Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-19630-w

Blockchain enabled MediVault for healthcare system

Brijesh Kumar Chaurasia[1]

Received: 16 February 2024 / Revised: 2 May 2024 / Accepted: 7 June 2024

Abstract
The management of healthcare data has significantly benefited from the use of cloud-assisted MediVault for healthcare systems, which can offer patients efficient and convenient digital storage services for storing their medical records. Nevertheless, there are security risks associated with the current digital healthcare data, as malicious parties may work with cloud storage service providers to alter patient records or to directly disclose health record content to other adversaries for monetary advantage. In this paper, a blockchain-enabled MediVault for healthcare systems is proposed not only to provide safe storage of healthcare data in digital form but also secure access for authenticated entities such as patients, doctors, and pharmacists. In this MediVault, we introduced NFT generation and storage over the cloud using Interplanetary File System (IPFS) and FireBase as per user adaptability, Ehtereum Blockchain for immutability, and encryption and decryption using asymmetric keys for confidentiality. The empirical results and the performance evaluation demonstrate that the proposed MediVault is secure, simple, and efficient with a limited computation overhead.

Keywords Non Fungible Token (NFT) · IPFS · Vault · Ehtereum Blockchain · Internet of Medical Things (IoMT) · Healthcare System

1 Introduction

The patient's medical health record is a crucial component of the medical system, transitioning from traditional paper-based records to contemporary electronic medical health records [1]. Administrative issues and privacy concerns come with the conventional medical record storage model. Accessibility suffers by the loss or damage of paper-based records. Security vulnerabilities in electronic systems make unauthorized access feasible [2]. One point of failure that is susceptible to hacking and system failures is posed by centralized databases. Furthermore, patients' control over their medical information is constrained. In order to ensure data integrity and privacy and to give patients control over their health information, Blockchain technology provides a decentralized, transparent, safe,

✉ Brijesh Kumar Chaurasia
brijesh.chaurasia@psit.ac.in

[1] Department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur, India

and secure solution [3]. Blockchain is a decentralized database that operates with verified nodes and securely stores immutable blocks of data to enable transactions with no interference. Data preservation is given priority, especially in the healthcare industry, where there is a great deal of information sharing. Blockchain-enabled MediVault and non-fungible tokens (NFT) [4] over cloud [5] are essential for tackling issues in healthcare like claim authentication and public health management due to their versatility for creating decentralized and trust-less transaction environments [6].

Blockchain technology used in the healthcare industry gives patients authority over data sharing, addressing ownership problems that are prevalent among current practices involving third-party data storage. It enables the secure integration, modification, and sharing of health data. This data can be retrieved by authorized authorities using consensus procedures. The reason behind the technology's delayed completion of expected results is a combination of organizational, social, security, and governance obstacles. The general public, which includes healthcare providers and patients, has difficulty comprehending Blockchain's technological features, data processing benefits, and workings [7]. It will take time to overcome these obstacles because the complexities of government regulations and legal enforcement are unclear. Current research endeavors to accelerate the adoption of Blockchain technology by mitigating these obstacles and bolstering operational expansion across diverse industries [8]. To address the issues in the healthcare industry, secure and fast medical record systems are needed. In this paper, Blockchain-enabled MediVault for healthcare systems is proposed to achieve secure and fast access over the cloud. Figure 1 shows the block diagram of the proposed MediVault. It is a combination of all current technologies, such as NFT, vault, and Blockchain. Moreover, from a security perspective, an adaptive authentication technique is also proposed. The patient can access it securely from the cloud at any time, and doctors may also access it using patient credentials or self-security credentials.

1.1 Motivation

In the healthcare system, there are heterogeneous formats and types of data. Patient healthcare records, such as X-ray images, a doctor's prescription, a blood test, and ECG/EEG

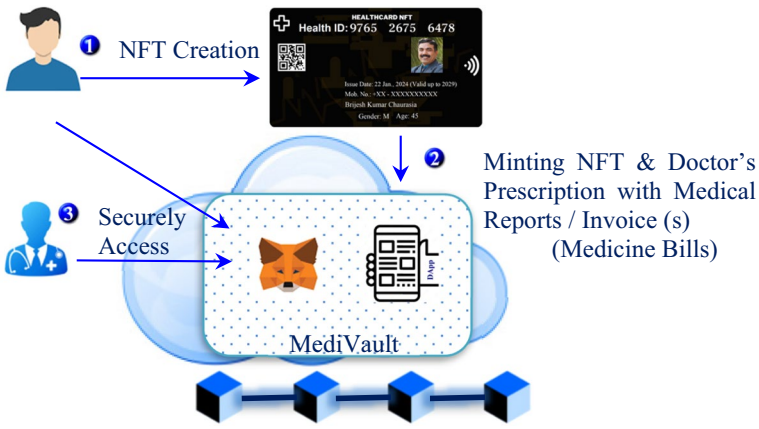

Fig. 1 The block diagram of the proposed MediVault over the cloud

reports (as shown in Fig. 2), are big issues to safely store and securely access. Every year, not only is patient medical data increasing, but it is also increasing digital data nationwide, increasing 20–40 percent [9]. Data is also growing due to the internet of medical things (IoMT) [10]. The main motivation is to address the store with such a massive amount of healthcare data and also ensure its security in terms of confidentiality and integrity while maintaining high availability among patients, doctors, and other collaborators.

1.2 Contributions

The following succinctly describes the main contributions of this paper:

- NFT generation and minting in Blockchain are presented.
- The Blockchain enabled MediVault for healthcare systems is proposed.
- User adaptive authentication and encryption/decryption for security issues are analysed.
- MediVault storage over the cloud using IPFS and Firebase is also discussed.
- Finally, the comparative analysis of the proposed system is also examined.

1.3 Structure of the paper

The rest of this paper is organized as follows. Section 2 introduces literature review of the Blockchain enabled healthcare system. Problem formulation is presented in Sect. 3. The proposed scheme and performance analysis are explained in Sects. 4 and 5, respectively. We make conclusion and future scope in Sect. 6.

2 Literature review

The Blockchain-enabled vault has not been the subject of many relevant previous studies; yet, Blockchain, NFT, and cryptography techniques are employed to overcome security issues. The patient's medical health record (PMHR) using Blockchain and cryptography is discussed in [1]. In this work, Blockchain provides immutability and a proxy re-encryption scheme to ensure confidentiality for health records. The cryptography approach for

Fig. 2 Health record data [9]

healthcare data, especially the authentication of entities, is presented in [10]. In this work, the IoMT that is based on zero-knowledge proofs (ZKP) is discussed. In addition, hashing functions with different data lengths over IoT devices are also analyzed. Blockchain-based privacy preserving e-health system to ensure the security and confidentiality of the patients' health record over cloud is illustrated in [11] and [5]. Both the work is combination of cryptographic approaches and Blockchain technology to provide not only immutability but also provide other security issues as key management, and confidentiality (Fig. 3).

Hyperledger Blockchain-based cloud storage approaches are discussed in [12]. The paper presents a Blockchain-based system for private data management, focusing on healthcare research. Users store their data securely off-chain, while consent details are recorded on a permissioned Blockchain. Admins control data sharing, ensuring transparency and compliance with privacy regulations. The proposed solution uses Hyperledger Fabric, and its performance is evaluated using Hyperledger Calliper, demonstrating its potential in domains where managing user data privacy is critical.

VAULT is a permissioned Blockchain protocol facilitating secure collaboration [13]. It uses quorum-based consensus for fairness. Users can add members, create projects, and manage files with content stored on IPFS and references on the Blockchain. Experimental evaluations confirm linear scalability and efficiency. Future work aims to enhance consensus fairness through measures like grey-listing, ensuring improved selection probabilities for nodes in quorums. One potential drawback of the VAULT protocol is its reliance on a quorum-based consensus system. While designed for fairness, it may face challenges in situations where nodes exhibit biased behavior or if there are malicious actors attempting to manipulate the consensus process.

A distributed ledger is essentially a shared database that is dispersed over several nodes, such as computers or institutions [14]. The distributed ledger in VAULT, which they've dubbed "Fragchain," functions decentralized, protecting data. With capabilities like hashing and encryption, it securely saves data using strong cryptographic algorithms. Fragchain acts as an unchangeable log in VAULT, recording each file upload since "time zero" and logging any further actions taken, such as sharing or deleting. It serves as the foundation for ensuring traceability and transparency in file activity.

In Blockchain technology, the NFT is widely utilized to offer digital assets or certificates integrity, trustability, safe access, and speed [4, 15]. Using Blockchain technology, the NFT functions as a certificate of ownership and proof of ownership for digital assets. NFTs are digital currencies that, because of their unique characteristics, cannot be traded or exchanged in the same way as Bitcoin or Ethereum. NFTs cannot be exchanged or replaced, in contrast to cryptocurrencies and actual currency, which are both fungible [6]. Although the idea of NFT is predicated on the characteristics of scarcity and uniqueness,

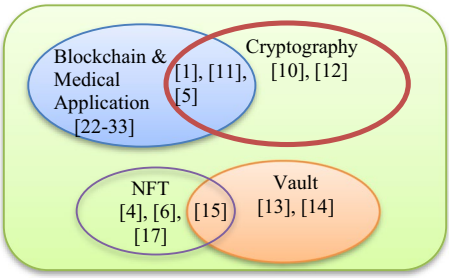

Fig. 3 Classification of cutting-edge techniques

it is also frequently applied to inanimate objects. The use of NFTs for healthcare services is demonstrated in [4, 15]. They use NFTs on the private Blockchain infrastructure known as Hyperledger Fabric to ensure that patient records belong to their proper owners, monitor all related activities, and offer accessibility, safety, and speedy access [16]. Health-related data like as scans, test results, prescriptions, ultrasound reports, and more are represented by NFTs, digital assets stored using DLT with fixed, unchanging addresses. The evidence pertaining to crimes, property, or forgeries is delicate and simple to tamper with; NFT usage is presented in [6, 17]. Medical related document directly cannot enter into the Blockchain, document may minted either NFT or prescription or outcome of any disease computed from ML or DL approach [22–33]. In [22–24], a lightweight security mechanism for ensuring patient privacy, authentication, and confidentiality using watermarking and the ChaCha20 algorithm are discussed in detail. In the healthcare system, there are heterogeneous formats and types of data. Patient healthcare records, such as X-ray images, a doctor's prescription, a blood test, and ECG/EEG reports, are processed by deep learning and machine learning [25–29]. The outcome of processed healthcare records may be entered into the blockchain or stored in the cloud using the IPFS protocol. IoMT anomaly detection, wireless body area network data sensed by sensors and communicated with lightweight IoT protocols, and blockchain-enabled trust evaluation for networks are studied in [30–33]. Several studies are available on healthcare data privacy, preservation, and security; however, a complete solution for urban and rural areas is needed.

3 Problem formulation

In the healthcare system, there is a lot of paper and file work. The health reports, such as X-rays, CT scans, EGC/EEG, and the doctor's prescription handling, are not only a big problem for villagers but also a major challenge for citizens. Time and expenses in terms of money are also a major issue if the patient needs to show the reports to the doctor, who is in another city or country. Doctors can better understand the history of all diagnoses and medications by digitizing all previous patient health records. This will facilitate a speedy and accurate diagnosis by the physician, and the digital form of the health record will ensure security. By digital record keeping, access to medical records is available for patients for a lifetime. Time can be completed in a couple of seconds if the patient needs to show the reports to the doctor, who is in another city or country. People can get accurate medical care faster, even in rural areas without modern hospitals. In spite of the many pros of digitizing health records, there are some cons. Storage, safety, and secure accessibility are the major problems. As a result, securely storing health records and providing doctors and patients with secure access to the system are needed. In this work, MediValut is proposed using Blockchain, NFT, and cryptography approaches over cloud storage to address all available issues.

4 Proposed methodology

In this section, a Blockchain-enabled MediVault for healthcare system is proposed. The proposed scheme aims to ensure the privacy-preserved authentication of patients, the integrity of the healthcare data of patients, and the use of an adaptive encryption approach to preserve the confidentiality of patients' healthcare records.

4.1 System architecture

Figure 4 illustrates a proposed blockchain-enabled MediVault system architecture, which comprises five main steps: NFT generation request, health card storage and access, registration for a doctor's appointment (visit), minting of NFT and medical documents by blockchain, and secure access. The detailed description is as follows:

Step 1: NFT Generation Request.
In this proposed system, the patient is an actor and sends a request for any government agencies or competent authority to generate the healthcare NFT as an Ayushman Card [4, 18]. The NFT will be stored in the cloud and processed using IPFS [19] or FireBase [20].
Step 2: Health Card storage and Access.
The proposed system recommends the FireBase service to store NFT in the cloud; however, it is a centralized service. The patient may also store NFT in the cloud using IPFS for distributed service; however, results also prove that it takes much more access time in comparison to FireBase.
Step 3: Registration for a Doctor's appointment (Visit).
In this step, patient may directly visit a doctor or hospital. In hospital case after registration, as per the deceases and availability of doctors or patient recommendation appointment will be fixed.
Step 4: Minting NFT and Medical Documents by Blockchain.
After the doctor's visit, prescriptions from doctors, NFT, medical bills, and medicine invoice(s) will be minted by Ehtereum Blockchain. We have also analyzed other Blockchain to prove the efficacy of our proposed MediVault.
Step 5: Secure Access.
We have also proposed user adaptive encryption and decryption approaches for the confidentiality of data. At anytime and anywhere, patients can access secure data, which also resolves the physical handling and damaging of medical records.

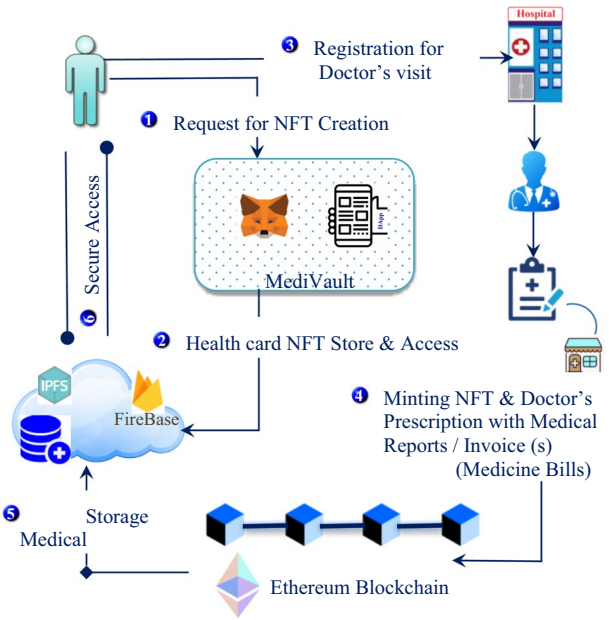

Fig. 4 An architecture overview of Blockchain enabled MediVault

4.2 Working process

In order to implement the workflows outlined in our proposed MediVault, illustrated in Fig. 5, Here, patient, hospital, doctor, and chemist are actors. Firstly, patients will register after completing the NFT process; if NFT is not available, patients may generate NFT through the hospital as well. Secondly, on the basis of disease and availability of doctors, the hospital will allocate the doctors, or the patient may directly select the doctor for consultation. After receiving a doctor's advice or prescription with medical reports (if available), the patient may take medicine from a chemist. Lastly, all records will be stored in MediVault using Ehtereum Blockchain transactions. NFT and records may be stored with encryption by the public key of the patient to provide confidentiality; however, this process is user-adaptive as per the requirements of the patient.

The encryption process is presented in Fig. 6. In this process, the master key, along with other security credentials such as public and private keys, will be generated by competent authorities. The patient will remain safe with his or her security credentials. The process will also provide authentication for patients and other actors on the basis of Adhar Card credentials. In the proposed MediVault, we have taken three-factor authentication for patients, doctors, and pharmacists. However, for security constraints and simplicity, we have considered the OTP process for registered mobile Adhar cards only. After the authentication process, a patient may take keys and, as per the requirement, may generate other pairs of keys from trusted, competent authorities. The key generation process is optional, and the authentication process uses a cryptography approach, so the authentication process is user-adaptive.

Figure 7 shows the authentication process for the patient and his or her medical records. The process will be repeated on every access record from MediVault, whether it is NFT-only or all records. The authentication process depends on three factors. Here, we have used all the credentials of the Adhar Card. For simplicity, any rural and urban patient will show Adhar card entries, and on the basis of these credentials, the authentication process will be completed, followed by NFT creation. Rural people will also use the proposed MediVault, so key generation processes are user-adaptive. We used asymmetric ECC-based key generation, encryption, and

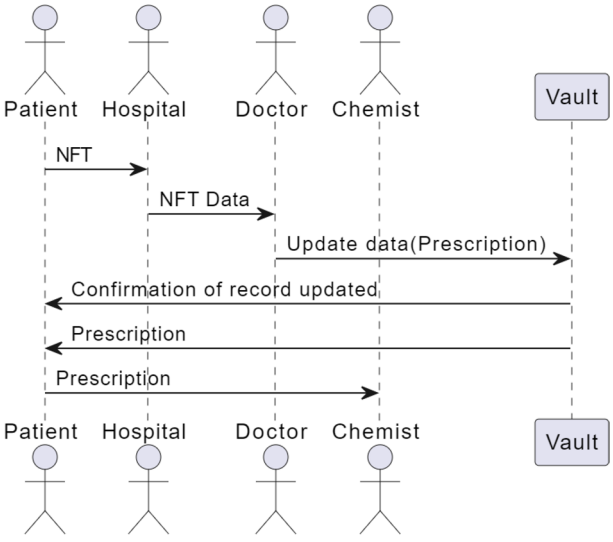

Fig. 5 Working process of Blockchain enabled MediVault

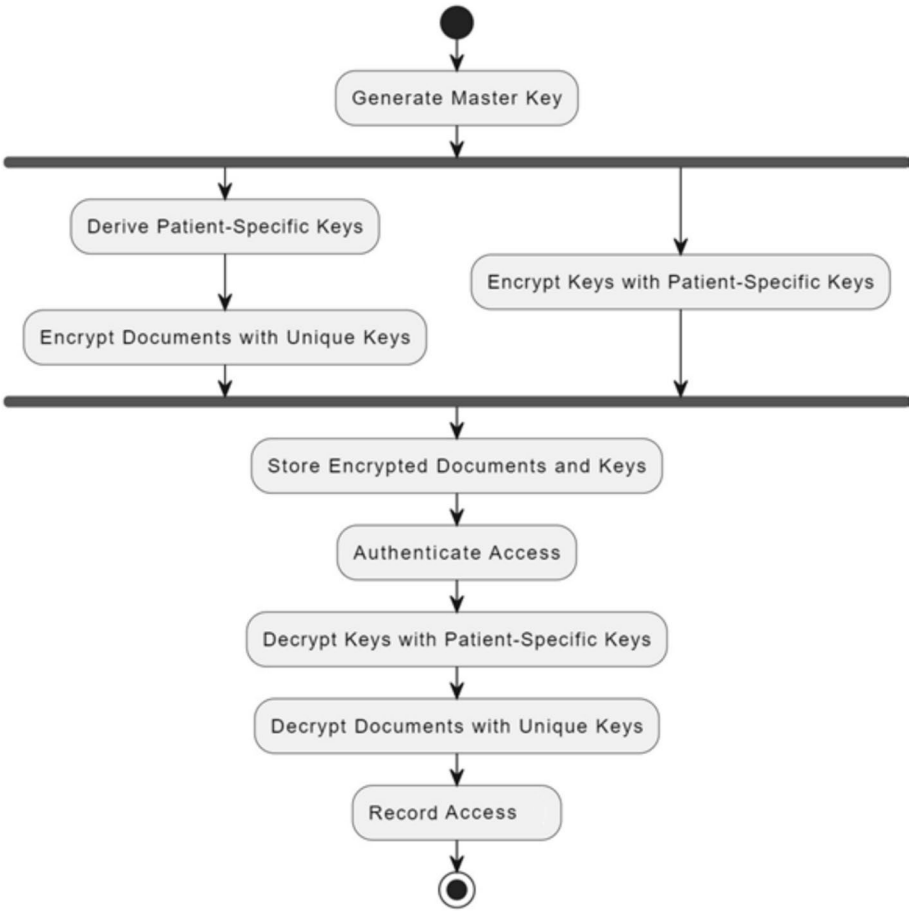

Fig. 6 Working process of encryption/ decryption for secure access

decryption in this work. The user may access MediVault by Adhar Card entities, OTP, registered mobile number, username/password, or public/private keys. The key generation may be at a registered, competent, trusted authority, such as a registered hospital, Adhar Card generation office, NFT or Health Card generation authority, or any Kiosk centre.

4.3 Algorithms for mediVault

The algorithms of MediVault are discussed in this section. The smart contracts that are integrated into our system are made to make the system's numerous functions simple.

4.3.1 NFT generation and minting algorithm

The generation of NFTs, as depicted in Fig. 8, and their minting in the Blockchain are outlined in Algorithm 1. The first step in the process is uploading an NFT file in JSON

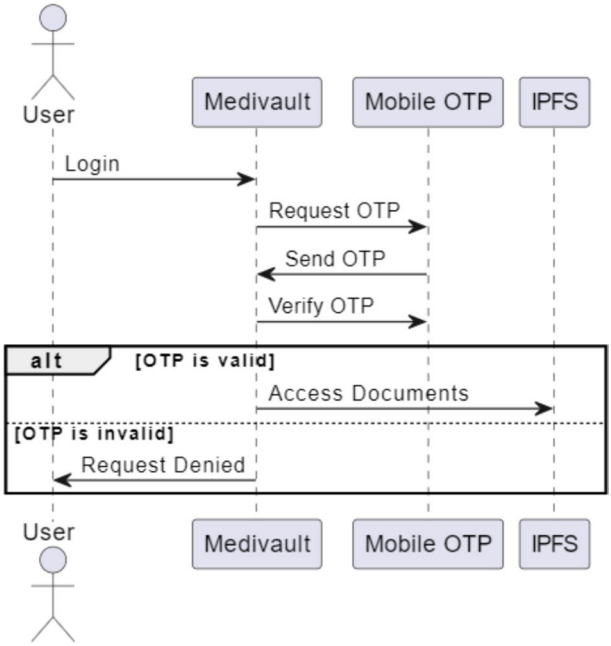

Fig. 7 Working process of authentication for secure access

format that represents the object to IPFS. Figure 8 illustrates the NFT architecture and also shows some relevant information; most of the private information is in hidden form. The values in the proposed medical NFT are taken from the Ayushman Bharat Health Account (ABHA) [18]. Since the NFT being minted is dynamic, conditional privacy will be provided by the hash ID that is generated after minting. After storing the info on IPFS. The content is retrieved and accessed using the content identifier (CID), a unique hash of the content. To link the NFT record on the CID, a token Uniform Resource Identifier (URI) is generated. The token ID, owner address, and metadata URI of the freshly minted NFT are announced along with the token URI associated to the NFT following the completion of the minting process.

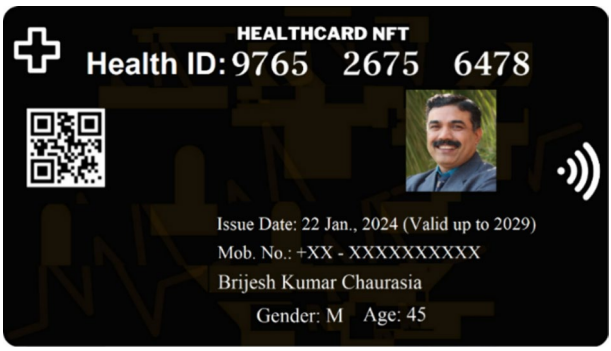

Fig. 8 Health card NFT architecture

4.3.2 Blocks and blockchain transactions

The immutability of the MediVault and patient privacy in the MediVault, which uses a distributed system for data storage, have been confirmed in a significant way attributed to the Blockchain [21]. Figure 9 show that the block structure and Blockchain transactions. Algorithm 2 shows the block entries and process of the Blockchain transaction.

Algorithm 1 NFT generation and minting

Input: Patient health data
Output: NFT storage and CID

```
contract MediNFTcol is ERC721, ERC721URIStorage
{
    constructor()
        ERC721("MediNFTcol", "MediNFT")
        {}
    function_baseURI()
        {
            return "ipfs://cd2306f3800684bd829e7670680742ed66195fcfbb
            7037e48485a7fdb66e17f"
        }
    function_safeMint(address to, unint256 tokenID, string memory uri)
        {
            public
            _safeMint(to, tokenID)
            _setTokenURI(tokenID, uri)
        }
    function_tokenURI(unint256 tokenID)
            public
            view
            override(ERC721, ERC721URIStorage)
            return (string memory)
        {
            return super.tokenURI(tokenID);
        }
    Function supportsInterface (bytes4 interfaceID)
            public
            view
            override(ERC721, ERC721URIStorage)
            returns (bool)
        {
            return super.supportsInterface (interfaceID);
        }
}
```

Algorithm 2 Block structure and Blockchain transactions

Input: NFT hash value, and Patient entries
Output: Blockchain Transactions IDs

Block number #2
{
Node ID #BMHS101
Signature list #@@@@###$$$&&
}
Transaction A
{
Transaction Type Methods: Add File/ Update File/Access File
File Name\Description: 2@..8Ortho
File ID: 2@..8
IPFS Hash: cd2306f3800684bd829e7670680742ed66195fcfbb
7037e48485a7fdb66e17f
Owner List: BKC
}
Transaction B
{
……..
}

4.3.3 Delay computation

To evaluate the efficacy and performance of our proposed MediVault, we have computed the delays of transactions in Blockchain. We have considered both types of Blockchain permission and permissionless.

Fig. 9 Block structure and Blockchain transactions

Algorithm 3 Blockchain transaction(s) delay

```
Input: Blockchain Transaction(s)
Output: Delay (# ms.)
call async function calculateLatencies(promiseArr)
{
  declare variable currBlock to store the block_number
  declare variable startTime to store the date of current transaction
  call the await function Promise.all(promiseArr)
   if the event occurs then
    {
      declare variable elapsedTime which stores date - StartTime
      declare variable lastBlock which stores receipts[0].blockNumber
       for each receipt
        {
          set receipt.blockNumber>lastBlock ?
                                  receipt.blockNumber : lastBlock
         set variable lastBlock - currBlock  to variable blockLatency
        }
    }
}
```

4.3.4 Encryption and decryption delays

MediValut is also providing secure access for patients, doctors, and medical insurance companies. Secure access in terms of confidentiality for authenticated users. At the time of authentication, the patient may receive the public and private keys. The keys will also provide encryption and decryption. Algorithm 4 and Algorithm 5 are encryption and decryption, respectively.

Algorithm 4 Encryption process from user to cloud

```
Input: Keys, Data
Output: Encrypt(Data)
def encrypt(file_path, receipt_public_key_path, encrypted_path):
    with open(receipt_public_key_path, 'rb') as public_key_file:
        receipt_public_key = import_key(public_key_file.read ( ))
        max_chunk_size = 190
        encrypted_chunks = [ ]

    with open(file_path, 'rb') as file:
        data = file.read()
        size = len(data)
        start = 0
        while start < size:
            end  = min(start + max_chunk, size)
            chunk = data(start : end)
            cipher = PKCS1_OAEP.new(recipient_public_key)
            encrypted_chunk = cipher.encrypt(chunk)
            encrypted_chunks.append(encrypted_chunk)
        start = end

    encrypted_data = b " ".join(encrypted_chunks)
    with open(file_path, 'wb') as file:
        data = file.read()
        size = len(data)
        start = 0
        while start < size:
            end  = min(start + max_chunk, size)
            chunk = data(start : end)
            cipher = PKCS1_OAEP.ner(recipient_public_key)
            encrypted_chunk = cipher.encrypt(chunk)
            encrypted_chunks.append(encrypted_chunk)
        start = end

    encrypted_data = b " ".join(encrypted_chunks)
    with open(encrypted_path, "wb") as encrypted_file"
  encrypted_file.write(encrypted_data)
```

Algorithm 5 Decryption process from cloud to user

```
Input: Decryption(key)
Output: Data
def decrypt(encrypted_path, receipt_private_key_path, decrypted_path):
    with open(receipt_private_key_path, 'rb') as private_key_file:
        receipt_private_key = import_key(private_key_file.read ( ))
    with open(encrypted_path, 'rb') as encrypted_file:
        encrypted_data = encrypted_file.read ( )
        decrypted_chunk = [ ]
        start = 0
        while start < len(encrypted_data):
            end  = min(start + 256, len(encrypted_data))
            chunk = encrypted_data[start : end]
            cipher = PKCS1_OAEP.new(receipt_private_key)
            decrypted_chunk = cipher.decrypt(chunk)
            decrypted_chunks.append(decrypted_chunk)
        start = end

    decrypted_data = b " ".join(decrypted_chunks)
    with open(decrypted_path, "wb") as decrypted_file"
decrypted_file.write(decrypted_data)
```

All algorithms are analyzed in terms of results in the results analysis section. We have also analyzed different Blockchain using IPFS and Firebase.

5 Results analysis

In this section, results and analysis are presented. The simulation is tested using the Ethereum Blockchain over IPFS in the cloud against different throughputs. We have considered data such as patient NFT [4], medical reports in jpg and pdf, doctor's prescriptions, medicine purchase invoices, etc.

The simulation was run on an Asus Rog Strix G15 equipped with a Ryzen 7, 4800H Base Speed: 2.90 Ghz processor with eight cores and 16 GB of RAM. For realistic scenarios, we have also evaluated our proposed MediVault over two wired LANs with a capacity of 30 mbps with ten shared nodes and 1.5 gbps with more than 100 shared nodes. Moreover, the proposed Blockchain-enabled MediVault was also evaluated over a wireless LAN of 30 mbps with a single shared node. The actors in Blockchain are patients, government agencies (NFT creators), hospitals, doctors, and medical stores.

The results are analyzed in five phases in the proposed MediVault. Firstly, NFT will be generated for patients by any government agencies as an Ayushman card [18]; after that, patients will take appointments from doctors or be registered in any hospital for appointments of respective doctors as per disease.

5.1 Phase -1 NFT generation and registration in hospital or doctors clinic

Figure 10 shows the NFT generation delay and storage in the cloud using the IPFS. We have also considered that NFT may be in jpg format. The results show that the delay of NFT uploading and downloading of different sizes of NFT in the cloud using IPFS is up to 2628 ms and 5733 ms, respectively of 750 size of NFT. However, the recommended size of NFT is 350 kb, and the delays of uploading and downloading are 2284 ms and 2546 ms, respectively. To reduce the delay of NFT uploading and downloading, we have also analyzed the proposed NFT over the cloud using the FireBase service [20].

Figure 11 shows the delay in uploading and downloading in the cloud using the FireBase service. It is clearly observed that the delay is reduced significantly from IPFS up to 3.33 ms and 4.12 ms of uploading and downloading time in a cloud of 750 kb NFT size using the FireBase service. However, at the recommended NFT size, the uploading and downloading times are only 3.12 ms and 3.5 ms, respectively.

Medical reports may be in different forms or formats in different hospitals and countries. So, we have also evaluated the uploading and downloading delays of different formats of files in the cloud using both the IPFS and Firebase approaches.

Figure 12 shows the uploading and downloading overheads of medical reports using IPFS from the cloud. It is evident from the results that the maximum downloading delay of doc/docx format medical records is up to 9600 ms; however, the uploading delay of pdf format medical records is up to 3200 ms. size of data.

Figure 13 shows the uploading and downloading overheads of medical reports using FireBase from the cloud. It is evident from the results that the maximum uploading delay of pdf format medical records is only 24.45 ms; however, the downloading delay of doc/docx format medical records is only an order of 5.41 ms.

5.2 Phase 2: blockchain transactions

Blockchain transactions are assessed in this step with regard to latency. Consequently, Fig. 14 presents the phase 2 outcome. It is observed that a data size of 1.0 *mb* is taken up to 4154 ms using Ehtereum Blockchain. The delays are computed over different sizes as per the real sizes of different reports with NFT minting in Ehtereum Blockchain. In addition, the general results show that the blockchain delays are up to 2500 ms*;* however, at sizes of 600 and 1000 kb*,* the delays are 3564 and 4154 ms*,* respectively.

5.3 Phase 3: delay computation

In this phase, Blockchain delays are computed over different Blockchain technologies. Figure 15 shows the comparative analysis of computational overheads between the proposed Ethereum-based public Blockchain and the Hyperledger Fabric, which is a private Blockchain. In comparative results, the public Blockchain is referred to as BC1, and the proposed Blockchain is considered BC. It is observed that delays are exponentially increasing in both cases; however, proposed BC is completed transactions of 10 *nodes* in order of 308 ms, and BC1 is completed within about 1000 ms. This proves the viability of our proposed Blockchain-enabled MediVault for healthcare systems.

We have also evaluated the efficacy of the proposed MediVault for different Blockchain technologies. The computational overheads associated with various Blockchain technology are highlighted in Table 1. Additionally, it is mentioned that applying BC1 to other polygon

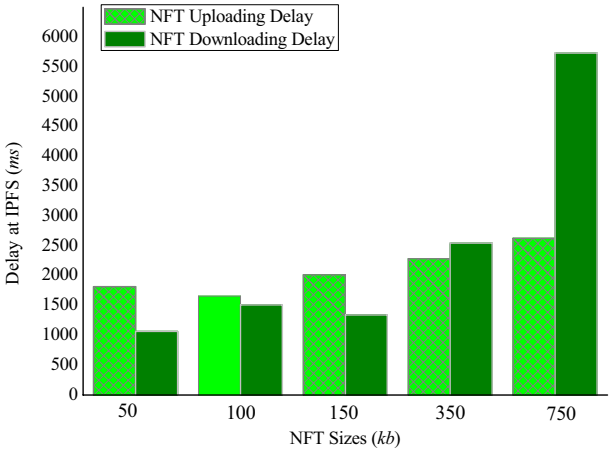

Fig. 10 NFT access delay from cloud using IPFS

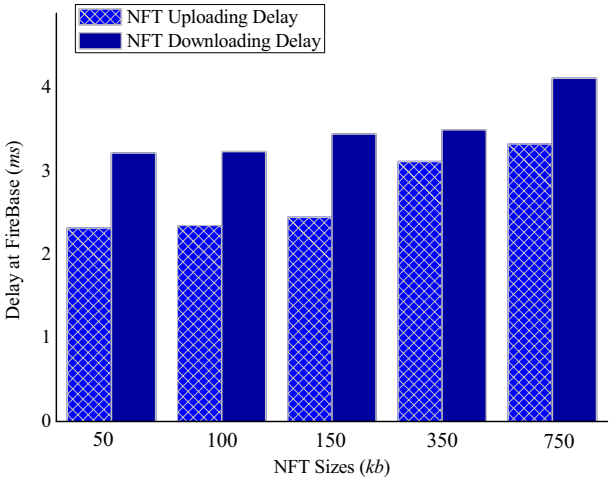

Fig. 11 NFT access delay from cloud using FireBase

(private or permissioned) and public (permissionless) Blockchain is once more an effective approach. The result shown in the table clearly indicates that the computation of the 10 nodes of the proposed Blockchain is taking only 308 ms, which is less in comparison to other Blockchain technologies.

5.4 Phases 4 & 5: delay computation of encryption/decryption process

In this phase, encryption and decryption process delays are evaluated in Fig. 16. The computational delays are evaluated as encryption and decryption overheads using both the approaches of uploading with encryption and downloading with decryption overheads. To the best of my knowledge, it is the first work of all combined technologies; however, we have also evaluated our proposed MediVault over the FireBase and IPFS approaches. The uploading with

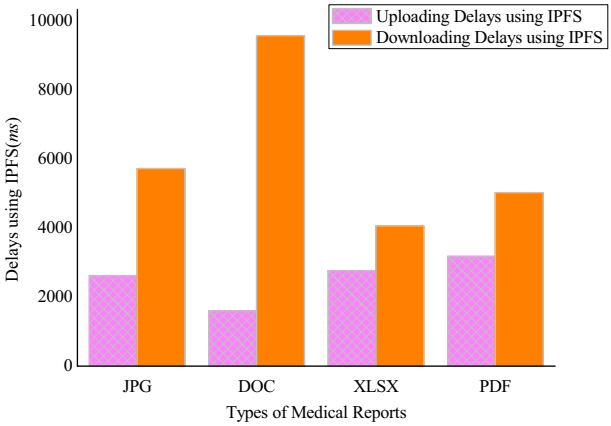

Fig. 12 Healthcare system data uploading/downloading time from cloud using IPFS

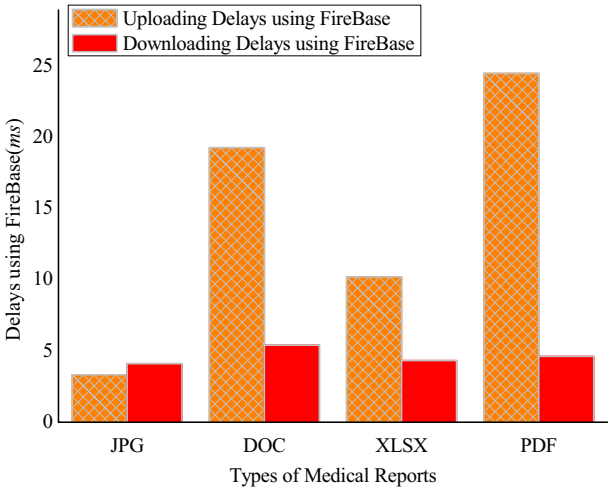

Fig. 13 Healthcare system data uploading/downloading time from cloud using FireBase

encryption and downloading with decryption delays are under 10,000 ms. The approach is user-adaptive and may be used as per the requirements of the users (patients, doctors, etc.).

6 Conclusion and future scope

In this paper, we have designed a Blockchain-enabled MediVault for healthcare systems. This ensures patients effective and practical digital storage solutions for keeping their health records. Specifically, we first demonstrated the creation and minting of NFTs along with the authentication process for MediVault. This was followed by Blockchain transactions over the cloud, which are intended to offer secure access for patients, physicians, and chemists, in addition to safe digital storage of healthcare data.

To the best of my knowledge, it is the first complete, secure, and simple solution for rural and urban patients. The comparative analysis and performance evaluation have demonstrated the usefulness and efficiency of our proposed MediValut, which has a low computation overhead in order of milliseconds. In this work, blockchain-enabled MediVault

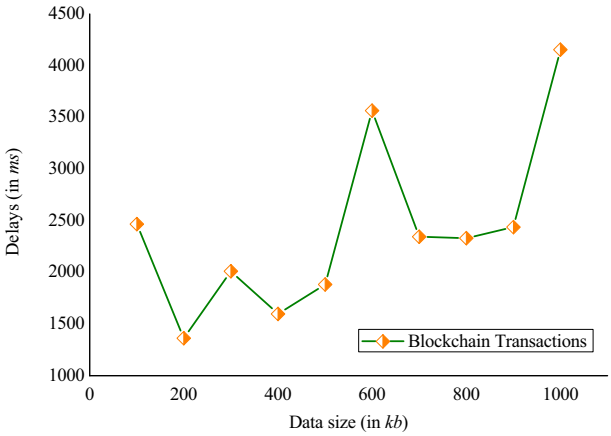

Fig. 14 Blockchain Transactions over different size

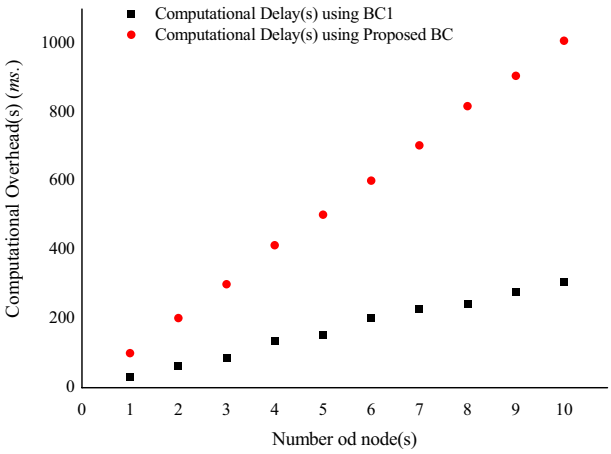

Fig. 15 Comparative analysis of transaction delays in Blockchain(s)

Table 1 Blockchain technologies overheads

Blockchain Technologies	Number of Nodes	
	5	10
Ethereum (BC)	154	308
Binance (Permissionless)	155	338
Polygon (Permissioned)	190	316

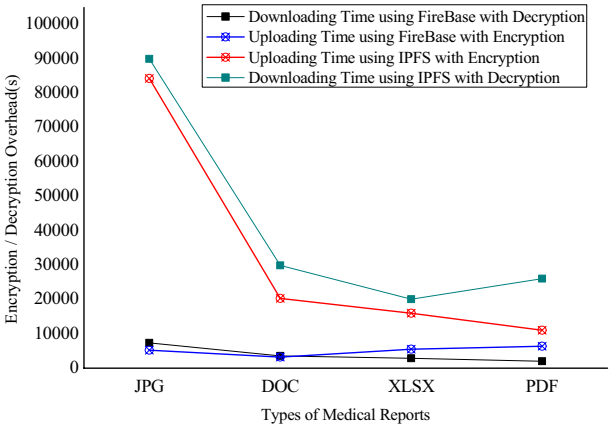

Fig. 16 Encryption/decryption computational overhead

is secured by ECC-based asymmetric cryptography due to its wide usage. However, such approaches are suffering attacks. In our future study, we will investigate the use of blockchain technology to guarantee the cloud-based deployment of patient health records while fending off collusion attempts from unscrupulous physicians, hospitals, and chemists. The fusion of post-quantum cryptography with blockchain is also the future.

Author contribution Solo author paper; all concept, implementation, and writing done by myself.

Funding The authors are not received funding from any of the sources.

Data availability The data set generated and/or analyzed during the current study is available upon reasonable request from the corresponding author. However, there is no need to data, it may be generated by MediVault.

Declarations

Conflict of interest The work is not submitted in any other journal. There is no conflict of interest.

References

1. Yuan W-X, Yan B, Li W, Hao L-Y, Yang H-M (2023) Blockchain-based medical health record access control scheme with efficient protection mechanism and patient control. Multimed Tools Applic 82:16279–16300. https://doi.org/10.1007/s11042-022-14023-3
2. Jin H, Luo Y, Li P, Mathew P (2019) A review of secure and privacy-preserving medical data sharing. IEEE Access 7:61656–61669. https://doi.org/10.1109/ACCESS.2019.2916503
3. Azaria A, Ekblaw A, Vieira T, Lippman A (2016) MedRec: using blockchain for medical data access and permission management. In: 2nd IEEE International Conference on Open and Big Data (OBD). pp 25–30. https://doi.org/10.1109/obd.2016.11
4. Rai S, Chaurasia BK, Gupta R, Verma S (2023) Blockchain-based NFT for healthcare system. In: 12th IEEE International Conference on Communication Systems and Network Technologies (CSNT). pp 700–704. https://doi.org/10.1109/CSNT57126.2023.10134632
5. Raghav AN, Venkatesan S, Verma S (2023) Privacy-preserving cloud data sharing for healthcare systems with hybrid blockchain. Peer Peer Netw Appl 16(5):2525–2547. https://doi.org/10.1007/s12083-023-01521-w

6. Sharma AK, Chaurasia BK (2023) Blockchain-based NFT for evidence system. In: Roy BK, Chaturvedi A, Tsaban B, Hasan SU (eds) Cryptology and network security with machine learning. ICCNSML 2022. Algorithms for intelligent systems. Springer, Singapore, pp 441–451. https://doi.org/10.1007/978-981-99-2229-1_37
7. Agbo CC, Mahmoud QH, Eklund JM (2019) Blockchain technology in healthcare: a systematic review. Healthcare, MDPI 7(56):1–30. https://doi.org/10.3390/healthcare7020056
8. Sharma AK, Chaurasia BK (2023) Blockchain-based NFT for evidence system. In: Roy BK, Chaturvedi A, Tsaban B, Hasan SU (eds) Cryptology and network security with machine learning. ICCNSML 2022. Algorithms for intelligent systems. Springer, Singapore, pp 441–451. https://doi.org/10.1007/978-981-99-2229-1_37
9. Healthcare data, Online available at: https://csd.columbia.edu/sites/default/files /content/docs/ICT%20India/Papers/ICT_India_Working_Paper_25.pdf, Last accessed 22 Jan., 2024
10. Misra G, Hazela B, Chaurasia BK (2023) Zero knowledge based authentication for internet of medical things. In: 14th IEEE International Conference on Computing, Communication And Networking Technologies (ICCCNT). pp 1–6. https://doi.org/10.1109/ICCCNT56998.2023.10307359
11. Zhang G, Yang Z, Liu W (2022) Blockchain-based privacy preserving e-health system for healthcare data in cloud. Comput Netw 203(108586):1–9. https://doi.org/10.1016/j.comnet.2021.108586
12. Kakarlapudi PV, Mahmoud QH (2021) Design and development of a blockchain-based system for private data management. Electronic General, MDPI 10(3131):1–22. https://doi.org/10.3390/electronics10243131
13. Justin S G, Zafreen S, Dagher GG, Long M (2021) "VAULT: a scalable Blockchain-based protocol for secure data access and collaboration. In: IEEE International Conference on Blockchain (Blockchain). pp 376–381. https://doi.org/10.1109/Blockchain53845.2021.00059
14. Peiris TRNR, Bandara WMUKMT, Sachintha KVA, Senarathne A, Ganegoda BA (2019) VAULT - a shared distributed and redundant storage solution. In: International Conference on Advancements in Computing (ICAC). pp 458–463. https://doi.org/10.1109/ICAC49085.2019.9103371
15. Gebreab SA, Salah K, Jayaraman R, Zemerly J (2023) Trusted traceability and certification of refurbished medical devices using dynamic composable NFTs. IEEE Access 11:30373–30389. https://doi.org/10.1109/ACCESS.2023.3261555
16. NFT Marketplace, Online available at: https://arxiv.org/pdf/2304.10632.pdf, Last accessed on 29/3/2023
17. Bamakan SMH, Nezhadsistani N, Bodaghi O, Qu Q (2022) Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. Sci Rep 12(1):2178–2182
18. Digital health infrastructure, Online available at: https://abdm.gov.in/SDF, Last accessed on 22/1/2024
19. InterPlanetary File System (IPFS), Online available at: https://ipfs.tech, Last accessed on 22/1/2024
20. Firebase, Online available at: https://firebase.google.com/docs /storage/web/start, Last accessed on 22/1/2024
21. Miao J, Wang Z, Wu Z, Ning X, Tiwari P (2024) A blockchain-enabled privacy-preserving authentication management protocol for internet of medical things. Expert Syst Applic 237(121329), Part A. https://doi.org/10.1016/j.eswa.2023.121329
22. Anand A, Bedi J, Rida I (2024) MIWET: medical image watermarking using encryption and fusion technique. Comput Electr Eng 115(109114):1–15. https://doi.org/10.1016/j.compeleceng.2024.109114
23. Anand A, Bedi J, Aggarwal A, Khan MA, Rida I (2024) Authenticating and securing healthcare records: a deep learning-based zero watermarking approach. Image Vis Comput 145(2s):104975, 1-12. https://doi.org/10.1016/j.imavis.2024.104975
24. Wenhua Z, Hasan MK, Jailani NB, Islam S, Safie N, Albarakati HM, Aljohani A, Khan MA (2024) A lightweight security model for ensuring patient privacy and confidentiality in telehealth applications. Comput Hum Behav 153(108134):1–10. https://doi.org/10.1016/j.chb.2024.108134
25. Iqbal S, Qureshi A, Aurangzeb K, Alhussein M, Haider SI, Rida I (2023) AMIAC: adaptive medical image analyzes and classification, a robust self-learning framework. Neural Computing and Applications, Special Issue-Intelligent Systems in Biomedical and Healthcare Informatics. pp 1–29. https://doi.org/10.1007/s00521-023-09209-1
26. Chaurasia BK, Raj H, Rathour SS, Singh PB (2023) Transfer learning driven ensemble model for detection of diabetic retinopathy disease. Med Biol Eng Comput, Springer 61:2033–2049. https://doi.org/10.1007/s11517-023-02863-6
27. Nawaz M, Nazir T, Baili J, Khan MA, Kim YJ, Cha J-H (2023) CXray-EffDet: chest disease detection and classification from x-ray images using the EfficientDet model. Diagnostics 13(248). https://doi.org/10.3390/diagnostics13020248

28. Kumar A, Chaurasia BK (2024) Detection of SARS-CoV-2 virus using lightweight convolutional neural networks. Wirel Pers Commun 1–23. https://doi.org/10.1007/s11277-024-11097-0
29. Saxena R, Arora D, Nagar V, Chaurasia BK (2024) Blockchain transaction deanonymization using ensemble learning. Multimed Tools Applic 1–30. https://doi.org/10.1007/s11042-024-19233-5
30. Chen, Y., Zeng, Z., Lin, X., Du, X., Rida, I., Xiao, R. (2023) FDEPCA: a novel adaptive nonlinear feature extraction method via fruit fly olfactory neural network for IoMT anomaly detection. IEEE J Biomed Health Inform 1–13. https://doi.org/10.1109/JBHI.2023.3318892
31. Tripathi G, Singh VK, Chaurasia BK (2023) An energy-efficient heterogeneous data gathering for sensor-based internet of things. Multimed Tools Applic 82:42593–42616. https://doi.org/10.1007/s11042-023-15161-y
32. Srivastava S, Agrawal D, Chaurasia BK, Adhikari M (2024) Blockchain-enabled Trust Computation in Internet of Vehicle. Multimed Tools Applic 1–19. https://doi.org/10.1007/s11042-024-18874-w
33. Aski VJ, Dhaka VS, Parashar A, Kumar S, Rida I (2023) Internet of things in healthcare: a survey on protocol standards, enabling technologies, WBAN architectures and open issues. Phys Commun 60(102103):1–15. https://doi.org/10.1016/j.phycom.2023.10210

Brijesh Kumar Chaurasia has a Ph.D. in Privacy Preservation in Vehicular Ad-hoc NETworks from the Indian Institute of Information Technology, Allahabad, India as well as M. Sc. Computer Science from Jiwaji University Gwalior, India, and M. Tech. Computer Science from Devi Ahilya Vishwavidyalaya, Indore, India. He has served as a Professor in the Department of Computer Science & Engineering & Dean Academics with the ITM University Gwalior in Madhya Pradesh, India. Prof. Chaurasia has also completed role as a founder HoD (IT) at IIIT Lucknow, India. Currently, working in the Department of Computer Science and Engineering as a Professor & Dean Research and Innovation with the Pranveer Singh Institute of Technology, Kanpur, India. His research interests encompass security in mobile ad-hoc networks, sensor networks, cloud computing, Vehicular cloud, trust management in VANETs and mobile ad-hoc networks Blockchain, Machine Learning, and IoT. Prof. has published more than 120 research papers in international journals and conferences. He has over 24 years of teaching experience and has also been involved in organizing international conferences, workshops and science conclave academic activities. He has supervised more than 28 PG/ UG/ Ph. D. Scholars. He is a member of the Machine Intelligence Research (MIR) Labs, Gwalior, India, a fellow of CSI, a senior member of IEEE and Fellow IETE, Gwalior sub-section, India.