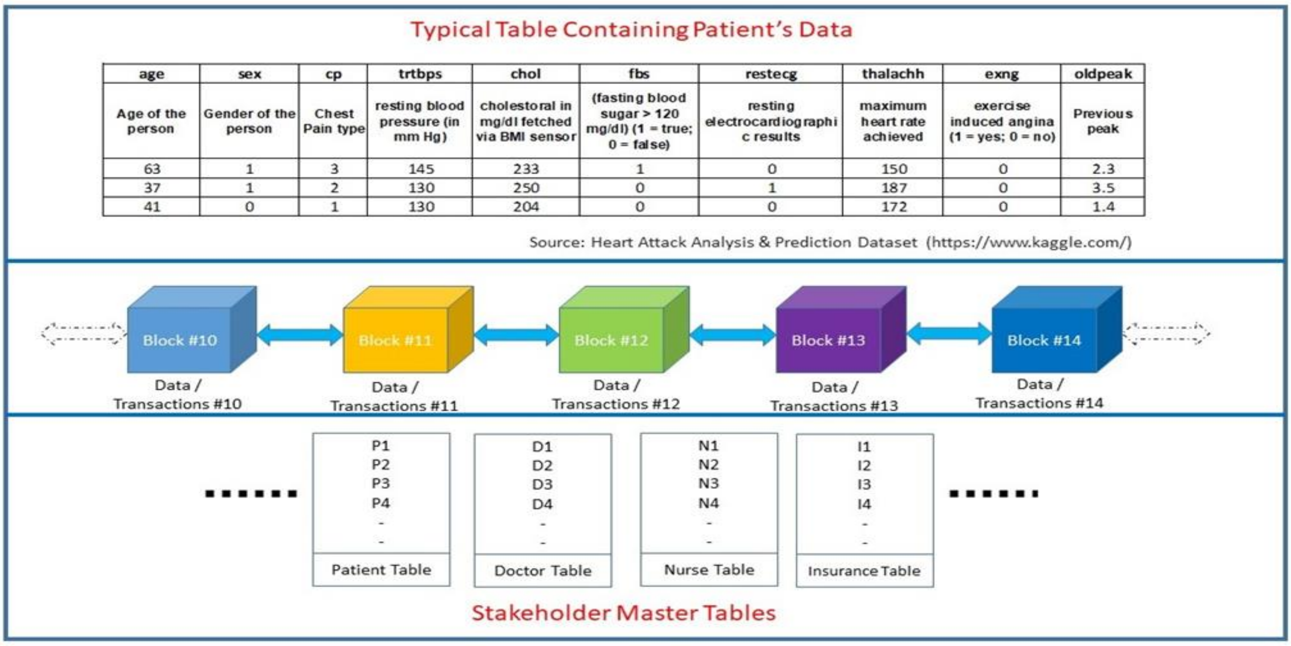

Patient
Trusted Third Party (TTP) / Certificate Authority (CA)
Hospital (Doctor 1)
IPFS
Blockchain Network
Hospital (Doctor 2)
Request for Registration (Patient Details)
Registration Confirmation
ACKPositive
(PID, PRPatient, PUPatient)
Request for Registration (Doctor Details)
Registration Confirmation
ACKPositive
(D1ID, PRDoctor1, PUDoctor1)
Request for Registration (Doctor Details)
Registration Confirmation
ACKPositive
(D2ID, PRDoctor2, PUDoctor2)
Patient Consult Hospital / Doctor
Patient Data (DataPatient)
Data′Patient ←EK (DataPatient)
K′ ← EPUDoctor1 (K)
h ←SHA256 (Data′Patient), K′
Request for Patient Data
Data′Patient
K′ ← EPUDoctor2 (K)
K ← EPRDoctor2 (K′)
DataPatient ←DK (Data′Patient)
PID: Patient's Identification,
D1ID : Identification of Doctor 1,
DataPatient : Patient's Data (Original),
K : Symmetric Key,
EK : Symmetric Encryption using Key K,
PRPatient : Patient's Asymmetric Private Key,
PRDoctor1 : Asymmetric Private Key of Doctor 1,
Data′Patient : Patient's Data (Encrypted using Symmetric Encryption)
K′ : Symmetric Key encrypted using Asymmetric encryption
DK : Symmetric Decryption using Key K
PUPatient : Patient's Asymmetric Public Key
PUDoctor1 : Asymmetric Public Key of Doctor 1

Fig 3. IBLOSH: Sequence Diagram



Typical Table Containing Patient's Data

age	sex	cp	trtbps	chol	fbs	restecg	thalachh	exng	oldpeak
Age of the person	Gender of the person	Chest Pain type	resting blood pressure (in mm Hg)	cholestoral in mg/dl fetched via BMI sensor	(fasting blood sugar > 120 mg/dl) (1 = true; 0 = false)	resting electrocardiographic results	maximum heart rate achieved	exercise induced angina (1 = yes; 0 = no)	Previous peak
63	1	3	145	233	1	0	150	0	2.3
37	1	2	130	250	0	1	187	0	3.5
41	0	1	130	204	0	0	172	0	1.4

Source: Heart Attack Analysis & Prediction Dataset (https://www.kaggle.com/)

Fig 4: IBLOSH: Typical Blockchain

4. Experimentation and Result

In our research, we concentrated on utilizing Blockchain technology to create IoT-based healthcare. Let's examine the elements that are utilized and how they link to implementation.

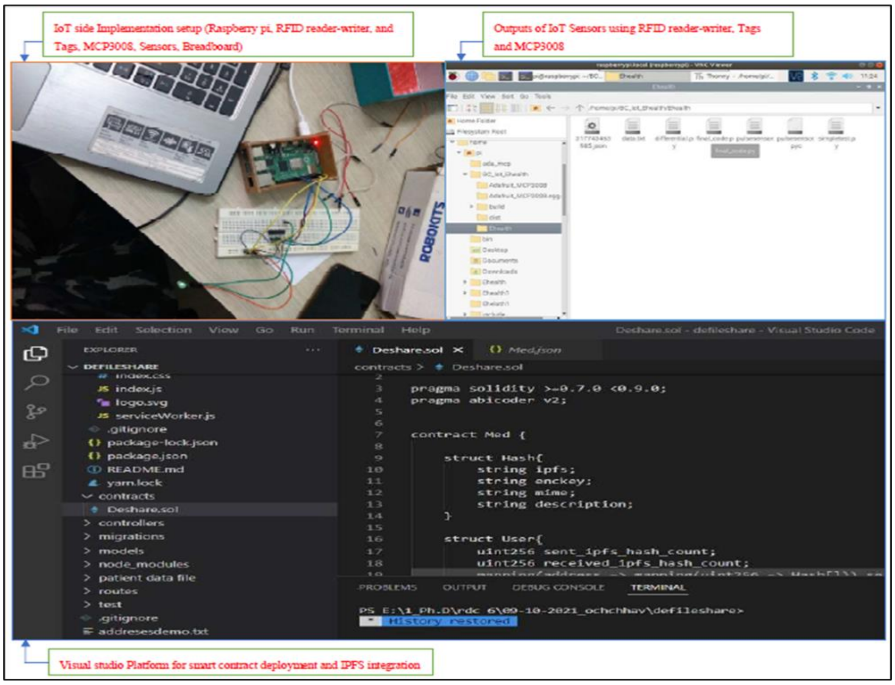
- Raspberry Pi: Single-board computers like the Raspberry Pi are compact, affordable, and programmable. As an Internet of Things (IoT) device, we used it to connect and manage other devices in the healthcare system by acting as a central hub or gateway. The Blockchain platform and the RFID reader-writer MCP3008 most likely communicated via the Raspberry Pi [19].

- RFID: Radio Frequency Identification (RFID) technology enables wireless identification and tracking of objects using tags and readers. In order to provide seamless tracking and monitoring inside the IoT ecosystem, these tags could be connected to a variety of healthcare-related things, such as medical devices, sensors, or patient wristbands [20].

- MCP3008: An analog-to-digital converter (ADC) chip is the MCP3008. It enables the transformation physiological sensor data (such as temperature and heart rate), which are analog signals, into digital form for the Raspberry Pi's processing and analysis [21].

- Ethereum Blockchain Platform: we chose the Ethereum Blockchain platform as the foundation for our work. Ethereum offers a safe, decentralized platform for storing data and performing smart contracts. Self-executing contracts, or "smart contracts," have rules and conditions that are already established. Using Ethereum's capabilities, researchers can build a trustworthy, open, and unchangeable healthcare system.

- Smart Contract: A smart contract is a piece of software that uses established criteria to automate and enforce the performance of predefined activities. Smart contracts are used in this implementation to control and verify interactions inside the healthcare system. These smart contracts may have made it easier to carry out procedures like sharing patient data, controlling access, or conducting financial transactions by ensuring that everything is done in accordance with predetermined norms and without the involvement of middlemen.



IoT side Implementation setup (Raspberry pi, RFID reader-writer, and Tags, MCP3008, Sensors, Breadboard)

Outputs of IoT Sensors using RFID reader-writer, Tags and MCP3008

```
pragma solidity >=0.7.0 <0.9.0;
pragma abicoder v2;


contract Med {

    struct Hash{
        string ipfs;
        string enckey;
        string mime;
        string description;
    }

    struct User{
        uint256 sent_ipfs_hash_count;
        uint256 received_ipfs_hash_count;
```

```
PS E:\1_Ph.D\rdc 6\09-10-2021_ochchhav\defileshare>
 * History restored
```

Visual studio Platform for smart contract deployment and IPFS integration

Fig 5. Setup of Implementation Work

Figure 5 demonstrates how the implemented work is concentrated on combining IoT devices, such as Raspberry Pi and RFID technologies, with Blockchain technology (particularly, the Ethereum platform), in order to create a secure and efficient healthcare system. When these technologies are used together, healthcare applications can benefit from better data management, interoperability, and trustworthiness. In our experimentation, we have measured the average download and upload times for various data files on the Firebase and IPFS platforms. Figure 6 shows experiments conducted to measure the average download time for different data file formats (json, jpeg, and pdf) on two platforms: Firebase and IPFS (InterPlanetary File System). Here are the specific details and findings for each file format.

1. JSON file (164 KB):

- Firebase download time: 3.26 seconds
- IPFS download time: 1.33 seconds

2. JSON file (1 MB):

- Firebase download time: 19.83 seconds
- IPFS download time: 8.58 seconds

3. JPEG file (130 KB):

- Firebase download time: 1.22 seconds
- IPFS download time: 0.78 seconds

4. PDF file (1.33 MB):

- Firebase download time: 23.21 seconds
- IPFS download time: 10.33 seconds

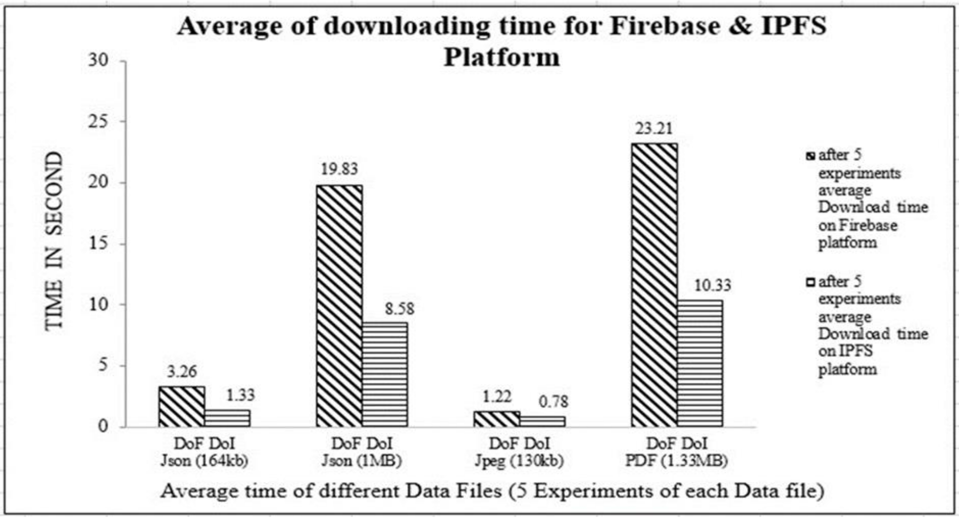


Fig 6. Average Download time of different data files on the Firebase and IPFS platforms

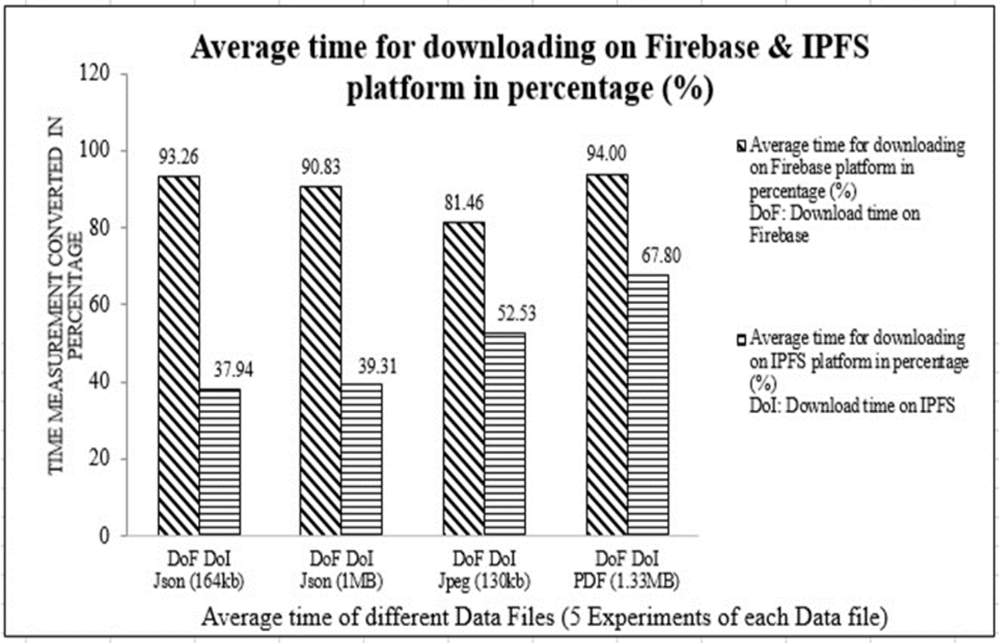


Fig 7. Average Download time of different data files on the Firebase and IPFS platforms in form of percentage (%)

Firebase is a mobile and web application development platform provided by Google. It offers a wide range of services, including cloud storage. Variables including network latency, server load, and the platform's particular configuration may have an impact on Firebase's measurements of download times. Contrarily, IPFS is a distributed file system that employs a decentralized method for storing and retrieving files. It attempts to offer a more reliable and effective method of hosting and delivering material. IPFS uses a peer-to-peer network where files are split among several nodes, potentially enabling faster content retrieval.

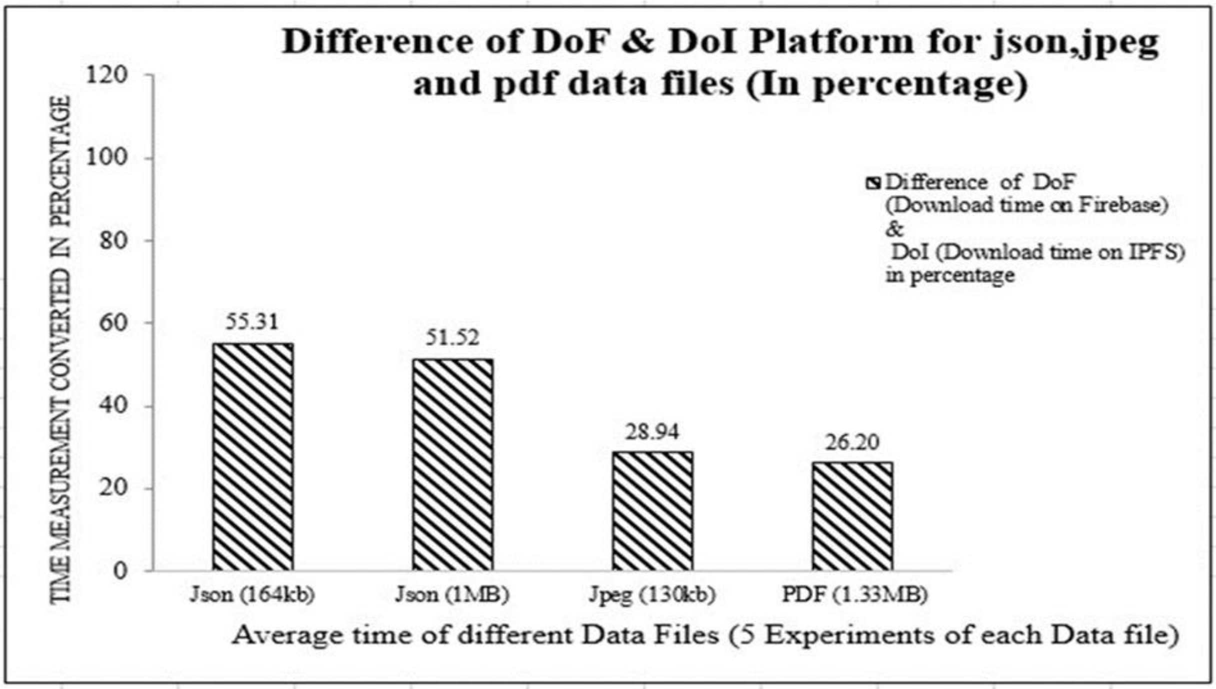
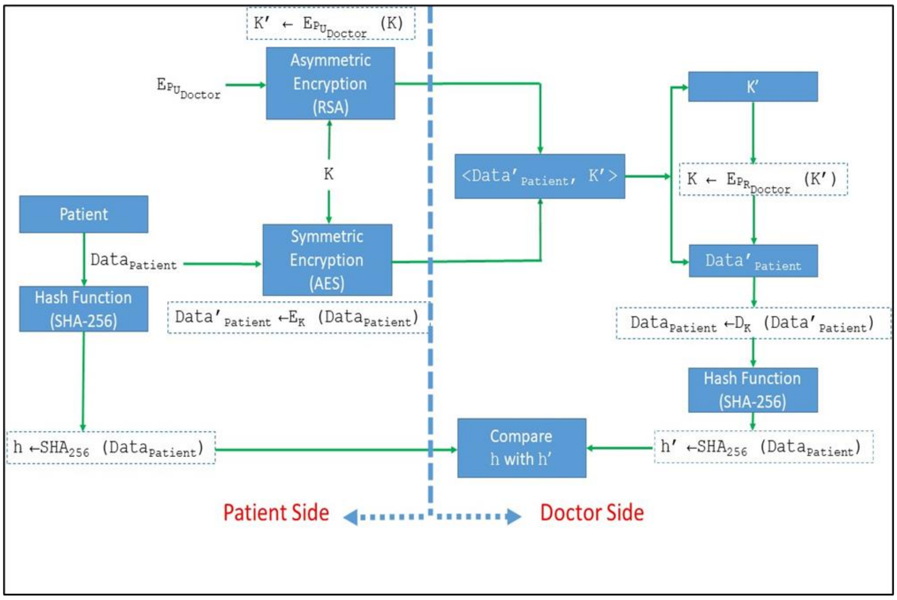


Fig 8. Difference in Average Download time between Firebase and IPFS platforms in percentage (%)



$K' \leftarrow E_{PU_{Doctor}}(K)$
$E_{PU_{Doctor}}$
Asymmetric Encryption (RSA)
K
Patient
$Data_{Patient}$
Symmetric Encryption (AES)
Hash Function (SHA-256)
$Data'_{Patient} \leftarrow E_K(Data_{Patient})$
$h \leftarrow SHA_{256}(Data_{Patient})$
$<Data'_{Patient}, K'>$
K'
$K \leftarrow E_{PR_{Doctor}}(K')$
$Data'_{Patient}$
$Data_{Patient} \leftarrow D_K(Data'_{Patient})$
Hash Function (SHA-256)
$h' \leftarrow SHA_{256}(Data_{Patient})$
Compare h with h'
Patient Side
Doctor Side

Fig 9. IBLOSH: Security Verification

In Figure 7, the average download time of JSON, JPEG, and PDF data files on the Firebase and IPFS platforms is represented as a percentage. This representation allows for a clearer understanding of the performance differences between the two platforms for each file format. Figure 8, on the other hand, illustrates the difference in average download time between the Firebase and IPFS platforms, also represented as a percentage. It provides a comparative view of the performance gap between the two platforms for each file format. These percentage differences indicate the relative performance advantage of IPFS over Firebase in terms of download time for the respective file formats. The higher the percentage value, the greater the improvement in download time when using IPFS compared to Firebase. In conclusion, based on the experiments conducted, it can be inferred that IPFS generally outperforms Firebase in terms of download time for JSON, JPEG, and PDF files of various sizes. The percentage differences in download time highlight the relative efficiency of IPFS in comparison to Firebase, with IPFS consistently showing superior performance across the evaluated file formats.

Security is the primary concern for the data of IoT. We provide the proof of concept for security verification as shown in Figure 9. The objective is to ensure data confidentiality, integrity, and secure access to patient data in a healthcare system. Here is how we achieve our objectives:

Confidentiality of Patient Data:

- The original patient data file ($Data_{Patient}$) is encrypted using symmetric encryption (AES) to achieve data confidentiality.
- The encryption process generates a new encrypted data file called ($Data'_{Patient}$).
- Encryption Key (K): A symmetric encryption key (K) is used to encrypt the patient data file.
- $Data'_{Patient} \leftarrow E_K (Data_{Patient})$

Hiding the Symmetric Key:

- To protect the symmetric encryption key (K), it is encrypted using the recipient's (doctor's) public key ($E_{PU\mathbf{Doctor}}$).
- The encrypted symmetric key is denoted as K', and it ensures that only the recipient can decrypt and access the data.
- $K' \leftarrow E_{PU\mathbf{Doctor}} (K)$

Integrity of Data:

- The protected data file ($Data'_{Patient}$) is sent to the InterPlanetary File System (IPFS) for storage and distribution.
- IPFS returns a hash value (h) that represents the stored file, ensuring data integrity.
- $h \leftarrow SHA_{256} (Data_{Patient})$

Secure Storage:

- Both the hash value (h) and the encrypted symmetric key (K') are stored on the Blockchain platform.
- This ensures that the information about the data file and the encrypted key are securely recorded and tamper-proof.
- $< Data'_{Patient,} K'>$

Secure Retrieval:

- When the recipient (doctor) wants to retrieve the data file from IPFS, they need to go through the Blockchain network.

- The recipient uses their private key ($E_{PR\mathbf{Doctor}}$) to decrypt the encrypted symmetric key (K') retrieved from the Blockchain.
- The decrypted symmetric key (K) is obtained.

Data Decryption:

- The protected data file ($\text{Data'}_{\text{Patient}}$) is converted back into its original form ($\text{Data}_{\text{Patient}}$) using the decrypted symmetric key (K).
- Decryption is performed using the decryption function (D_K).
- $K' \leftarrow E_{PU\mathbf{Doctor}}(K)$

Integrity Verification:

- To ensure data integrity, the original hash value (h) of the data file ($\text{Data}_{\text{Patient}}$) is compared with a newly computed hash value (h').
- Both hash values are generated using the SHA256 hashing algorithm.
- If the hash values match, it indicates that the data file has not been tampered with and remains intact.
- $h \leftarrow SHA_{256}(\text{Data}_{\text{Patient}}) = h' \leftarrow SHA_{256}(\text{Data}_{\text{Patient}})$

This process ensures that the confidentiality and integrity of patient data is protected, and only authorized entity can access the same. The Blockchain platform maintains the necessary information for secure access and verifies the integrity of the data. The recipient can retrieve and decrypt the data using their private key, and data integrity is ensured through hash value comparisons.

5. Conclusion and Future Work

The primary concern for this paper is to introduce IBLOSH, a Blockchain-based data security framework that utilizes IoT-enabled data for a Healthcare system. With modern cryptosystem options such as AES, RSA, SHA, and ECDSA, IBLOSH provides a secure and efficient alternative for various stakeholders in the medical industry to interact among themselves in a transparent way. We provide a detailed architecture of IBLOSH with a full schematic, complete data flow, security verification, along with practical setup. In the future, we will incorporate more stakeholders in the healthcare ecosystem, such as pathological laboratories, insurance agencies, and pharmaceutical industry.

Author contributions

Ochchhav Patel: Role of Primary Author (a) Feasibility Study of Healthcare (b) Requirement Analysis from Health Stakeholder (c) Requirement Gathering from Medical Officers (d) Planning (e) Designing (f) Implementation/Coding [Python / Ethereum] (g) Testing/Validation (h) Setting up

Dr. Hiren Patel: Guidance about research problem, Documentations, Deadline Maintenance.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Peter, O., Pradhan, A., & Mbohwa, C. (2023). Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies. *Procedia Computer Science*, *217*, 856-865.

[2] Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things, 19, 100564.

[3] Wazid, M., & Gope, P. (2022). BACKM-EHA: A novel Blockchain-enabled security solution for IoMT-based e-healthcare applications. ACM Transactions on Internet Technology (TOIT).

[4] Samuel, O., Omojo, A. B., Mohsin, S. M., Tiwari, P., Gupta, D., & Band, S. S. (2022). An anonymous IoT-based E-health monitoring system using Blockchain technology. IEEE Systems Journal.

[5] Wenhua, Z., Qamar, F., Abdali, T. A. N., Hassan, R., Jafri, S. T. A., & Nguyen, Q. N. (2023). Blockchain technology: security issues, healthcare applications, challenges and future trends. Electronics, 12(3), 546.

[6] Taloba, A. I., Elhadad, A., Rayan, A., Abd El-Aziz, R. M., Salem, M., Alzahrani, A. A., ... & Park, C. (2023). A Blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. Alexandria Engineering Journal, 65, 263-274.

[7] Subashini, A., & Raju, P. K. (2023). Hybrid AES model with elliptic curve and ID based key generation for IOT in telemedicine. Measurement: Sensors, 100824.

[8] Alsuqaih, H. N., Hamdan, W., Elmessiry, H., & Abulkasim, H. (2023). An efficient privacy-preserving control mechanism based on Blockchain for E-health applications. Alexandria Engineering Journal, 73, 159-172.

[9] Chakraborty, C., Nagarajan, S. M., Devarajan, G. G., Ramana, T. V., & Mohanty, R. (2023). Intelligent AI-based Healthcare Cyber Security System using Multi-Source Transfer Learning Method. ACM Transactions on Sensor Networks.

[10] Sharma, P., Namasudra, S., Chilamkurti, N., Kim, B. G., & Gonzalez Crespo, R. (2023). Blockchain-based privacy preservation for IoT-enabled healthcare system. ACM Transactions on Sensor Networks, 19(3), 1-17.

[11] Alruwaill, M. N., Mohanty, S. P., & Kougianos, E. (2023, June). hChain: Blockchain Based Healthcare Data Sharing with Enhanced Security and Privacy Location-Based-Authentication. In Proceedings of the Great Lakes Symposium on VLSI 2023 (pp. 97-102).

[12] Durga, R., & Poovammal, E. (2022). Fled-block: Federated learning ensembled deep learning Blockchain

model for covid-19 prediction. Frontiers in Public Health, 10, 892499.

[13] Bhattacharjya, A., Kozdrój, K., Bazydło, G., & Wisniewski, R. (2022). Trusted and secure Blockchain-based architecture for Internet-of-Medical-Things. Electronics, 11(16), 2560.

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

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

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

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

[18] Heart attack analysis & prediction dataset. (n.d.). Kaggle: Your Machine Learning and Data Science Community. https://www.kaggle.com/datasets/rashikrahmanpritom/heart-attack-analysis-prediction-dataset.

[19] Sengan, S., Khalaf, O. I., Priyadarsini, S., Sharma, D. K., Amarendra, K., & Hamad, A. A. (2022). Smart healthcare security device on medical IoT using raspberry pi. International Journal of Reliable and Quality E-Healthcare (IJRQEH), 11(3), 1-11.

[20] S. Jangirala, A. K. Das, and A. V. Vasilakos, “Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment,” IEEE Transactions on Industrial Informatics, pp. 1–1, 2019.

[21] Radwan, A., & Abdelhady, A. (2022). IOT Virtual Doctor Robot. MSA.

[22] Mr. Rahul Sharma. (2018). Monitoring of Drainage System in Urban Using Device Free Localization Neural Networks and Cloud computing. International Journal of New Practices in Management and Engineering, 7(04), 08 - 14. https://doi.org/10.17762/ijnpme.v7i04.69

[23] Gangula, R. ., Vutukuru, M. M. ., & Kumar M., R. . (2023). Network Intrusion Detection Method Using Stacked BILSTM Elastic Regression Classifier with Aquila Optimizer Algorithm for Internet of Things (IoT). International Journal on Recent and Innovation Trends in Computing and Communication, 11(2s), 118–131. https://doi.org/10.17762/ijritcc.v11i2s.6035

[24] Sherje, N. P., Agrawal, S. A., Umbarkar, A. M., Kharche, P. P., & Dhabliya, D. (2021). Machinability study and optimization of CNC drilling process parameters for HSLA steel with coated and uncoated drill bit. Materials Today: Proceedings doi:10.1016/j.matpr.2020.12.1070