A Robust Model for a Healthcare System with Chunk Based RAID Encryption in a Multitenant Blockchain Network

Bharath Babu S, Jothi K R*
School of Computer Science and Engineering
Vellore Institute of Technology
Vellore, TamilNadu, India 632014

***Abstract*—Healthcare informatics has revolutionized data extraction from large datasets. However, using analytics while protecting sensitive healthcare data is a major challenge. A novel methodology for Privacy-Preserving Analytics in Healthcare Records addresses this essential issue in this study. The multi-tenant Blockchain framework uses chunk-based RAID encryption. For the healthcare business, chunk-based RAID encryption in a multi-tenant blockchain architecture creates a durable, safe, and efficient solution for processing confidential healthcare information. This solution improves data security, integrity, availability, performance, regulatory compliance, and scalability by combining RAID and blockchain technology. Contemporary healthcare systems need these qualities to work well. This approach was done in Python, and the libraries used the VSCode tool. To maintain data security, integrity, and accessibility, a strong healthcare system architecture with chunk-based RAID encryption in a multi-tenant blockchain network requires various advanced technologies.**

Keywords*—Multi-tenant; chunk-based; RAID; blockchain; healthcare records

I. Introduction

The quick progress in the internet of things (IoT) concept has transformed healthcare businesses by introducing significant enhancements in e-health/medical records drug prescription data, and insurance information. The rapid advancement of the internet of things (IoT) has revolutionized healthcare industries by offering substantial improvements in e-health/medical records, drug prescription data, and insurance information. IoT devices enable real-time monitoring of patients. Additionally, they have the potential to decrease the necessity of hospital visits for regular health examinations. Home health monitoring systems that are connected can effectively decrease the duration of hospital visits and lower the expenses associated with readmission. The Internet of Things (IoT)-enabled medical devices have the capability to aid in the process of diagnosing medical conditions by providing alerts and triggering notifications prior to the onset of symptoms. Numerous software as a service applications make advantage of multi-tenant data storage, which involves the sharing of resources and the layout of the data-store across multiple tenants. The fact that each user or tenant is given their own instance of a single tenant application, on the other hand, results in increased expenses for servicing and maintenance for both the tenants and the suppliers. When resources are shared across multiple tenants in a multi-tenancy setting, those costs are reduced for all of the parties involved [1, 2]. Despite this, multitenant architectures pose data security risks. When multiple tenants share a storage area, data infringement is more likely if their data is not properly isolated. A hostile tenant can assault other tenants' data by sending harmful information, making unauthorized transactions, or interrupting exchanges. This can be done several ways. Therefore, a robust system is essential to ensure that multi-tenant data cannot be altered without authority. Flexibility and data segregation are crucial in multi-tenant applications [3].

Blockchain technology is a recent invention that allows secure data storage in multi-user applications. In addition to bitcoin, blockchain technology is becoming a powerful tool for secure and immutable storage systems [3]. Blockchains or Distributed Ledgers prevent data tampering by decentralizing and cryptographic hashing. Blockchain storage is designed to securely and permanently store data and transactions, preventing tampering. Access to private or permissioned blockchains is limited to identifiable members [4]. Blockchains offer an unchangeable ledger that lets authorized network participants see stored data in real time.

Blockchain is a highly promising technology that has the potential to greatly improve the efficiency of healthcare data management operations. It achieves this by offering unparalleled data efficiency and ensuring trust in the system. The platform provides a diverse array of notable and inherent characteristics, including distributed storage, visibility, permanence, verification, adaptability in data access, interlinking, and safeguarding, thereby facilitating extensive adoption of blockchain technology for healthcare data management [5].

Blockchain employs smart contracts to establish mutually agreed upon terms and conditions among all healthcare partners in the network, eliminating the need for intermediaries [6,7]. It minimizes superfluous administrative expenses. Blockchain primarily depends on three fundamental concepts: peer-to-peer networks, public key cryptography, and consensus procedures [8]. Blockchain is categorized into three types based on permission management: public, private, and consortium blockchains [9]. Any individual with internet access can participate in the consensus procedure of public blockchains.

*Corresponding authors

Public blockchains incorporate incentives and employ proof-of-work or proof-of-stake techniques to ensure encrypted digital verification. The public blockchain system is completely visible, meaning that the identity of each participant is kept pseudo-anonymous. In a private blockchain, network control is exclusively held by a single company. Thus, this particular type of blockchain necessitates a reliable intermediary to achieve consensus. The consortium blockchain integrates the benefits of public and private blockchain networks. This solution is specifically ideal for select enterprises who have the objective of optimizing communication within their own network. Healthcare businesses have the flexibility to choose any sort of blockchain network based on their individual requirements or use case scenarios, as each network has its own advantages and disadvantages.

The framework laid out in this article aims to enhance other related blockchain-based systems for storage in the following aspects: The aim of chunk-based RAID encryption in a multi-tenant blockchain model for the healthcare sector is to provide a robust, secure, and efficient framework for managing sensitive healthcare data. By leveraging the strengths of both RAID and blockchain technologies, this approach ensures enhanced data security, integrity, availability, performance, regulatory compliance, and scalability, which are crucial for the effective operation of modern healthcare systems. Utilize separate ledgers or channels to ensure that the data of different tenants remains isolated and inaccessible to others. This approach is commonly employed in permissioned blockchain networks such as Hyper-ledger Fabric. Implement strong access control mechanisms to restrict access to each tenant's data, ensuring only authorised individuals can view or interact with it. Deploy resilient authentication techniques to bolster security for users accessing the blockchain network. One such solution is to use multi-factor authentication (MFA) in order to improve security measures. Role-Based Access Control (RBAC) is a mechanism for controlling access to resources in a methodical manner. Administrators can utilize this feature to allocate roles to users, thereby specifying the permissions and privileges they possess. RBAC enables companies to enforce access controls that limit users to only the information and functionality essential for their specific position. This enhances security and minimizes the likelihood of unauthorized access. It is crucial to assign responsibilities to users and establish permissions depending on their duties in order to ensure efficient management. This enhances the administration of resource and operation authorization within the network.

Section II investigates existing approaches and discusses the issues of protecting medical records in multi-tenant systems. Section III discusses the proposed solutions along with the block chain technology with chunk-based RAID encryption to address the existing problems. Section IV explains the analytical and technological implementation of the cryptographic methods, RAID setups and data transfer protocols. Section V evaluates the proposed method over other existing techniques. Section VI examines the model's limitations, applications and further scopes.

A. Literature Review

Extensive research is being conducted in various interdisciplinary fields using blockchain technology. The research conducted in [10] has aimed to tackle the issue of internet piracy in the movie business by the creation of a blockchain-powered anti-piracy system called "Vanguard". This system replaces the traditional method of registering intellectual property (IP) and monitors the ownership of IP rights to prevent unauthorised distribution of data. The utilisation of blockchain technology and certificateless cryptography has been employed in [11] to create a data storage system that effectively manages and safeguards vast quantities of IoT data.

The authors of [12] have employed blockchain technology to develop methods for sharing data in smart cities. In [13], a proposal was made for a Blockchain Tree to store information from smart ID cards. This method enhances security by incorporating blockchain technology at a lower level and extending it to a higher level.

The research in [14] centres on the utilisation of blockchain technology for several applications in the food business, such as food tracing, land registrations, customer awareness programmes, and farm insurance. The proposed system has been implemented by authors using the open-source platform Multi-Chain. An important benefit of utilising blockchain technology is its ability to effectively deter forgery and fraud due to its inherent immutability and transparency. In a study referenced as [15], a blockchain-based solution is proposed to avoid property fraud, including fraud related to bank loans.

Ping end-to-end Reporting (PingER) is a framework created by the SLAC National Accelerator Laboratory in the United States for measuring internet performance across the globe. The proposal suggests implementing a distributed blockchain technology to store data for PingER in a decentralised manner. Instead of storing data in a centralised location, this system distributes the data files across various sites using Distributed Hash Tables (DHT). Only the metadata of these files is saved on the blockchain.

The study [16] discusses a novel concept called Blockchain-as-a-Service (BaaS), which is comparable to Software-as-a-Service (SaaS). This is a cloud-based service that simplifies the process of setting up a blockchain. It also offers a platform for running apps and provides security and other essential elements of blockchain technology.

The authors of [17] have suggested a system based on blockchain technology for a multitenant architecture. Each tenant possesses an independent blockchain with certain permissions, which is then linked to a central chain. The collaboration for this project was conducted with Laava ID Pty Ltd (Laava), and the execution was accomplished using the Ethereum platform. This study examines the healthcare sector as a prominent field for the implementation of blockchain technology. Extensive research and documentation have been dedicated to studying the application of blockchain in the healthcare industry. Researchers in [18] have integrated blockchain technology into digital services, such as online consultations. They have successfully implemented a decentralised system to ensure utmost security in the healthcare industry. Blockchain technology has improved transparency in communication between users and clients, particularly in the context of doctor-patient interactions. Furthermore, the authors have included three separate case studies in this specific field: Telemedicine, Patientory, and Medblock.

The study [19] provides a thorough examination of the research conducted on electronic health record (EHR) systems that utilise blockchain technology. Several consensus algorithms have been explored by researchers for implementation in public blockchains. These include the Practical Byzantine Fault Tolerance replication algorithm (PBFT), RAFT, Proof of Authority (PoA), Proof of Capacity (PoC), and Proof of Elapsed Time (PoET). An innovative solution called MediBchain has been developed in [20] to ensure the security and privacy of healthcare data by leveraging blockchain technology. They have utilised Elliptic Curve Cryptography (ECC) to secure sensitive information.

A mobile application has been created utilising blockchain technology to store data related to cognitive behavioural therapy for patients with insomnia [21]. The data is stored in the Hyperledger Fabric blockchain network using JSON format. This system utilises blockchain technology to ensure data transparency and accessibility while eliminating the risk of data tampering. Blockchain technology has been successfully integrated with artificial intelligence systems to develop a predictive system for managing the clinical risks associated with COVID-19 infection [22-25]. This integration has shown promising results in improving clinical risk management.

B. Challenges Faced in the Existing Techniques

1) Single database, shared schema: In the healthcare industry, a single database with a shared schema shown in Fig. 1 presents many challenges, especially when considering security, confidentiality, data consistency, and expandability. These are the main issues with this approach. A unified database with a shared schema can attract attackers. A compromise could disclose all patient data from numerous departments or institutions. It's difficult to restrict access to specific data in a shared schema to authorized users. Data segmentation to protect sensitive patient data is tough. Multiple users updating the database at once might cause data conflicts and overwrites, compromising data integrity. Single-database uniformity is key. Inconsistencies can cause serious medical errors. Data leaking is a prominent concern in a shared schema architecture, when multiple tenants utilize the same schema. These factors can result in security breaches, and impairments in performance [26]. Access control is intricate, and conflicts over resources can have a negative influence on performance. Increasing the number of renters may lead to scalability concerns. Optimizing searches across several tenants is a challenging task that requires the construction of efficient indexing and caching solutions to prevent performance issues. Handling schema changes poses difficulties, and data migration carries a high chance of errors. Insufficient options for personalization and adaptability are further obstacles. Tenant management include the effective process of bringing new tenants on board, removing tenants when necessary, ensuring equitable distribution of resources, and implementing security measures at the individual row level. By implementing resource quotas, automatic monitoring tools, and conducting frequent audits, it is possible to reduce these issues and enhance the management of a single database common schema.

2) Single database, separate schema: Implementing a solitary database with distinct schemas for individual tenants in the healthcare sector poses numerous difficulties. These difficulties

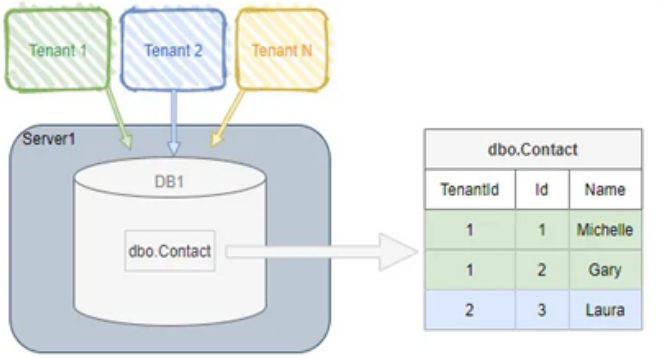

Fig. 1. Single database, shared schema model.

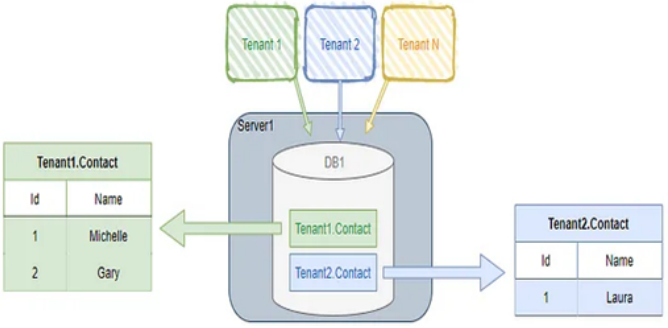

Fig. 2. Single database, separate schema model.

can have an impact on performance, security, maintainability, and compliance [27]. The system Restoring data for a single tenant is not a simple task, although it is slightly easier than the technique of using a single database with a shared schema (Fig. 2), because the tenant data is kept separate. As the tenant count increases, a significant number of database objects will be generated to handle and uphold. Schema modifications require a more complex process, as they need to be distributed to several tenants.

C. Database per Tenant

Drawbacks to using a Database per tenant (Fig. 3) approach include the need for additional server maintenance and security measures, an increase in the number of database objects to manage and maintain as the number of tenants rises, and the complexity of creating new schemas when adding new tenants [28].

1) Multiple databases, multiple tenants per database, shared schema: The disadvantages of having numerous databases, multiple tenants per database, and a shared schema (Fig. 4) are as follows: Tenants persist in employing a shared database and schema alongside other folks. Further maintenance is required. Those in charge of managing many databases face complex operational challenges, the risk of data breaches, the necessity for efficient performance monitoring, obstacles in attaining scalability, increased maintenance responsibilities, and concerns over security [29]. Enforcing compliance with regulations like GDPR and HIPAA can be challenging in shared schema setups. Operational complexity

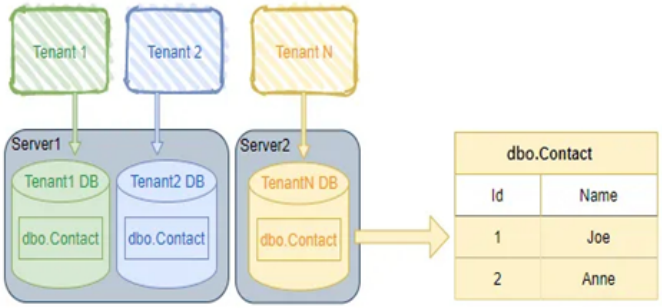

Fig. 3. Database per tenant model.

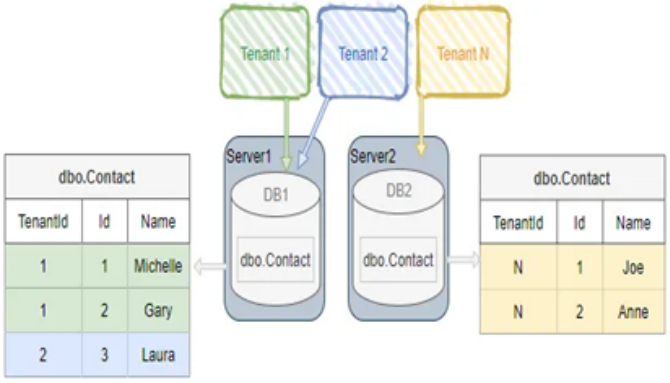

Fig. 4. Multiple databases, multiple tenants per database, shared schema model.

refers to the range of duties involved in managing a system, including backup and recovery methods, monitoring, problem-solving, and limitations on modification. Efficiently managing economic issues, including infrastructure expenses, is essential for properly allocating resources and ensuring compliance.

II. Research Method

This research takes a methodical approach to tackle the identified challenges. Researcher thoroughly examine and incorporates insights from various sources such as academic papers, industrial blogs, and related research initiatives. The proposed approach efficiently combines the benefits of blockchain technology and chunk-based RAID encryption to address important difficulties in healthcare data management, such as security, fault tolerance, scalability, performance, and regulatory compliance. Its sturdy design protects sensitive medical information while retaining high efficiency and adaptability, making it a great option for the changing demands of modern healthcare organizations.

A. Proposed System

To address the difficulties presented by current multi-tenancy database systems, we suggest an innovative method that utilizes the dynamic arrangement of tenant connections and incorporates blockchain technology to overcome the stated issues. Our goal is to establish a flexible and scalable environment by implementing a dynamic topology in healthcare organizations which can create a robust, scalable, and flexible environment that supports their evolving needs while maintaining high standards of performance and security. This will enable tenants to communicate with each other smoothly, without being limited by a predefined schema. This dynamic connectivity facilitates improved data isolation, which enables quick restoration of individual tenant data without the complications associated with a single shared schema. In addition, we implement blockchain technology to securely handle the relationships between renters. The decentralized and tamper-resistant characteristics of blockchain guarantee the reliability and safety of tenant connections, effectively resolving problems regarding High Availability, Disaster Recovery, and Monitoring techniques. This novel method reduces the requirement for extensive maintenance and schema modifications, offering a strong basis for a scalable, secure, and easily controllable multi-tenancy database structure. Through the use of blockchain technology, we address the difficulties associated with existing models by decentralizing connectivity and ensuring security. This provides a revolutionary solution for a dynamic and safe database environment that can accommodate multiple users. Healthcare businesses have the ability to establish a strong, adaptable, and versatile infrastructure that caters to their changing requirements while upholding exceptional levels of performance and security.

B. Secured Data Transaction of Tenants using Blockchain Technology

Implementing secure data transactions for healthcare tenants using blockchain technology entails utilizing the inherent characteristics of blockchain, like decentralization,immutability, and transparency, to guarantee the integrity,security, and privacy of data. Our proposed system incorporates Blockchain Technology to guarantee the secure transfer of data between clients. Blockchain, being a distributed and tamper-proof ledger, offers an unchangeable record of all transactions. Data transactions are cryptographically encrypted to guarantee data integrity and prevent unauthorized access. This not only improves the overall security of healthcare data but also establishes a clear and responsible framework for data transfers inside the multi-tenant environment. The model of multi-tenant blockchain network for the health sector is illustrated in the Fig. 5.

C. A Mathematical Framework for Enhancing Data Security in Multi-Tenant Blockchain Technology

Securing data in multi-tenant blockchain technology requires utilizing a mathematical framework that integrates different cryptographic techniques and consensus mechanisms. This framework is designed to guarantee the security and reliability of healthcare data, while also ensuring the smooth operation and effectiveness of the blockchain network. Here is a comprehensive approach to developing such a framework.

1) Cryptographic Hash Functions: Cryptography uses mathematical hash functions. Hash functions usually take variable-length inputs and output fixedlength outputs. Computing systems depend on hash functions for message integrity and data validation. Though “weak” cryptographically due to their polynomial-time solvability, these algorithms are not easily decipherable. By using cryptographic hash functions, ordinary hash functions become more secure, making it harder

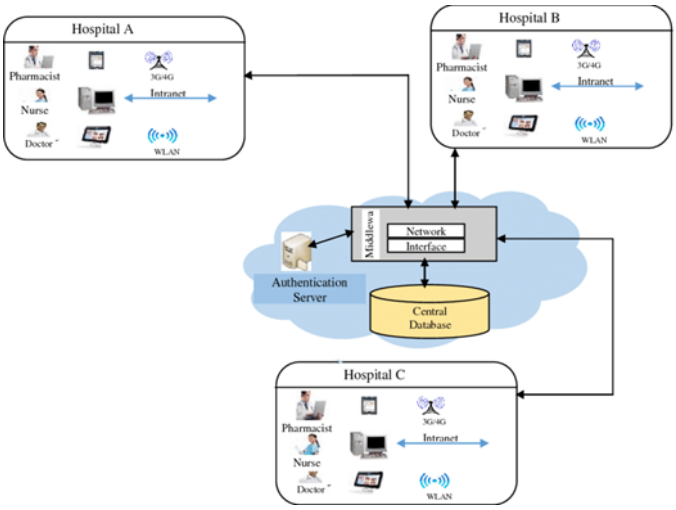

Fig. 5. Multitenant blockchain model for healthcare sector.

to decrypt communications or find their originators. Cryptographic hash functions have three traits: They never meet. It is vital that each input provides a unique output hash. Can hide. It should be difficult to discern a hash function's input from its output [30]. They should help solve riddles. A specified output can make selecting an input difficult. Therefore, input must come from a variety of sources. Cryptographic hash functions are employed in a chunk-based RAID encryption system to guarantee the integrity of each individual chunk of data. The procedure is dividing the data into pieces, applying a hashing function to each chunk, encrypting each chunk, and subsequently dispersing the encrypted chunks throughout the RAID array. This method aids in safeguarding against data corruption and guarantees the ability to identify any modifications made to the data Table I.

TABLE I. CHUNK-BASED RAID ENCRYPTION

Mathematical Approach for Hashing in Chunk-Based RAID Encryption	
Step1	**Data Chunking** Let D be the data to be stored in the RAID. Divide the data D into n chunks Ci Where i = 1,2,3.... n as shown in the equation D=C_1C_2C_n.
Step2	**Hashing Each Chunk** Compute the hash of each chunk using a cryptographic hash function H. $H_i = H(C_i)$ Where Ci is the ith chunk of data Hi is the hash value of the ith chunk H is the cryptographic hash function. Apply SHA-256 to each chunk Ci, and obtain in the equation, $H_i = SHA - 256(C_i)$.
Step3	**Encrypting Each Chunk** Encrypt each chunk using an encryptional algorithm E with a key K as shown in below equation. $E_i = E(K, C_i)$ Where E is the Encryption Function K is the encryption Key Ei is the encrypted chunk. Encrypt each chunk Ci with AES and key K, and obtain the equation below. $E_i = AES(K, C_i)$.
Step4	**Storing Hashes and Encrypted Chunks** EStore the hash values Hi and the encrypted chunks Ei in the RAID array. Distribute Ei across the RAID disks according to the chosen RAID configuration.

2) Password Verification: Most websites store passwords as hashes because text files are unsafe. Passwords are hashed when entered. The company's servers' hashed values are compared to the outcome. Hackers have created rainbow tables, databases containing common passwords and their hashes, to gain unauthorized access to accounts.

A chunk-based RAID encryption system can employ cryptographic hash functions and password-based key derivation functions (PBKDFs) to verify passwords. The objective is to securely authenticate the password utilized for the encryption and decryption of data chunks. Belowis a comprehensive formula and step-by-step process for verifying passwords in a system.

The user has provided a confidential pass code, denoted as P. To prevent precompiled attacks, a distinct salt value S is appended to the password prior to hashing. The process of generating a cryptographic key K from a password and salt is referred to as a key derivation function (KDF). In order to authenticate the password during the decryption process, the system must verify that the entered password is capable of generating the accurate encryption key. The mathematical function to derive the key K using the provided password P and the stored salt S is given in Eq. (1):

$$K = KDF(P, S) \tag{1}$$

Decrypt each encrypted chunk E_i using the derived key K using Eq. (2):

$$C_i = Decrypt(K, E_i) \tag{2}$$

Compute the hash H' of each decrypted chunk Ci by Eq. (3):

$$H' = Hash(C_i) \tag{3}$$

Verify the computed hash H' matches the stored hash H_i, if $H' == H_i$ for all i, then the passcode is verified.

3) Signature Generation and Verification: Signature creation plays a vital role in ensuring the validity and integrity of data pieces in chunk-based RAID encryption solutions. Signature generation commonly entails the utilization of cryptographic methods to generate a distinct identifier (signature) for every chunk.

Mathematical signature verification verifies digital documents and messages. When all conditions are met, a valid digital signature proves to the recipient that the communication was sent by a known sender and was not tampered with. Use the private key privK and a digital signature algorithm DSA to sign the hash Hi by the Eq. (4) and (5):

$$SignPrivatekey(x) = SignatureSignprivatekey(x) = Signature \tag{4}$$

$$Sign_i = DSA_{sign}(priv_K, H_i) \tag{5}$$

The equation depicts the process of generating a digital signature using a private key, ensuring data authenticity and non-repudiation within the blockchain. The average digital signature technique has three algorithms. The key generation algorithm creates keys first. Signing algorithms use messages and private keys to create signatures. Finally, the signature verifying method verifies signatures.

To verify the signature, recalculate the hash Hi of the received chunk Ci using Eq. (6):

$$H^{'} = SHA - 256(C_i) \tag{6}$$

To validate the signature, utilize the public key pubk that corresponds to the private key privK and employ the same digital signature procedure, DSA as in Eq. (7) and (8):

$$Verif = DSA_{Verif}(pub_K, H^{'}, Sign_i) \tag{7}$$

$$Verifypublickey(Signature, Data, Blockchain) = \{True, False\} \tag{8}$$

This equation represents the verification process, ensuring that data transactions are authentic and valid through the use of public key verification. If the verification process is successful, then the Signi, is considered legitimate, and it is confirmed that the data chunk Ci has not been altered or tampered with.

4) Verifying File and Message Integrity: Hashes ensure the integrity of transmitted messages and information by preventing unauthorized alterations. The practice establishes a "chain of trust". Users have the ability to release a hashed representation of their data together with the corresponding key. This allows recipients to verify the integrity of their data by comparing the hash value they compute with the published value.

5) Advanced Smart Contract Implementations for Transactions: Smart Contracts are essential for automating and ensuring compliance with the conditions of agreements between renters. Our system integrates sophisticated Smart Contract implementations to simplify and automate intricate transaction procedures. Smart Contracts enforce predetermined norms and conditions, guaranteeing the smooth, secure, and compliant execution of data transactions. This not only decreases the requirement for human intervention but also improves the effectiveness and dependability of transactions inside the multi-tenant system. A smart contract SCi is created for each transaction through Eq. (9) as follows:

$$SC_i = \{H_i, Sign_i, \sigma, \gamma, Term_i\} \tag{9}$$

Where σ and γ are the security and compliance parameters and Termi is the terms and conditions specified for the data transaction. Now deploy this SCi in the blockchain through the following Eq. (15):

$$B \leftarrow B \cup \{SC_i\} \tag{10}$$

6) Dynamic Network Creation: In order to overcome the difficulties related to fixed network structures, we suggest the adoption of a Dynamic Network Creation technique. Tenants have the opportunity to connect and disconnect from the network as required, offering adaptability and scalability. The process of creating a dynamic network allows tenants to easily adjust to changing needs, resulting in a flexible and responsive multi-tenant environment. This strategy addresses the problems associated with inflexible network setups, enhancing the system's ability to adapt to the changing requirements of tenants.

Establishing a dynamic network in a multi-tenant blockchain system entails overseeing numerous autonomous tenants, such as distinct businesses or users, and enabling them secure and scalable interaction within the blockchain network. This can be accomplished through the utilization of a synergistic integration of intelligent agreements, dynamic node allocation, and robust communication protocols. Presented here is a mathematical framework for such a system:

During dynamic node allocation, Nodes Nm is allocated to tenants Tm depending upon several criteria like load, requirement, etc. This is done by Eq. (11):

$$N_{T_m} = \{N_m | N_m is assigned to T_m\} \tag{11}$$

To prevent bottlenecks, it is important to evenly distribute nodes among tenants. This is done by Eq. (12):

$$\sum\nolimits_{m=1}^{i} = \frac{load(N_m)}{i} \approx \frac{Totalload}{m} \tag{12}$$

Then deploy the created smart contract to the multitenant blockchain model Bm. Then the Tenants submit transactions TXm which are validated by smart contracts by the following Eq. (13) and (14):

$$TX_m = \{Sender = T_m, Receiver, data, signature\} \tag{13}$$

$$Valid(TX_m) \Leftrightarrow Verif(TX_m, SC_i) \tag{14}$$

Finally, the network graph g (Tm, Nm) is adjusted to the changing load and new tenants through the Eq. (15):

$$g(T_m, N_m) \rightarrow g(T_m^{'}, N_m^{'}) \tag{15}$$

This mathematical framework supports the creation of a flexible, scalable, and secure dynamic network for multi-tenant blockchain applications in healthcare or other sectors.

D. Data Transaction Architecture

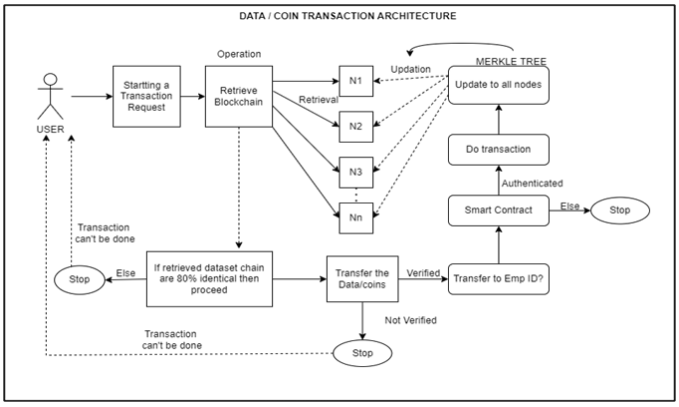

Fig. 6. Data transaction architectures block diagram.

For the purpose of ensuring redundancy and mirrored storage, data is consistently stored in RAID 1 sets. RAID 0 striping is a method that enhances speed by distributing data in an equitable manner across many drives. It is the Monitoring AI that oversees the whole system, ensuring that it operates at its highest possible level. Significant occurrences are gathered and encrypted by the log storage system in a safe manner for the purpose of subsequent reference and analysis. The block diagram of the data transaction architecture of the proposed model is shown in the Fig. 6.

1) Data Transaction and Protocols of Key Generation: The proposed technology integrates data transactions with methods for key generation to bolster the security and privacy of data transactions. Every transaction is linked to a cryptographic currency, and the key generation procedures guarantee secure communication among users. This not only enhances security but also enables the tracking and responsibility of data flows. The utilization of cryptographic coins and resilient key generation procedures enhances the overall security stance of the multi-tenant system.

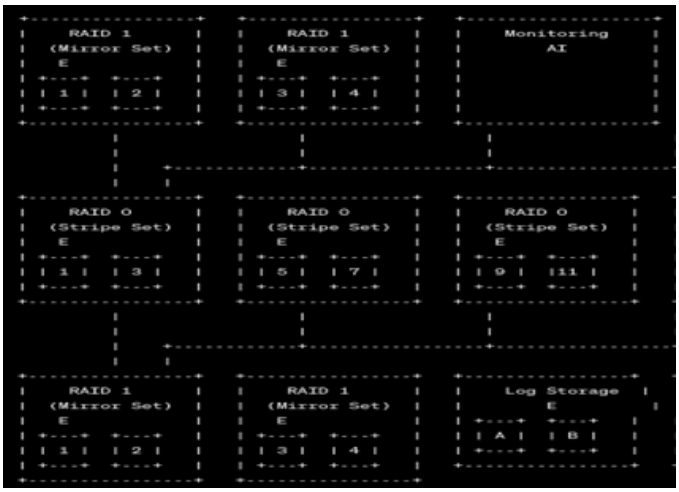

Fig. 7. Chunks with RAID encryption model.

2) Chunks with Raid Concept Encryption: When setting up a chunk-based RAID system, it is standard practice to follow the procedures outlined below: Split the data into i number of Chunks. Choose an appropriate chunk size based on the workload and characteristics of the data. Select the RAID level that optimally meets the requirements for both performance and redundancy. Ensure the disks are ready for use in the RAID array by properly formatting and initializing them. Use RAID management software or hardware to create the RAID array, specifying the appropriate chunk size and RAID level as shown in the Fig. 7. When data is written to the RAID array, it is divided into smaller segments and distributed among the disks according to the chosen RAID level.

Our solution utilizes the concept of Chunks with RAID (Redundant Array of Independent Disks) for encrypting and managing a huge number of database items. This strategy maximizes storage economy while ensuring fault tolerance. Data is divided into smaller segments called chunks, and the RAID idea guarantees both redundancy and reliability. Data security is enhanced by encrypting each piece separately. This approach not only streamlines the administration of an increasing number of tenants but also guarantees the security and accessibility of data through duplication and encryption. Our system utilizes Blockchain Technology, Smart Contracts, dynamic network formation, coin transactions with key generation protocols, and chunks with RAID concept encryption to transform the multi-tenant database design. This comprehensive method tackles issues related to security, scalability, and adaptability, offering a strong basis for a contemporary and effective multi-tenant system.

RAID 1 (Mirror Sets): There are several RAID 1 (mirror) sets indicated by the first and second rows. Each RAID 1 set comprises two drives that replicate each other, ensuring redundancy. Each RAID 1 block contains a "E" which signifies encryption, suggesting that the data saved on these mirrored sets is encrypted.

RAID 0 (Stripe Sets): The third row comprises RAID 0 (stripe) sets, which enhance performance by striping data across the RAID 1 sets. Each RAID 0 set comprises two drives, and the "E" denotes encryption for the striped data.

Monitoring AI: The central "Monitoring AI" block symbolizes an artificial intelligence system that oversees the entire RAID arrangement. This AI system has the responsibility of monitoring and managing the health, performance, and security of the storage system.

Log Storage: There are two "Log Storage" blocks in the last row, each containing its own pair of mirrored drives. Each log storage block is encrypted, as shown by the "E". Storing logs is essential for documenting events, faults, and activities in the storage system, which helps with diagnosing and resolving issues.

3) Advantages of chunk-based raid encryption:

- **Enhanced Efficiency:** By dividing data chunks across many drives, read and write operations may be executed simultaneously, resulting in improved overall performance.
- **Data Redundancy:** Chunk-based RAID offers different levels of data redundancy, which helps guard against disk failures.
- **Scalability:** RAID systems can be extended by including more disks into the array, augmenting storage capacity and perhaps enhancing performance.

III. Results and Discussion

We assess the efficacy of the chunk-based RAID Encryption scheme in the context of a sole data owner, specifically focusing on the operations of data encryption, token generation, query generation, search, decryption, and verification. This is implemented using the VSCode $(Version 1.89.1)$.

A. Data Encryption Assessment

With this encryption system, the data is broken down into smaller parts and each piece is securely encrypted before being sent, guaranteeing that transactions are protected and cannot be intercepted. By analyzing this technique, it becomes clear that the effectiveness of chunk-based RAID encryption is impacted by the size of the chunks and the total number of chunks. The encryption process duration Te can be affected by factors such as the data size D, the number of chunks Ci, and the computational complexity CXe as shown in the Eq. (16):

$$T_e = CX_e. \mid D \mid \tag{16}$$

Thus the encryption time for each block is calculated as follows:

$$T_{(e,block)} = CX_e.B \tag{17}$$

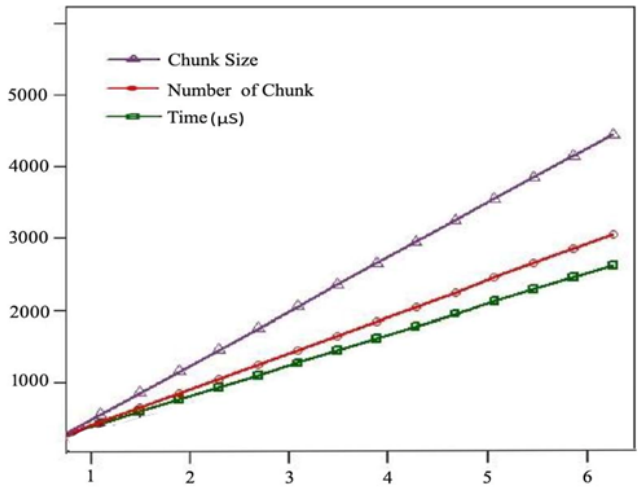

Fig. 8. Data encryption assessment graph.

It is evident from the graph shown in Fig. 8, the encryption progressively grows as the quantity of the data increases and stays within the lowest number that is feasible.

B. Decryption Assessment

The decryption phase consists of two distinct phases. The first stage entails deciphering the encrypted identities of the papers, while the following step concentrates on decrypting the encrypted documents themselves. The encrypted document identities and documents are decrypted with a symmetric decryption technique. After examining the data, it is clear that the size of the obtained result is directly related to the size of the dataset. The decryption process duration Td can be affected by factors such as the data size D, the number of chunks Ci, and the computational complexity CXd as shown in the Eq. (18):

$$T_d = CX_d. \mid D \mid \tag{18}$$

Thus the decryption time for each block is calculated as follows:

$$T_{(d,block)} = CX_d.B \tag{19}$$

Thus the decryption increases gradually with the increased data size and sticks to the minimum possible value within the limits.

C. Assessing the Verification Process

The verification process is utilized to ascertain the accuracy and entirety of the recovered papers. Based on the results, we can see that the verification performance is minimally impacted by the amount of the received result. The verification technique takes around 0.0001 seconds to complete because to the high efficiency of SHA-256 [41].

D. Explorations Involving Multiple Data Owners

Blockchain facilitates the involvement of multiple data owners. In this study, we evaluated the efficacy of the recommended technique, which only involved a single data owner. When multiple individuals or entities possess data, there is a notable discrepancy in the processes of generating encryption keys and performing encryption. The time required for key generation remains the same, regardless of the number of data owners. To perform a search across data owners, the client must obtain authorization from each individual data owner. This results in the creation of a large number.

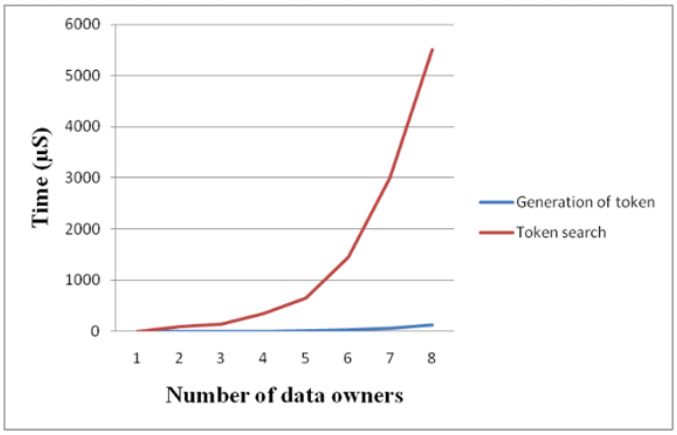

Fig. 9. Performance of multi owners in terms of generation and search tokens.

of tokens. Utilizing tokens enables a focused search operation on data that has been granted authorized access, as opposed to looking over the entirety of the data. To evaluate the effectiveness of the token generation and search algorithm, we execute them on 2, 4, 8, 16, and 32 data owners who authorize a client to access their data. Every data owner has a dataset containing 3125 keywords and 412,477 documents. The results are depicted in Fig. 9. The figure clearly demonstrates that as the number of data owners increases, both the time needed for token production and search both increase in a rather linear fashion. However, the time needed for token manufacturing is small in comparison to the time spent on the search process.

E. Latency

Chunk-based RAID encryption causes slowness owing to inherent factors in data processing and protection. Every segment of data must undergo encryption before being written to the RAID array, and decryption before being read. The intricacy and processing requirements of the encryption technique, such as AES, have a direct impact on the latency. RAID levels that employ parity, such as RAID 5 or RAID 6, necessitate extra computations to determine and confirm parity information. This procedure has the potential to cause delays, particularly when used in conjunction with encryption. Concurrency in disk operations can lead to increased latency, especially when the RAID controller is required to handle numerous simultaneous tasks across multiple disks. The delay can be influenced by the size of the data chunks utilized in the RAID arrangement. Using smaller chunks can result in more frequent encryption and parity calculations, while larger chunks may decrease these additional tasks but could introduce other inefficiencies. The efficiency of the RAID controller in handling encryption and parity computations has a considerable impact on total delay. In Network attached

storage systems, network latency can impact the performance, especially when data needs to be transmitted across a network and then encrypted before being stored in the RAID array.

The latency in encryption, specifically in the context of chunk-based RAID encryption, can be determined by taking into account multiple factors: data splitting and distribution, encryption processing, disk I/O operations, and possibly network delays. Below is a universal equation for determining the overall latency:

$$L_{Total} = L_{Split} + L_{Encrypt} + L_{(Disk_{io})} + L_{Network} \quad (20)$$

Where: L_{Split} = Latency due to data splitting and distribution
$L_{Encrypt}$ = Latency due to encryption processing
L_{diskio}= Latency due to disk I/O operations
$L_{Network}$ = Latency due to network transmission.

Latency caused by data splitting and distribution refers to the duration required to partition the data into segments and disperse them among many drives. The outcome is contingent upon the size of the data chunks (C), the quantity of disks (Dn), and the efficacy of the RAID controller. This is given by the Eq. (21):

$$L_{Split} = f(C, D_n) \quad (21)$$

Latency caused by encryption processing encompasses the duration required to encrypt individual portions of data. The time required for encryption depends on factors such as the specific encryption technique employed (AES-256), the size of the data chunk (C), and the processing capacity (CPU speed). This is given by the Eq. (22):

$$L_{Encrypt} = \sum_{(i=1)}^{n} (\frac{c_i}{B_{encrypt}}) + O_{Encrypt} \quad (22)$$

Where: n = Number of chunks
C_i = Size of the ith chunk
$B_{Encrypt}$ = Encryption bandwidth (throughput, e.g., MB/s)
$O_{Encrypt}$ = Overhead associated with the encryption process (initialization, padding, etc.)

Latency caused by disk I/O activities refers to the duration required for read and write operations on the physical disks. This latency is influenced by factors such as the kind of disk (HDD or SSD), the RAID level, and the read/write speed of the disks. This is given by the Eq. (23):

$$L_{diskio} = \sum_{i=1}^{n} (\frac{C_i}{B(disk_{io}} + O_{diskio} \quad (23)$$

Where: B_{diskio} = Disk I/O bandwidth (throughput, e.g. MB/s)

$O_{disk_{io}}$= Overhead associated with disk I/O operations (seek time, rotational latency, etc.)

Latency due to network transmission includes the time taken to transmit data over a network and depends on the network bandwidth and latency. This is denoted by the Eq. (24).

$$L_{network} = \sum_{i=1}^{n} (\frac{C_i}{B_{network}}) + O_{network} \quad (24)$$

Where $O_{network}$ = Overhead associated with network transmission (latency, packet loss, etc.)

The data size is 1 MB, divided into 10 pieces. The encryption bandwidth is 50 MBpS, the disk I/O bandwidth is 100 MBpS, and the network bandwidth is 100 MBpS. Assuming LSplit is negligible or already included in other components The assumed overhead is 0.01S. The calculated total loss is

$$LTotal = 0.21 + 0.11 + 0.11 = 0.43s$$

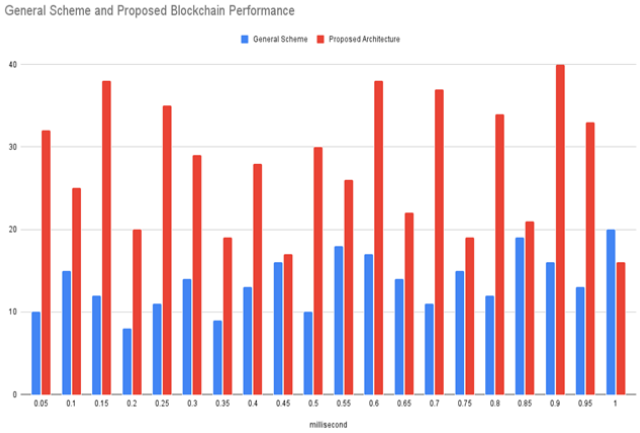

Fig. 10. Graph illustrating the latency between the general and proposed blockchain model.

Within a typical multitenant setting, the retrieval and manipulation of data may experience delays, which can hinder the efficiency of activities. Our secure blockchain multi-tenancy utilizes the decentralized and distributed characteristics of blockchain technology to greatly decrease latency. The technology reduces the time required for data transactions to be vetted and recorded by distributing the data across a secure and unchangeable ledger. The recorded values are plotted in the graph as shown in Fig. 10. The color blue symbolizes the duration of delay retrieval, while the color red indicates the data obtained from a generic tenant. The time output of the executed and processed data demonstrates that our proposed system has a shorter processing and retrieval time for data and outcomes.

F. Bruteforce Attack Vulnerability Assessment

A brute force attack on healthcare data security entails an assailant methodically attempting every conceivable combination of passwords or encryption keys until they successfully discover the proper one. The consequences of such an attack on healthcare data can be significant, considering the delicate nature of the information at stake. Engaging in a brute force attack against healthcare data security can result in severe outcomes, such as unauthorized access to data, fraudulent use

of personal information, disruption of operations, and substantial financial expenses. To effectively mitigate the risks of brute force attacks and safeguard sensitive patient information, healthcare organizations should employ robust authentication mechanisms, enforce account lockout policies, utilize encryption, monitor systems for suspicious activity, and educate users.

Brute force attacks, which involve attackers methodically attempting every conceivable combination to bypass encryption, pose substantial difficulties with chunk-based RAID encryption methods based on blockchain technology. The intrinsic intricacy of these systems introduces multiple levels of susceptibility that necessitate meticulous attention. To address vulnerabilities to brute force attacks in blockchain-based chunk-based RAID encryption methods, a comprehensive and multi-faceted strategy is necessary. Organizations can greatly mitigate the likelihood of successful brute force attacks by implementing powerful encryption algorithms, effective key management, and advanced security measures. Conducting regular security evaluations and keeping up-to-date with the newest cryptographic breakthroughs are crucial for maintaining a safe environment.

In this framework Chunk based encryption, has offered a key space of 256. Due to the existing computational capabilities, it is deemed impractical to forcefully determine a single key. Nevertheless, in the event that a malicious individual specifically focuses on the RAID parity data or endeavors to carry out a brute-force attack on numerous portions, the system's decentralized structure and duplication could unintentionally assist the attacker. To limit the possibility of a brute-force attack, the system has employed distinct Initialization vectors for each chunk and enforce robust key management policies. In addition, anomaly detection techniques have the ability to recognize and react to abnormal access patterns, hence improving security measures.

G. Comparison with Other Encryption Technologies

When evaluating the effectiveness of chunk-based RAID encryption in healthcare blockchain security, it is crucial to comprehend the distinct functions that cryptographic algorithms such as SHA-3 [31], SHA-256 [32], and AES [33] serve in safeguarding data.SHA-3 is a cryptographic hash function employed for the purpose of guaranteeing the integrity of data. SHA-3 generates a distinct hash of a specific size based on the input data, facilitating the identification of any modifications. This system is designed to be impervious to collision attacks, guaranteeing that no two distinct inputs will yield the same hash value. Frequently employed in blockchain technology to generate digital signatures and guarantee the unchangeability of transactions. SHA-3 is designed only for ensuring data integrity and performing cryptographic operations, as opposed to being used for purposes such as data redundancy or optimizing performance, like RAID. Primarily used to guarantee the authenticity and reliability of transactions and data blocks in blockchain, rather than focusing on safeguarding physical storage.

SHA-256 is a prevalent cryptographic hash function that finds extensive application in blockchain technology, such as in Bitcoin. Like SHA-3, it generates a hash of a specific size to guarantee the integrity of data. Additionally, it is impervious to both collision and preimage strikes. Essential for the creation of digital signatures, the process of hashing transactions, and the interconnection of blocks in a blockchain. Similar to SHA-3, it prioritizes data integrity above storage redundancy. Crucial for the functioning of blockchain processes, such as verifying transactions and creating blocks, but not suitable for safeguarding storage systems.

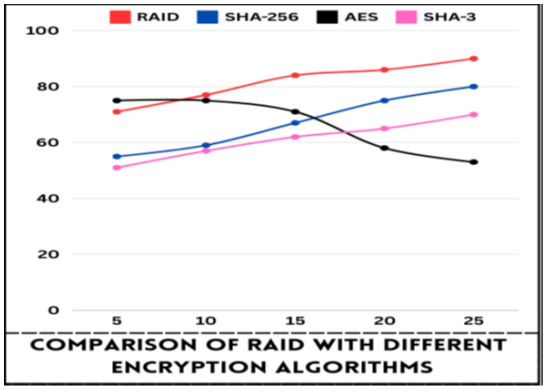

Fig. 11. Comparison of the proposed model with the existing models.

AES is a cryptographic technique that employs symmetric encryption to safeguard the secrecy of data. Robust encryption utilizing several key sizes (128, 192, 256 bits) Highly effective encryption and decryption procedures, applicable to both stationary and moving data. Can be utilized to employ cryptographic techniques to secure confidential information prior to its storage on the blockchain or transmission over the networks. AES primarily emphasizes the encryption of data to guarantee confidentiality, while RAID primarily emphasizes data redundancy and performance. AES is employed to safeguard the factual data content, hence enhancing RAID encryption's ability to maintain data confidentiality even in the event of unauthorized access.

Encryption of RAID using chunk-based methodology. Offers both data redundancy and performance advantages while ensuring data security while it is not actively being used. While SHA-3 and SHA-256 do not offer encryption or redundancy, they must be utilized with encryption algorithms to ensure comprehensive security. AES does not offer data redundancy or integrity. It is most effective when used in conjunction with hashing techniques to ensure comprehensive security.

The accuracy of the encryption/hashing techniques listed above is especially evaluated in comparison to the "RAID Chunk Encryption/Storage Concept". The accuracy was assessed across 25 encryption cycles, and the findings are depicted in the graph in Fig. 11.

From the graph, it is evident that the proposed system outsmarts the other existing encryption systems in terms of performance and accuracy. Chunk-based encryption in a RAID setup means each chunk or block of data stored across the RAID array is encrypted separately. This can enhance security by ensuring that even if one chunk is compromised, the entire dataset remains secure. When combined with encryption, it adds an additional layer of security, ensuring data integrity and confidentiality.

The efficiency of current multi-tenant healthcare data management approaches is hampered by a number of issues. Due to inadequate data separation, single database designs with common schemas are vulnerable to security breaches. Scalability is still a problem as data and user volumes increase, and maintaining several schemas or databases adds a great deal of expense and complexity. Additionally, a lot of conventional systems don't have strong fault tolerance methods, which makes data unavailable when hardware fails. Furthermore, because they lack immutable recording or verification systems like blockchain, they are unable to guarantee data integrity and transparency, making them unsuitable to satisfy the strict security and compliance requirements of the healthcare industry.

IV. Conclusion

Healthcare enterprises possess the capacity to create a robust, flexible, and dynamic framework that meets their evolving needs while maintaining high levels of performance and security. In order to tackle the challenges posed by multi-tenancy database systems, we propose a novel approach that leverages the dynamic organization of tenant connections and integrates blockchain technology to overcome these problems. Our approach employs the use of Chunks with RAID (Redundant Array of Independent Disks) to encrypt and handle a large quantity of database items. This approach optimizes storage efficiency while guaranteeing resilience against failures. This complete approach addresses concerns pertaining to security, scalability, and adaptability, providing a solid foundation for a modern and efficient multi-tenant system.

Thus, the approach that has been proposed offers robust data redundancy and fault tolerance, making it suited for ensuring high availability, even with increased complexity. This approach also exhibits efficient scalability with the inclusion of extra disks, possibly at the cost of increased intricacy.

References

[1] Khan, A. A., Bourouis, S., Kamruzzaman, M. M., Hadjouni, M., Shaikh, Z. A., Laghari, A. A., ... & Dhahbi, S. (2023). Data security in healthcare industrial internet of things with blockchain. IEEE Sensors Journal.

[2] Al Zaabi, M., & Alhashmi, S. M. (2024). Big data security and privacy in healthcare: A systematic review and future research directions. Information Development, 02666669241247781.

[3] Sharma, A., & Kaur, P. (2023). Tamper-proof multitenant data storage using blockchain. Peer-to-peer Networking and Applications, 16(1), 431-449.

[4] Rai, B. K. (2022). Security Issues and Solutions for Healthcare Informatics. In Federated Learning for IoT Applications (pp. 185-198). Cham: Springer International Publishing.

[5] Sharma, A., & Kaur, P. (2023). A survey of distributed data storage in the cloud for multitenant applications. International Journal of Performability Engineering, 19(3), 184.

[6] Almalki, J. (2024). State-of-the-art research in blockchain of things for healthcare. Arabian Journal for Science and Engineering, 49(3), 3163-3191.

[7] Mathivanan, P., MohanaPriya, D., Manjula, P., & Ouaissa, M. (2024). Protecting the Privacy of IoT-Based Health Records Using Blockchain Technology. In Technological Advancement in Internet of Medical Things and Blockchain for Personalized Healthcare (pp. 127-144). CRC Press.

[8] Vaiyapuri, T., Shankar, K., Rajendran, S., Kumar, S., Acharya, S., & Kim, H. (2023). Blockchain assisted data edge verification with consensus algorithm for machine learning assisted IoT. IEEE Access.

[9] Pittaras, I., & Polyzos, G. C. (2023, November). Multi-tenant, Decentralized Access Control for the Internet of Things. In 2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS) (pp. 28-34). IEEE.

[10] Dhasaratha, C., Hasan, M. K., Islam, S., Khapre, S., Abdullah, S., Ghazal, T. M., ... & Akhtaruzzaman, M. (2024). Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things. CAAI Transactions on Intelligence Technology.

[11] Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. Sensors, 23(21), 8944.

[12] Malik, H., Anees, T., Faheem, M., Chaudhry, M. U., Ali, A., & Asghar, M. N. (2023). Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions. Internet of things, 100860.

[13] Gupta, B. B., Prajapati, V., Nedjah, N., Vijayakumar, P., El-Latif, A. A. A., & Chang, X. (2023). Machine learning and smart card based two-factor authentication scheme for preserving anonymity in telecare medical information system (TMIS). Neural Computing and Applications, 35(7), 5055-5080.

[14] Li, K., Lee, J. Y., & Gharehgozli, A. (2023). Blockchain in food supply chains: a literature review and synthesis analysis of platforms, benefits and challenges. International Journal of Production Research, 61(11), 3527-3546.

[15] Shahaab, A., Khan, I. A., Maude, R., Hewage, C., & Wang, Y. (2023). Public service operational efficiency and blockchain–A case study of Companies House, UK. Government Information Quarterly, 40(1), 101759.

[16] Chee, T. H., & Rana, M. E. (2023, January). An Exploratory Study on the Impact of Hosting Blockchain Applications in Cloud Infrastructures. In 2023 15th International Conference on Developments in eSystems Engineering (DeSE) (pp. 381-386). IEEE.

[17] Dhiman, P., Henge, S. K., Singh, S., Kaur, A., Singh, P., & Hadabou, M. (2023). Blockchain Merkle-Tree Ethereum Approach in Enterprise Multitenant Cloud Environment. Computers, Materials & Continua, 74(2).

[18] Albassam, A., Almutairi, F., Majoun, N., Althukair, R., Alturaiki, Z., Rahman, A., ... & Mahmud, M. (2023). Integration of Blockchain and Cloud Computing in Telemedicine and Healthcare. IJCSNS, 23(6), 17-26.

[19] Sayal, A., Jha, J., & Chaithra, N. (2024). Blockchain: A Digital Breakthrough in Healthcare. In Blockchain for Healthcare 4.0 (pp. 1-25). CRC Press.

[20] Gupta, M., & Dwivedi, R. K. (2023). Blockchain-Based Secure and Efficient Scheme for Medical Data. EAI Endorsed Transactions on Scalable Information Systems, 10(5).

[21] Masri, D., Jaber, L., Mashal, R., Albourini, F., Alsaoud, M. A., & Al-Tarawneh, A. M. (2024, February). The Role of Wearables & Technology in Mental Health. In 2024 2nd International Conference on Cyber Resilience (ICCR) (pp. 1-5). IEEE.

[22] Alrashdi, I., & Alqazzaz, A. (2024). Synergizing AI, IoT, and Blockchain for Diagnosing Pandemic Diseases in Smart Cities: Challenges and Opportunities. Sustainable Machine Intelligence Journal, 7, 6-1.

[23] Khan, R. U., Kumar, R., Haq, A. U., Khan, I., Shabaz, M., & Khan, F. (2024). Blockchain-Based Trusted Tracking Smart Sensing Network to Prevent the Spread of Infectious Diseases. IRBM, 45(2), 100829.

[24] Verma, P., Rao, C. M., Chapalamadugu, P. K., Tiwari, R., & Upadhyay, S. (2024). Future of Electronic Healthcare Management: Blockchain and Artificial Intelligence Integration. In Next-Generation Cybersecurity: AI, ML, and Blockchain (pp. 179-218). Singapore: Springer 25ture Singapore.

[25] Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2023). Blockchain and COVID-19 pandemic: Applications and challenges. Cluster Computing, 26(4), 2383-2408.

[26] Jabbar, R., Fetais, N., Krichen, M., Kaoui, K. (2020, February). Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 310-317). IEEE.

[27] Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information processing & management, 58(3), 102535.

[28] Ikuomola, A. J., & Owoputi, K. S. (2024). Development of a Secured and Interoperable Multi-Tenant Software-as-a-Service Electronic Health Record System. In Intelligent Data Analytics, IoT, and Blockchain (pp. 286-301). Auerbach Publications.

[29] Raouf, A. E. A., Abo-Alian, A., & Badr, N. L. (2021). A predictive multi-tenant database migration and replication in the cloud environment. IEEE Access, 9, 152015-152031.

[30] Kuznetsov, A., Oleshko, I., Tymchenko, V., Lisitsky, K., Rodinko, M., & Kolhatin, A. (2021). Performance analysis of cryptographic hash functions suitable for use in blockchain. International Journal of Computer Network & Information Security, 13(2), 1-15.

[31] Susanto, H., Ibrahim, F., Rosiyadi, D., Setiana, D., Susanto, A. K. S., Kusuma, N., & Setiawan, I. (2022). Securing Financial Inclusiveness Adoption of Blockchain FinTech Compliance. In FinTech Development for Financial Inclusiveness (pp. 168-196). IGI Global.

[32] Itnal, S., Kannan, K. S., Suma, K. G., & Neelakandan, S. (2022, May). A secured healthcare medical system using blockchain technology. In ICCCE 2021: Proceedings of the 4th International Conference on Communications and Cyber Physical Engineering (pp. 169-176). Singapore: Springer Nature Singapore.

[33] Gabriel, S. J., & Sengottuvelan, P. (2021, October). An enhanced blockchain technology with AES encryption security system for healthcare system. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 400-405). IEEE.