Efficient Data Sharing Approach in Blockchain for Smart Healthcare

A thesis submitted to the
UPES

For the award of
Doctor of Philosophy

In

COMPUTER SCIENCE & ENGINEERING

By

Deepak Kumar Sharma

July 2024

Supervisor

Dr. Adarsh Kumar

School of Computer Science (SoCS)

UPES

Dehradun, 248007: Uttarakhand, India

Efficient Data Sharing Approach in Blockchain for Smart Healthcare

A thesis submitted to
UPES

For the award of
Doctor of Philosophy

In

COMPUTER SCIENCE & ENGINEERING

By

Deepak Kumar Sharma

SAP Id: 500055803

July 2024

Supervisor

Dr. Adarsh Kumar

Professor, SoCS

UPES, Dehradun

School of Computer Science (SoCS)

UPES

Dehradun, 248007: Uttarakhand, India

DECLARATION

I declare that the thesis entitled **"Efficient Data Sharing Approach in Blockchain for Smart Healthcare"** has been prepared by me under the guidance of Dr. Adarsh Kumar, Professor, School of Computer Science, UPES, Dehradun. No part of this thesis has formed the basis for the award of any degree or fellowship previously.

Deepak Kumar Sharma
School of Computer Science
UPES
Energy Acres, P.O. Bidholi, via Prem Nagar,
Dehradun, 248007: Uttarakhand, India

UPES
UNIVERSITY OF TOMORROW

Great Place To Work. Certified FEB 2024-FEB 2025 INDIA

CERTIFICATE

I certify that Deepak Kumar Sharma has prepared his thesis entitled **"Efficient Data Sharing Approach in Blockchain for Smart Healthcare",** for the award of PhD degree of the UPES, under my guidance. He has carried out the work at the School of Computer Science, UPES.

16/07/24

Supervisor
Dr. Adarsh Kumar
Professor
School of Computer Science
UPES Dehradun
Uttarakhand

ABSTRACT

An Electronic Health Record (EHR) is a digital system crucial for improving collaboration among healthcare providers, training, and research. Given their sensitive nature, securing EHRs is a critical challenge. This study proposes a robust system using blockchain technology to enhance EHR security and integrity. Blockchain's decentralized structure, immutability, and non-repudiation make it an ideal solution, ensuring no single authority controls the system and data cannot be tampered with, thus building trust in medical record storage and sharing.

The first study introduces a Distributed Zero Trust-based Blockchain Structure (DZTBS), combining smart contracts with a zero-trust framework to secure data sharing. This approach ensures data integrity, availability, and confidentiality. DZTBS demonstrates significant improvement over existing methods in managing delays. Its consistent effectiveness across diverse network complexities highlights its reliability and efficiency.

The second study proposes a data sharing and retrieval method within a blockchain framework designed for smart healthcare systems. This method addresses data management, security, and accessibility challenges using a distributed data-sharing scheme and an innovative retrieval algorithm with Merkle-Patricia Trie (MPT) and Bloom filters. The system shows improved performance in upload/download times, latency, delay, and response times, promising enhanced patient care and data analytics.

The third study presents a novel EHR access solution in a blockchain-based healthcare system. Key components include Redis caching, an Adaptive Balanced Merkle (AB-M) tree, and a lattice-based ring signature system. These elements provide a secure and efficient foundation for a smart healthcare ecosystem. Testing reveals outstanding performance, with rapid upload and download times, significantly better than traditional methods. The integration of Redis caching further enhances system speed, showcasing the potential to revolutionize EHR retrieval in smart healthcare.

Overall, these studies demonstrate the significant benefits of using blockchain technology in healthcare, improving EHR management through enhanced security, efficiency, and data accessibility.

Keywords: Electronic Health Record, Blockchain, Security, Data sharing, Decentralized structure, Data integrity, Smart healthcare.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the following people and institutions for their invaluable support and guidance throughout my PhD journey.

First and foremost, I am incredibly grateful to my guide, Dr. Adarsh Kumar, for his constant guidance, encouragement, and expertise. His belief in my work and willingness to dedicate his time has been instrumental in shaping this thesis. Further, I would also like to thank my doctoral committee members for their insightful feedback and suggestions that significantly improved the quality of this thesis. Additionally, I am thankful to the School of Computer Science and UPES for providing me with the resources and opportunities to conduct my research. My deepest gratitude goes to my parents, spouse and kids, Shivansh and Dhruvika, for their unwavering love, support, and encouragement throughout my PhD studies. I would also like to thank my friends, for their friendship and understanding, and for providing me with a much-needed break when needed.

Deepak Kumar Sharma
UPES Dehradun
July 2024

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Adaptive Balanced Merkle	AB-M
Adaptive Balanced MT	AB-M tree
Advanced Encryption Standard	AES
Advancement Data Security Architecture in Healthcare Environment	ADSAH
Auditable and Privacy Preserving Health QR Code	APHC
Big Healthcare Data	BHD
Binary Tree	BT
Blockchain based Privacy Preserving and Robust Healthcare Data	BPPRH
Blockchain Technology	BCT
Blockchain-based IoMT Security System	BC-IoMT-SS
Blockchain-Based Zero Knowledge Proof	BKZP
Computed Tomography	CT
Content Identifiers	CIDs
Deep Fuzzy-Based Neural Network	DFBNN
Differential Privacy	DP
Dilated Transaction and Retrieval Method	DTARM
Distributed Zero Trust-based Blockchain Structure	DZTBS
Dual Policy Attribute Based Encryption	DP-ABE
Dynamic Joining and Exiting Protocol	DJEP
Edge-Cloud-based Collaborative System	ECCS
Efficient Byzantine Reputation-based Consensus	EBRC
Electronic Health Records	EHR
Electronic Medical Records	EMR
Elliptic Curve Cryptography	ECC
Elliptic Curve Digital Signature Algorithm	ECDSA

Extended Lightweight Blockchain	ELB
Federated Learning	FL
General Data Protection Regulation	GDPR
Generative Adversarial Networks	GANs
Health Information Exchanges	HIEs
Hyperledger Fabric	HLF
Identity-Based Proxy Re-Encryption	IB-PRE
Information and Communication Technology	ICT
Internet of Medical Things	IoMT
Internet of Things	IoT
Interplanetary File System	IPFS
Keyword-Based Re-Encryption	KRE
Local Differential Policy	LDP
Medical Information System	MIS
Modified Fuzzy Particle Swarm Optimization	MFPSO
Multi-Transaction Mode Consortium Blockchain	MTMCB
Oblivious Transfer-Based Re-Encryption	OTRE
Overlay Block Managers	OBM
Personal Health Record	PHR
Proof of Authority	PoA
Proof of Work	PoW
Registration Centre	RC
Regulatory Node System	RNS
Secure Health Networks	SHNs
Service Level Agreements	SLAs
Wireless Sensor Network-based IoT	WSN-IoT
Zero Trust Architecture	ZTA
Zero Trust Network Architecture	ZTNA
Zero Trust eXtended	ZTX

CHAPTER 1
INTRODUCTION

Blockchain is a digital database where data is cryptographically encrypted, validated, and managed over a decentralized network of computers by adopting a consensus process [1]. This integration enhances trust and confidentiality inside the existing internet infrastructure. Uniquely, blockchain functions at a cheaper cost and with better efficiency by eliminating redundancy and lessening dependency on intermediaries, thus minimizing operational expenses over non-blockchain systems. Its security features, leveraging known validation models, ensure transactions are secured, validated, and auditable, making it less prone to breaches and fraudulent activity. When implemented as a permissioned network, it checks members' identities, assuring correctness in transaction exchanges. Moreover, Blockchain Technology (BCT) increases privacy [2] by enabling users to define the specifics of transactional facts exposed to other participants through credentials and permissions. This flexibility extends to specialist users, like auditors, who may demand greater insights into transactional information, etc.

1.1 MAJOR ATTRIBUTES OF BLOCKCHAIN TECHNOLOGY

The blockchain technology is composed of mainly six attributes:

- **Decentralized**: The decentralized structure of blockchain using a peer-to-peer architecture reduces the need for a central server [3] thus ensuring that all participating machines have equal status and contribute resources collaboratively. As the number of machines increases inside this framework, the potential for quicker communications expands, leading to an overall enhancement of in-service performance. This distributed network approach encourages a durable and efficient framework for information transmission and validation.
- **Transparent:** A key element of blockchain technology is transparency, which guarantees that information recorded in the system is accessible to and seen by all pertinent parties. This transparency builds confidence and responsibility

inside the network, allowing users to check transactions and information independently. It also promotes integrity, as any discrepancies or fraudulent activity may be immediately discovered by the decentralized community, leading to a more secure and trustworthy ecosystem. Overall, transparency in blockchain provides a shared and tamper-proof record [4] that serves numerous industries, from finance to supply chain management.

- **Open Source:** Open Source within blockchain technology supports the unconstrained development of applications, offering an open ecosystem for innovation and creativity. This flexibility allows varied contributors to design, adapt, and enhance apps, fostering a collaborative ecosystem that feeds on pooled knowledge and skill. The transparent, accessible nature of open-source blockchain supports a broad variety of solutions, empowering developers and organizations to exploit its potential for many industries and use cases.
- **Autonomous:** Autonomy in blockchain, provided by the consensus protocol, ensures that each node has the authority to securely initiate data transfers or updates. By enabling nodes to engage in validating and recording transactions, the system runs autonomously, promoting confidence and reliability in the absence of a unique governing authority. This decentralized architecture ensures a resilient and democratic structure where consensus among nodes dictates the network's integrity and security.
- **Immutable:** Immutability within blockchain technology [5] indicates that any information once contributed to the chain becomes permanent as well as tamper-proof. This robustness originates from the distributed consensus method, ensuring data integrity. Changes to or deletions of recorded data are essentially impossible until a party has control of most of the network nodes, which increases the security and reliability of the system.
- **Anonymity:** Anonymity in blockchain transactions depends exclusively on the knowledge of an individual's blockchain address, effectively splitting up it from the owner's actual IP address. This distinguishing characteristic ensures the appearance of privacy, allowing transactions to be placed without explicitly

revealing the individual's personal identity or physical location [6]. Such separation of the blockchain address from the IP address acts as a critical aspect in protecting anonymity and security within the decentralized network.

1.2 BACKGROUND OF THE RESEARCH

In 2008, Bitcoin marked the arrival of the first decentralized and distributed currency, introduced by an entity known as Nakamoto. Combining 2P networks with digital services, it utilized innovative blockchain technology. Initially applied inside the banking arena, Blockchain’s success led its research beyond varied platforms as shown in Figure 1.1. [7]. Renowned for increasing data transparency and privacy, it has notably developed in the Internet of Things (IoT) arena. Serving as a distributed and decentralized database, blockchain validates and securely stores data. This technique supports the uninterrupted transmission, receiving, and updating of information in a peer-to-peer network, thereby supporting huge volumes of data. Through its methods, blockchain permits decentralized systems to record transactions, stressing worldwide applicability, immutability, and a spectrum of other intrinsic properties. Blockchain technology uses the P2P network as well as the consensus mechanism established by the Bitcoin protocol [6], producing a globally decentralized shared ledger with cryptographic security. The blockchain's consecutive chaining offers solid security qualities such as integrity, stability, and availability, preserving copies of sensitive information across all nodes in the network to prevent loss.

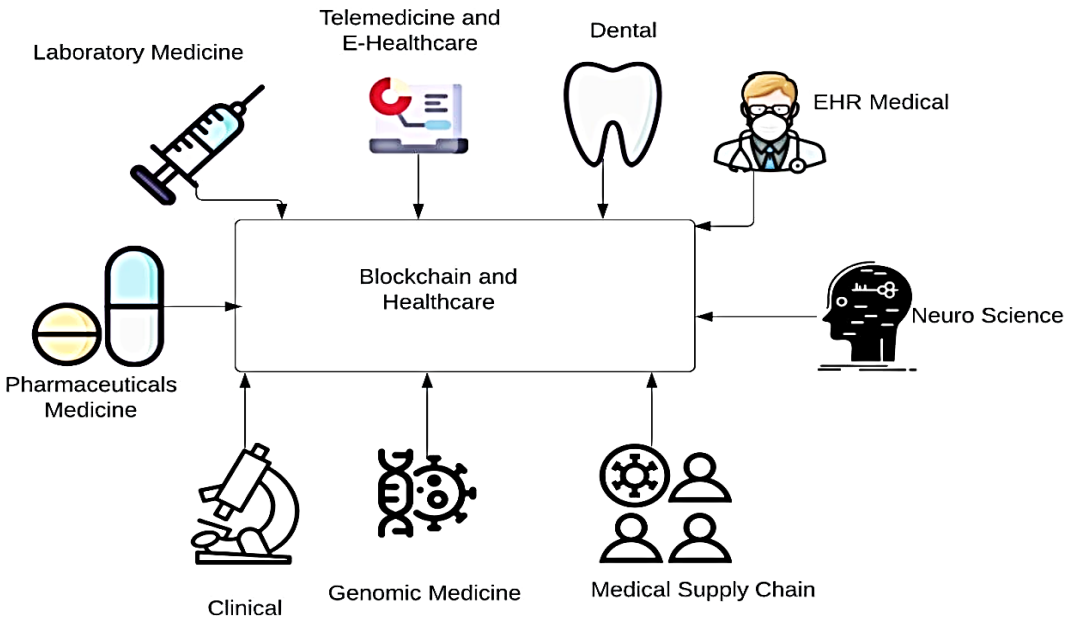

Figure 1.1 Blockchain and Healthcare

1.3 MOTIVATION OF THE RESEARCH

Electronic Health Records (EHRs) are kept in centralized databases across healthcare providers, resulting in a governance system vulnerable to a single point of failure. This configuration results in the fragmentation of health records across numerous entities such as hospitals, health centres, doctors, insurance companies, and wearable devices. This fragmentation poses issues, as patients may fail to effectively communicate information between different medical practitioners, probably leading to inaccurate diagnoses in following encounters. For more accurate diagnoses and successful treatments, an integrated system allowing all stakeholders to view, edit, alter, share, and delete EHRs is important. However, the sensitive nature of healthcare data needs comprehensive security, integrity, and availability protections inside storage methods [8]. Implementing multiple access control levels becomes vital to regulating which entities can access specific sorts of data. Addressing service availability and data immutability is crucial. Therefore, a decision was made to study and construct a user application employing blockchain technology as the backend service to tackle these difficulties.

1.4 TYPES OF BLOCKCHAIN NETWORKS

Blockchain technology connects nodes in a network to verify data and transactions. Blockchains can be classified as authorised or public based on the level of familiarity of the parties involved. Authorized blockchains involve members who are already acquainted with the network, while public blockchains are open to anyone interested in joining. The basic objective of blockchain is to construct and exchange digital ledgers while allowing data transfers inside a P2P network. Users have the potential to handle and validate transactions without the requirement for a central authority. This decentralized strategy considerably cuts expenses connected to arbitration, system modifications, configuration, and maintenance since they are no longer centralized. However, it's worth mentioning that despite its effectiveness, blockchain typically has scaling issues. Blockchain technology can be grouped into several groupings, each with its unique properties, which directly influence the behaviour of the network. These forms of blockchain can be characterized as:

1.4.1 PUBLIC BLOCKCHAIN

A public blockchain runs through transparent transactions accessible to all network nodes. Participation in the blockchain's consensus procedures is open to any node without requiring permission or authentication within the network. This decentralized method allows nodes to validate transactions collectively and at a wide scale, assisting one another in the process. This open contribution ensures the network's security, immutability, and trustworthiness by permitting varied nodes to join in the consensus mechanisms collectively.

1.4.2 PERMISSIONED BLOCKCHAIN

A permissioned blockchain operates under the administration of a certain entity, demanding explicit permission for nodes to participate. This organized environment grants better control over transactions, increasing security and privacy protections. By enforcing authentication for access, it ensures a heightened level of confidentiality within the network. MultiChain stands as an example of a platform

incorporating these traits, providing limited access and giving powerful privacy protocols in blockchain transactions.

1.4.3 CONSORTIUM BLOCKCHAIN

A consortium blockchain, similar to a permissioned blockchain, works under the supervision of a select group, demanding identification for network access. The distinctive aspect of this network is its validation process, managed by a limited number of nodes featuring predetermined features permitting transaction validation. The important part involves these selected nodes achieving a consensus to validate transactions, ending in the formation of a new block, thereby concluding the complete transaction process. This particular paradigm ensures a more controlled and often more efficient validation procedure, increasing the network's integrity and security [9].

1.4.4 SIDECHAINS

Sidechains enable the secure utilization as well as the subsequent transfer of digital assets and tokens to and from the principal chain of the database. Operating autonomously, a sidechain assures its own security and validation standards independently of the main chain. In the event of compromise or failure in the sidechain, the main chain keeps running and the reverse holds. Meanwhile, the main chain might employ a more resource-intensive consensus mechanism, like Proof of Work, to strengthen security. However, sidechains split assets on the ledger, and many asynchronous chains interacting at the network level increase complexity. Additionally, the requirement for federation in sidechains provides an extra layer that could potentially be a vulnerability for attackers. When done correctly, sidechains offer a solution to scalability and interoperability concerns without affecting the blockchain's integrity and security.

1.4.5 OFF-CHAIN TRANSACTION

An off-chain transaction describes the transfer of value occurring outside the principal blockchain network. Utilizing an off-chain state channel entails a bidirectional communication route between users, improving their participation

with the blockchain while minimizing the need for every transaction to be confirmed by a mining process. This strategy dramatically raises transaction throughput and decreases the data stored on the main chain. With this method, a part of the blockchain is momentarily locked using predefined smart contracts or multi-signatures that have been agreed upon by the parties involved. The whole set of transactions is then added to the main database on the chain once each transaction is jointly signed. This strategy tackles many difficulties by boosting transaction speed without compromising security. Moreover, this technique is situated to decrease the cost of transactions by decreasing the demand for thorough validation on the blockchain.

Permissionless blockchains, generally referred to as public blockchains, function without constraints on participation, whereas permissioned blockchains like consortium and private blockchains require specific access or rights to participate. Compared to permissionless competitors, permissioned blockchains provide advantages in speed, implementation ease, and energy efficiency. They promote the deployment of consensus methods beyond energy-intensive solutions. Permissioned blockchains, implementing consensus methods such as Byzantine Fault Tolerance, frequently demonstrate higher throughput compared to the energy-consuming alternatives. As represented in Figure 1.2 [10], a blockchain essentially comprises a consecutive chain of blocks.

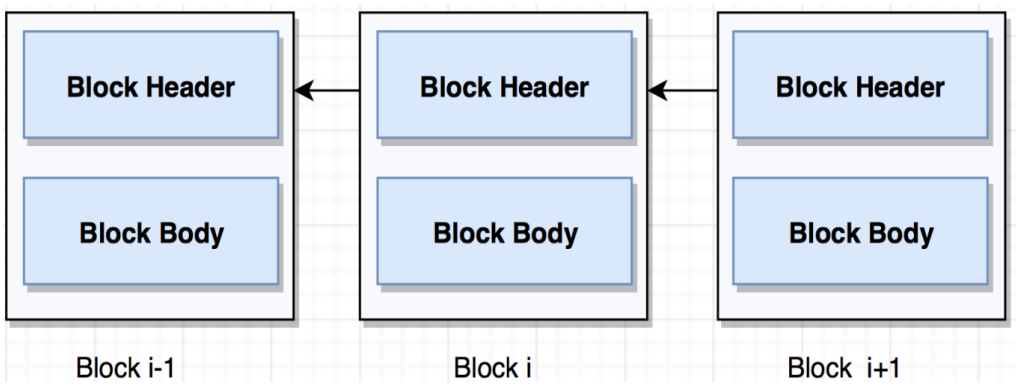

Figure 1.2 Diagrammatical representation of Blockchain

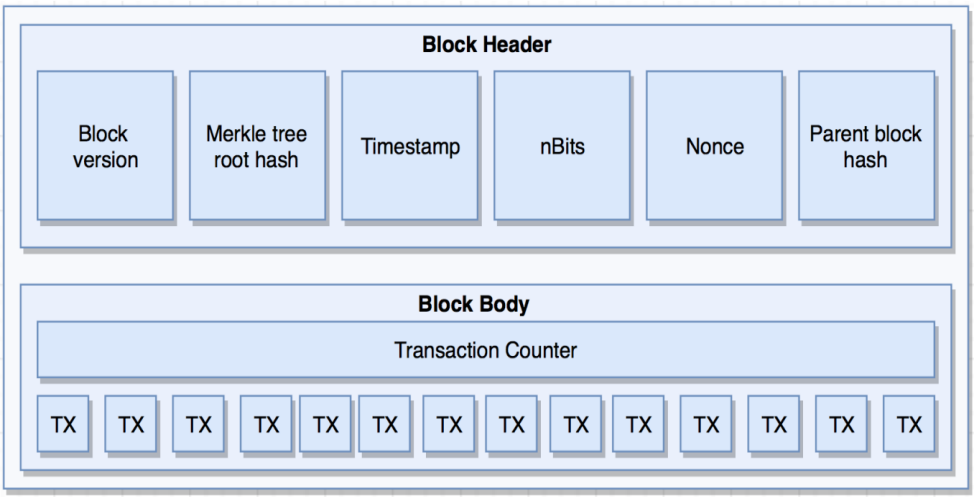

Figure 1.3 Diagrammatical representation of Block header

Blocks in a blockchain are essentially based on the previous block on the chain. They are generated by nodes involved in the consensus protocol. Each block comprises two basic components: the block header and the block body, as represented in Figure 1.3 [10].

A block's version starts the set of specifications for data verification. The combined hash value of all the transactions within the block is displayed via the Merkle tree root hash. The timestamp gives the exact moment in universal time expressed in seconds. The nonce, which typically starts at 0, increases with each hash computation, whereas the nBits field sets the goal threshold for a valid block hash. The 32-byte hash that corresponds to the previous block is the parent block hash.

The block body contains the block's transaction count and the individual transactions themselves, as seen in Figure 1.3. The essential operation of the blockchain protocol develops in the following manner:

1. Node construction and transmission of new information across the network.

2. Upon getting accurate information and owning sufficient stored data, a node constructs a new block, meeting a minimum transaction threshold.

3. Nodes engage in executing the consensus algorithm on the block. Successful consensus results in the block's insertion into the chain.

A consortium blockchain is the best alternative while considering the strong security measures in place. This form of blockchain allows the ability to create access restrictions, guaranteeing complete control over who can access particular medical records. Additionally, all transactions are digitally signed, assuring the non-repudiation of data. Each participant in the network keeps a copy of the transactions, preventing unauthorised changes and guaranteeing the accuracy of the data. Moreover, the immutability of the blockchain addresses the difficulty of data preservation, making it a strong solution.

1.5 MEDICAL INFORMATION SYSTEM

Medical Information System (MIS) is a digital platform built for the systematic storing of patient health records, encompassing medical history, test results, demographics, and billing details and diagrammatically illustrated in Figure 1.4 [7]. The official and unofficial public and private networks that encompass institutions, organisations, and resources dedicated to the advancement, preservation, or upkeep of people's health make up the health system. Beyond the physical healthcare facilities, this system integrates diverse stakeholders, ranging from caregivers like grandmothers helping sick relatives at home to private health practitioners, rehabilitation programs, vector control campaigns, health insurance providers, and researchers, among others. Effectively structured health information systems serve a crucial role in enabling decision-makers to accurately detect the field's progress, needs, and obstacles. Furthermore, these platforms promote evidence-based policymaking and informed problem-solving.

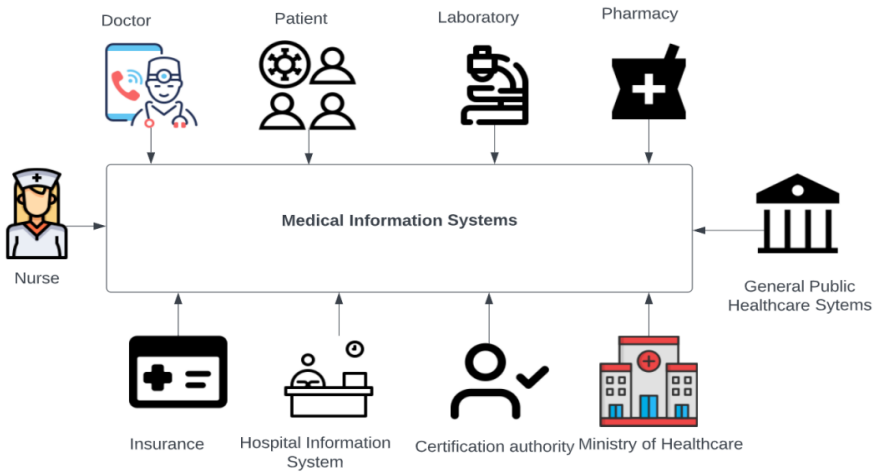

Figure 1.4 Overview of MIS

In many developing nations, notably in sub-Saharan Africa, health information systems confront substantial hurdles due to many variables. These include, among other things, a lack of IT and health professionals, a population that is growing faster than the amount of healthcare resources available, high telecommunication costs, unstable political environments, and unstable power supply. However, countries such as Ghana, Uganda, Zambia, and Tanzania have lately integrated technological solutions inside their healthcare sectors. Through the automation of data collection, validation, and analysis, information and communication technology (ICT) has been essential in reducing errors [11]. Despite these developments, there remains a need for enhanced industry collaboration to promote health data security and ensure improved compatibility among varied stakeholder systems.

1.5.1 INTEROPERABILITY, DATA INTEGRITY, AND PRIVACY IN HEALTHCARE SYSTEMS

Effective interoperable EHR systems within healthcare considerably improve operational efficiency, reduce costs, and streamline service delivery. Interoperability serves as a foundation for seamless communication, data sharing, and the utilization of information across varied IT systems and software applications. This interchangeability allows for data sharing among multiple

stakeholders, including clinicians, laboratories, hospitals, pharmacies, and patients, irrespective of the specific applications or vendors involved. Within health systems, interoperability facilitates the collaboration of health information systems both within and beyond organizational boundaries. Meanwhile, data integrity assures the accuracy and preservation of information shared or stored between EHRs. Ensuring the data's fidelity throughout transfer is vital to ensure the accuracy of databases, avoiding any concerns surrounding information reliability. Vital to patient safety, EHRs play a pivotal role in minimizing medical errors, alleviating health inequities, and advancing public health [12]. Furthermore, protection against medical identity theft is vital to prevent the inclusion of erroneous information into a victim's record. Such mistakes could lead to the victim's insurance being charged for services not obtained, thereby impacting the future treatment of the patient if directed by deceptive data that remains unrecognized by both the patient and the care provider. Insufficient faith in EHRs and Health Information Exchanges (HIEs) can lead patients to distrust the confidentiality and authenticity of their EHR, leading to reluctance to disclose crucial information. Since revealing private health information might have serious repercussions, EHRs must ensure the security and privacy of such data. Moreover, any breaches of health data pose major dangers, inflicting loss to both the company, in terms of reputation and cash, and the impacted patients. Weak privacy and security protocols heighten the vulnerability of patient information within EHRs, enhancing the susceptibility to cyber-attacks. Consequently, the incorporation of blockchain technology looks to be a possible option as existing healthcare systems have not adequately tackled difficulties with interoperability, patient data privacy, and data integrity.

1.5.2 THE NEED FOR BLOCKCHAIN TECHNOLOGY IN THE AREA OF HEALTHCARE

In this current period, the volume of digital health data is undergoing tremendous expansion, leading to the birth of what is frequently referred to as Big Healthcare Data (BHD). This phenomenon is integrally tied to the proliferation of software applications and mobile devices, plus the digitization of medical data and patient

information. Similar to other forms of big data, BHD holds considerable potential and value. It can increase patient outcomes, forecast epidemics, offer important insights, prevent avoidable diseases, reduce healthcare delivery costs, and boost overall quality of life. Nonetheless, the utilization of BHD presents problems regarding the security of health data and the privacy of individuals, which necessitate cautious attention. A survey by CynergisTek showed troubling statistics: in 2016, there was an enormous 320% increase in hacking attacks on healthcare facilities, and a substantial 81% of health data breaches came from such targeted hacking activities [13]. The vulnerability of old medical technology and software, along with the disregard for cybersecurity issues, dramatically enhances the possibility of cyberattacks. The interconnected nature of health data poses a considerable risk. When healthcare data is stolen, it can be utilized for blackmail or to conduct medical fraud. Unlike assets such as account numbers or credit cards, medical records and patient data remain consistent. Consequently, as shown in Figure 1.5 , BHD possesses enormous value due not only to their depth but also their enduring character, underlining the crucial need to guarantee their security.

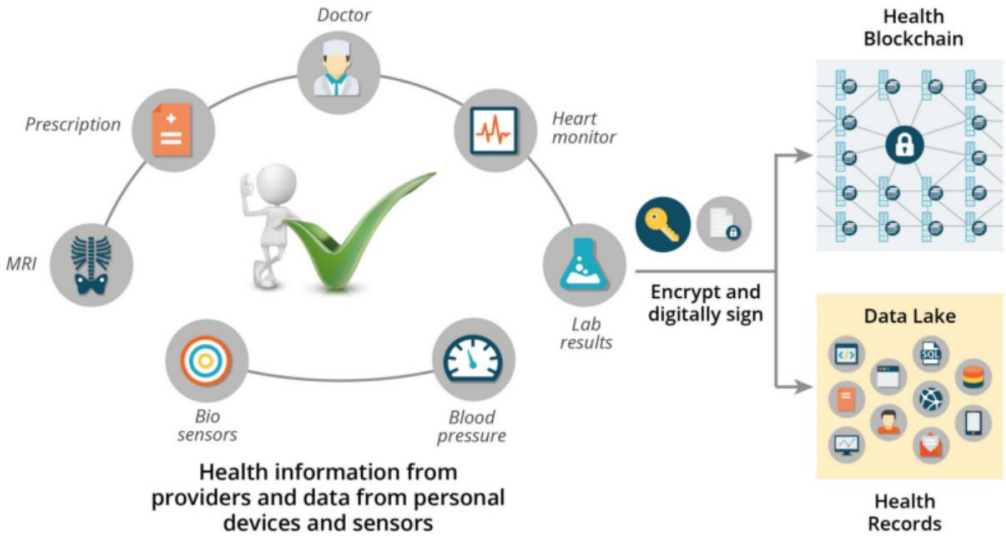

Figure 1.5 Blockchain use case in IoT healthcare scenario

The European Commission, in its paper first published in 2014 and amended in 2018, underlines three major concerns surrounding the exchange and access to healthcare data:

1. Facilitating secure access and smooth exchange of health data.

2. Aggregating health data for research purposes and the improvement of personalized therapy.

3. Implementing digital technologies and data access to empower citizens and prioritize person-centred healthcare.

The statement states a vision where health data is accessible to both owners and healthcare providers throughout the European Union. This accessibility is predicated upon strong assurances of security, privacy, and compatibility across varied platforms. A basic aim entails using a bigger number of health data for research while concurrently providing individuals complete control over their data. To go into a more formal and technical debate on privacy and security in healthcare, it is vital to establish explicit definitions of these basic concepts. Privacy refers to the capability to safeguard sensitive personally identifiable healthcare information, whereas security comprises protection against unauthorized access, frequently including the maintenance of data integrity and availability. Privacy focuses on the proper handling and oversight of an individual's data, while security focuses on shielding data from hostile breaches. Computing is a multidimensional discipline with applications across numerous knowledge domains, aimed to better and automate operations within each specific field. The breadth of computational tools available can offer important answers to several medical difficulties, potentially leading to increased quality, efficiency, and cost-effectiveness within healthcare systems [14].

1.6 TRADITIONAL SYSTEMS VS BLOCKCHAIN

The acceptance of blockchain's essential components has grown significantly in recent years, which has sparked an increase in research on the use of distributed

ledger technology in blockchain in the biomedical and health fields. These studies have led to the development of several new applications with distinct purposes, including speeding insurance claim processes, enhancing medical record management, accelerating clinical and biomedical research, and advancing biomedical and healthcare data records. These applications try to address widespread concerns within conventional healthcare and health information exchange systems, which are often centralized, with one intermediary controlling and keeping all data. In contrast, blockchain functions on a consensus process, where each node joins in selecting shared information and its recipients, ensuring that every node retains a copy of the recorded data. Furthermore, decentralized systems dramatically minimize transaction costs [15].

1.6.1 KEY ASPECTS OF BLOCKCHAIN IN HEALTHCARE

The key aspects of blockchain in healthcare systems are mentioned below:

- **Security:** Blockchain is largely known for its capacity to deliver security and permanence through decentralization and data encryption. Signing systems serve a vital role in encrypting data, regulating access, and validating digital signatures. Utilizing the Ethereum blockchain for storing medical information enables patients to securely administer their data through smart contracts.
- **Privacy:** Privacy is a vital problem within the healthcare business, and blockchain technology offers a solid method to handle this issue. It achieves this by the adoption of encryption technologies to ensure the confidentiality of patient data. To improve privacy, numerous mechanisms, including message signing by users, can be implemented. Furthermore, the Ethereum platform can be augmented with cryptographic technologies like encryption and proxy re-encryption to further increase privacy safeguards.
- **Access Control:** In healthcare data management, data ownership and access control are closely related concepts. Encryption using the public key of the owner is used to protect medical documents. The re-encryption key, which

is safely stored on a reliable intermediary called a gateway server, is one of the additional pieces of information required by the authorization process. Only the owners of the data are permitted access. Additionally, access control is based on the blockchain, which makes all actions transparently tracked and reported.

- **Data Immutability:** Data immutability in healthcare is crucial as it prevents unwanted adjustments. By applying cryptographic techniques within the blockchain hashing process, data transactions are made unchangeable. This fusion maintains the integrity and security of healthcare information, shielding it against unauthorized alterations.
- **Data Integrity:** Data integrity is an essential component of data storage, whether centralized or decentralized. One approach to ensure this is by applying public key cryptography, a characteristic employed in blockchain technology, to encrypt the data. This method contributes to the security and accuracy of the information. Access to records for specific activities or sessions is limited primarily to authorized individuals within the system. In the area of healthcare, patients have full discretion over granting or withdrawing access to their medical information, guaranteeing the confidentiality and privacy of their health data.
- **Confidentiality:** Privacy issues typically extend to confidentiality, and solutions using blockchains and encrypted signatures act as preventive measures against malicious attacks. The encryption protocols provide stable ciphertext sizes, increasing data security. By employing this technology, healthcare institutions may create discrete and adaptable access control systems to meet their evolving requirements.
- **Data Ownership:** The issue regarding data ownership applies to the anxiety over prohibited access to sensitive healthcare information by external parties. One potential solution to this challenge involves the employment of blockchain technology coupled with robust encryption mechanisms. Through the implementation of smart contracts and platforms like

Ethereum, this solution intends to empower patients by enabling them to retain control and ownership of their data.

- **Availability:** In the area of healthcare, accessibility remains a key challenge, with hurdles limiting patient access to important services. Smart contracts linked with keychains offer a possible solution by employing cryptographic technologies and distributed ledger technology. These revolutionary techniques increase security safeguards, preserving the integrity and confidentiality of critical medical data. By exploiting these improvements, keychains can promote increased accessibility to healthcare resources while enhancing security standards, thereby addressing the critical challenges of both accessibility and data protection within the healthcare sector.
- **Data Validity:** Data validity is vital in confirming validation processes. However, as the data collecting queue expands, the chance for errors also rises. In blockchain, different protocols exist to authenticate a user's private key during transaction validation. These approaches ensure that each transaction's signature is verified using the user's private key. Subsequently, the public key is utilized to confirm the created signature, confirming the integrity and security of the transaction.
- **Auditability:** Blockchain networks offer robust auditability through their intrinsic properties. The digital timestamping service offers an immutable record of transactions, increasing transparency and accountability. By applying effective cryptographic primitives, blockchain technology guarantees data integrity, allowing a trustworthy solution for healthcare applications [16]. This auditability is vital in preventing unwanted access, and ensuring patient data remains confidential and is only accessible by authorized staff. Consequently, the greater process reliability inside healthcare systems helps safeguard the integrity of sensitive information, fostering confidence and compliance with data rules.

1.7 CHALLENGES OF USING BLOCKCHAIN IN HEALTHCARE

Blockchain has proved its adaptability by finding applications in numerous sectors, despite its transdisciplinary character, which poses both problems and constraints. Researchers are currently addressing these challenges to lessen their impact. The following are some technological challenges associated with the application of blockchain technology in the healthcare industry.

- **Throughput:** The healthcare environment demands high transaction throughput, and when the number of transactions and network nodes increases, it might lead to a bottleneck. In healthcare systems, ensuring quick access is crucial, as any delay could impair timely diagnosis and life-saving measures.
- **Latency:** The block validation procedure normally takes a few minutes, which might pose security vulnerabilities, since attackers might abuse this time frame. In the dynamic domain of healthcare, constant access is crucial, since even tiny delays could have harmful impacts on exam analysis and patient care.
- **Security:** Ensuring security in this environment is crucial, as control over 51% of the network's processing power can threaten the integrity of the system. This is especially crucial in healthcare because any degradation can lead to a loss of trust in healthcare organizations.
- **Resource consumption:** The employment of this technology offers a considerable threat in terms of resource consumption, mainly due to the substantial energy expended in the mining process. Healthcare environments already face high energy costs with various patient monitoring devices, and the inclusion of blockchain could worsen these expenses. Managing these heightened costs becomes a challenge for corporations.
- **Usability:** Moreover, usability creates a hurdle with these systems due to their intrinsic complexity. Creating a user-friendly API is vital, especially for healthcare practitioners who may lack the technical understanding of IT

specialists. The systems must be built to be user-friendly, intuitive, and easily navigable for persons with varied degrees of technical experience.

- **Centralization:** Centralization inside the blockchain, despite its decentralized nature, can occur when certain mining approaches concentrate power around a few nodes, reducing the network's resilience. The vulnerability of these core nodes makes them susceptible to breaches, potentially providing access to stored information through malicious assaults.
- **Privacy:** The widespread assumption is that the Bitcoin system provides a level of anonymity for blockchain nodes. However, further solutions are essential to expand this capacity to other blockchain-based systems. Compliance with privacy rules like the General Data Protection Regulation (GDPR) is crucial for these systems due to the sensitive nature of data and information.
- **Costs:** The limits indicated pertain to the allocation of resources including time, capital, and economic concerns for building a blockchain system. The limits incorporate resource constraints inside IoT. Moreover, the expenses associated with orchestrating a decentralized application in adopting blockchain technology. These include the incremental rise in protocol expenses connected to the individual qualities and properties of the entities involved, resulting in high operational overhead for patients and higher access delay for requesters. Furthermore, the expenses associated with exchange and implementation are dependent on changeable inputs such as the size and length of a given string.

1.8 APPLICATIONS OF BLOCKCHAIN IN HEALTHCARE

Numerous authors and companies have created applications employing blockchain technology inside healthcare systems. This section will highlight four separate architectural examples using blockchain in the building of healthcare systems.

1.8.1 MEDREC

MedRec was created to overcome many difficulties with consumers' Electronic Medical Records (EMR). These challenges encompass fragmented and inefficient access to medical data, issues concerning system interoperability, inadequate patient awareness of their complete medical history and the modifications made to it, as well as the enhancement of both data quality and quantity for medical research purposes. Numerous authors and companies have created applications employing blockchain technology inside healthcare systems. This section will highlight four separate architectural examples that leverage blockchain in the building of healthcare systems.

The selection of the individuals is to employ the Ethereum public blockchain for its utilization of smart contracts in storing metadata relating to ownership, and rights, and ensuring the integrity of data. EMRs are saved in external databases, with the blockchain maintaining references to these databases. Crucially, the blockchain preserves a hash of the stored data to ensure its integrity. When an entity adds data concerning a patient, a notification is given to the patient, enabling them to examine and either accept or reject the data. Patients hold the ability to share their data with other authorized entities. To validate a participant's entity, a system uses the public key and a mapping system similar to DNS, combining the Ethereum address with the client's social security number or name. Three separate contracts were designed to manage the system's relationships between entities and users:

- **Registrar Contract (RC):** This contract connects a participant's identification to their Ethereum address, which is effectively the public key. It also controls the Summary Contract.
- **Contract for Patient-Provider Relationship (PPR):** This contract manages the connections between patients and providers and is designed with specified permissions to access data.

- **Summary Contract (SC):** This contract refers to the Patient-Provider Relationship Contracts and effectively encapsulates all interactions with system nodes.

1.8.2 ONCOLOGY SPECIFIC DATA MANAGEMENT

A recent study described a specific methodology for managing oncology data. This unique platform enables users to create data access control policies. One of its primary characteristics is that it enables improved data sharing among various businesses. Several considerations influenced the decision to use a permissioned blockchain as the underlying framework:

- Ensuring user identity verification is critical when dealing with sensitive health information.
- Protecting patient data privacy by monitoring communications between patients and involved entities.
- Prioritizing rapid system responsiveness for efficient procedures, given the critical nature of healthcare.
- Reducing usability constraints by reducing transaction costs for entities changing a user's health records.

1.8.3 HEALTHCHAIN

Healthchain has been thoroughly constructed in compliance with the requirements given out in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [17], which is applied within the United States. HIPAA serves as the framework for defining Protected Health Information (PHI). PHI comprises standards for ensuring the privacy of individually identifiable health information, spanning demographic and genetic data. The HIPAA privacy rule provides severe criteria to preserve control over individuals' PHI, safeguarding patients' rights over their information. This system guarantees that exclusively authorized personnel can access, evaluate, and alter an agreed-upon record. The patient takes the initiative to generate the original PHI version, and then place it into the blockchain. Smart contracts serve a crucial role in ensuring that the user system only incorporates the

original version into the blockchain. Healthchain's architecture has three important components:

- A private blockchain working on IBM blockchain,
- Implemented on Bluemix within the IBM cloud infrastructure, and a web page.
- The NodeJs server orchestrates interactions with Hyperledger Fabric and the chaincode.

1.8.4 MEDICALCHAIN

MedicalChain is a platform employing blockchain technology for the safe storage and transmission of EHR. Utilizing blockchain, it centralizes and secures health records, providing a solitary version of users' data. Privacy safeguards are applied by Hyperledger Fabric, which provides a private blockchain and enables exact data access management. The program gathers all medical documents, scanning and encrypting physical records before uploading them to the cloud. EHRs are standardized, encrypted, and similarly uploaded. The process involves the following steps:

- Data generation by wearable gadgets, doctor's notes, scans, or medicine dispensation.
- Encryption and transport of data to a cloud storage. The patient's blockchain stores an ID identifying the data stored in the cloud.
- Data retrieval utilizing the ID kept on the blockchain to retrieve the encrypted data upon request.
- Decryption and display of the data on the respective device or application.

1.9 ORGANIZATION OF THE THESIS

The emphasis of the thesis focuses on secure data sharing and storage using blockchain technology for healthcare data. The thesis is presented with the following general arrangement:

A thorough introduction to blockchain technology in healthcare systems is provided in Chapter 1. It includes an overview of blockchain technology, different kinds of blockchain networks, the healthcare information system, the need for blockchain in managing healthcare data, difficulties, and applications in the medical field. It also includes the research's motivation and background.

In Chapter 2, an overview of the literature on the ideas and difficulties of blockchain based secure healthcare data management is presented. A thorough literature review of various methodologies is also presented.

In Chapter 3, the DZTBS approach is suggested for securing data sharing, combining smart contracts, a zero-trust framework, and blockchain technology. This technique targets two major issues: the secure interchange of EHRs and the confidentiality of medical records gathered from varied sources. By using the zero-trust concept and employing smart contracts, DZTBS assures that medical records can be shared while respecting patient privacy even in circumstances where data requirements are substantial. Notably, this method greatly reduces total execution time and block generation, exceeding existing encryption techniques in terms of both encryption and decryption speed. The results underline the heightened security and operational efficiency gained by the DZTBS in healthcare management systems. This section also offers an extensive summary of the experimental results.

In Chapter 4, the 'sHealthCareBlockchain' framework is proposed. It aims to address data sharing and retrieval issues using dynamic sharding, parallel processing, and consensus-driven data propagation. The methodology includes an adaptive dynamic sharding algorithm, load balancing, and a parallel transaction validation method based on the Heinit criterion. The proposed data retrieval scheme combines Merkle-Patricia Trie and Bloom filters. Results show the efficiency of the proposed mechanism. Comparative analysis with a traditional blockchain highlights the superior performance of 'sHealthCareBlockchain,' with higher throughput, lower latency, and improved data-sharing efficiency. The findings

validate the efficacy of the proposed framework for secure and efficient healthcare data sharing.

In Chapter 5, an innovative solution for accessing EHR in a blockchain-based smart healthcare system has been created, including Redis caching, an Adaptive Balanced Merkle (AB-M) tree, and a lattice-based ring signature scheme. These three key components are immediately merged into a consortium blockchain architecture, producing a secure and efficient smart healthcare ecosystem. Extensive testing, encompassing changing user counts and two distinct block sizes, proves the usefulness of the suggested technique. The results of the study repeatedly illustrate the superiority of this methodology over other modern methodologies, surpassing their performance baselines. This highlights its potential to change EHR retrieval in smart healthcare scenarios. This section also offers an extensive summary of the simulation's results.

Finally, the chapter 'Conclusion and Future Research' summarizes several experimental findings as well as work that can be expanded in the future followed by References and Publication details.

CHAPTER 2
LITERATURE SURVEY

Blockchain technology is designed to enhance data security and accessibility inside a networked IoT environment. It recovers secure information from transactions, resulting in a higher quality of experience through systematic evaluations. While numerous research efforts have been committed to addressing patient privacy in Personal Health Record (PHR) and EHR systems, securing data privacy during the transit from sensors to end-users in an IoT-based healthcare technique requires distinct techniques. These systems must provide real-time data delivery while also accommodating sensor and gateway resource limits. While IoT-based healthcare systems have taken privacy into account, centralised solutions have run into problems, especially when it comes to collusion attacks. Consequently, several researchers have created blockchain-based solutions to protect patient privacy in IoT-based medical procedures. As a result, there is still a deficiency of blockchain-based alternative healthcare methods that can secure patient privacy, particularly when operating under the assumption that all system entities are undependable. Thus, this chapter presents a comprehensive analysis of various blockchain based healthcare systems utilized in existing analyses and it is organized as follows.

2.1 REVIEW OF BLOCKCHAIN-BASED HEALTHCARE SYSTEM

G. Amudha [18] described the use of the Dilated Transaction and Retrieval Method (DTARM) to develop information retrieval for blockchain associated IoT transactions. The primary goal of the implemented work was to increase the retrieval rate of information while decreasing retrieval time by presenting DTARM. Blockchain technology was used to secure data in a heterogeneous platform by processing some authentication techniques. The developed approach analysed existing transactions using non-replicated identities and recursive block association. Access and retrieval of information were randomly maintained by a non-recurrent binary procedure. The random procedure was augmented in time, so a transaction time restriction was applied to limit the number of random searches.

Based on numerous blocks, the splitting was assessed, and it was processed by distributing into sub-blocks. Multi-random searches were presented in a branched manner for block classification and for developing the transaction evaluation's precision, the significance-based retrieval was accomplished that followed by this access. The replicated and non-replicated blocks through similar information were significantly diminished in the various classifications by the performance of periodical trimming. The transaction evaluation's precision was accomplished by processing the algorithm of trimming tree classification. The developed method enhances the significance of information and retrieval ratio by access reduction and time of retrieval.

Ti-Wang et al. [19] suggested the enhanced Dual Policy Attribute Based Encryption (DP-ABE) for secure data transfer in cloud. This method was discovered for producing the DP-ABE that was more secure, flexible and effective to deploy in cloud sections. Based on prime-order asymmetric combination sets, suggested method encompassed two monotone LSSS-realizable large universe DP-ABE structures. A security classification formalization as well as appropriately provides its security in a random oracle model and implements the developed technique by utilizing the Charm framework. Initially, based on the CPA secure scheme, two improved flexible features of access control such as encryption and key generation were validated in single policy modes. Then, fully deployed computation as well as CCA security was realized which was much more efficient and protected for applied deployments. A proposed technique achieves some of the following results: i) Key generation and encryption via DP-ABE access control mechanisms are two features that it supports. ii) The multiple encryption, key-generation, and decryption processes were safely deployed to cloud servers, greatly reducing the overheads for users, PKG, and data owners. iii) The strong security idea of public-key encryption systems—also known as CCA security—was realised. The method involves transferring ciphertext retrieval computations into blockchain for third-party authority. Test results indicate that this approach is reasonable and effective.

Ruyan Liu et al. [20] developed the trusted data storage procedure based on blockchain for the industry 5.0. A process uses random low-density parity codes to code the tree in addition to integrating sharding and two-layer Merkle tree architectures. By increasing the blockchain throughput, it allowed the light nodes to verify the authenticity of the data and resolve data accessibility attacks. Initially, I/O bottleneck difficulties which disturb the blockchain throughput were addressed by employing STM-Tree. Then, by using LDPC codes to STM-Tree codes, light nodes could verify the authentication and lower the risk of false data by reducing data accessibility attacks brought on by multiple dishonest agreements on blockchain. At last, nodes of low-storage blockchain were developed which utilizes removal codes and is only required to store every block-coded fragment, also significant diminishment of weights on nodes. Using LDPC and MTs codes could lower the cost of incorrect coding proofs while ensuring the authenticity of data transfers. In order to preserve the decentralised blockchain assets, the presence of storage nodes via an erasure code technique could solve the rapidly increasing data storage volume challenges in data transfer. Additionally, the network load of nodes was efficiently diminished by employing erasure codes to build nodes of low-storage blockchain that address difficulties in the scalability of blockchain. Furthermore, the suggested method integrates coded computation through blockchain for a diminishment of storage pressure. But in order to validate transactions, the developed method had to make use of coded computation technology.

Da-Yu-Jia et al. [21] presented the new scale-out blockchain model (SE-Chain) which enhances storage scalability below principle of assuring safety as well as effective recovery actions. SE-Chains involve three layers such as data, processing as well and storage layers. Each transaction was stored on Adaptive Balanced MT (AB-M tree) in a layer of data which adaptively integrates stable Binary Tree (BT) and MT advancements. A contributing factor to the integration was the stable BT's quick search speed and quick data validation in MT. Additionally, the AB-M tree might benefit from having two trees. The multiple layers of stable BT nodes are

adaptively regulated by the AB-M tree based on the blockchain's request requirements. Every node stores every chain link in the processing layer chosen using the same ratio regulation method. To improve the overall node stability and lessen the challenges of incomplete data recovery brought on by the elimination of duplicate numbers in the storage layer, a node reliability validation technique was implemented. In contrast to the fabric system scenario, the typical storage capacity used by SE-chain nodes decreases as data sizes rise steadily.

Through an associated blockchain, Duo Zhang et al. [22] introduced safe and private medical data transfer. Attribute-based access control methods were used to achieve access; record requesters were defined by a set of attributes, and patients predetermined attribute-specific access strategies for their health records. In order to allow patients to store encrypted health data off-chain and write medical record access strategies on group blockchain, the hybrid storage mode was created. The blockchain and smart contracts could be used to achieve access privilege control and access tracking. When a medical record tree was created to improve key management for every patient, patients could advance their encryption keys at any time by simply storing medical record trees. Extensive analysis was performed to demonstrate the high security and efficacy of this developed technique. Last but not least, a sophisticated method for simulating transactions was developed with the Quorum consortium blockchain on the Tencent Cloud and smart contract organisation on blockchain. The strategy might create a channel for the transfer of medical data, thereby resolving the current information island problem. However, in order to quickly advance the wearable device and IoT framework, the security of medical data transfer in the human domain network was necessary.

On the basis of reputation in IoT blockchain, Xu Yuan et al. [23] created the Efficient Byzantine Reputation-based Consensus (EBRC) mechanism. The protocol enhances blockchain security with a deposit penalty mechanism and uses timestamps and reputation data from IoT devices to ensure node reliability. IoT devices could be encouraged to maintain excellent behaviour and meet the

requirements to be consensus nodes by using the reputation score, which was closely linked to a node's actions. Dynamic Joining and Exiting Protocol (DJEP), another feature of this protocol, enables blockchain systems to rapidly adjust to shifting network circumstances and reach consensus. Furthermore, EBRC increases the dynamic of the IoT blockchain network by allowing nodes to join and leave seamlessly, making it more fit for the ever-changing environment of the real IoT blockchain network. Extensive trials were carried out, demonstrating that EBRC outperformed the usual PBFT consensus procedure. This illustrates that the algorithm developed provides an excellent approach for constructing the IoT utilizing blockchain and Internet-based legal systems.

Renpeng Zou et al. [24] suggested a blockchain-based system for medical data transfer as well as preserving health privacy. Special key blocks and microblocks were presented for efficient storing of EMRs by patients, as well as a novel chain structure to alleviate the forking issue. They established a reputation system that allowed reputable institutions to access EMRs for medical research to incentivise medical institutions to participate in SPChain. SPChain served as the foundation for a strong eHealth system that allowed for safe data transfer and retrieval while protecting patient privacy. The system utilized proxy re-encryption strategies to protect EMRs stored in local databases at medical institutions, guaranteeing that only authorized institutions could access patient records. Furthermore, it provided patients with specific transactions to register in SPChain and report inaccuracies in their medical information. The reputation system was created to encourage medical institutions to participate actively in SPChain. SPChain enabled patients' privacy-preserving medical data transfer by utilizing proxy re-encryption methods. The system's performance and resistance to various threats were evaluated utilizing real-world miner distribution. To lower the communication overhead for patients and increase system throughput, a developed approach was necessary.

Xu Ma et al. [25] presented the trusted data transfer with flexible access control based on blockchain. To enhance retrieval result accuracy, a novel searchable

encryption approach that supports multiple keywords was introduced. This method describes a framework for secure and trustworthy data transfer that makes utilize of searchable encryption, Attribute-Based Encryption (ABE), and blockchain. A developed method for blockchain-based data transfer with multi-keyword capabilities makes utilize of CP-ABE to fulfil the need for data protection and control while allowing for flexible transfer utilisation. Ciphertext retrieval computation was offloaded to the blockchain, ensuring reliable execution without depending on a trusted third party. A technique attains severe security requirements for data, according to security analysis. The fact that the recovery procedure was moved from an untrustworthy cloud to a decentralized, trusted blockchain eliminated a need for reliance on any trusted third party. An analysis and a series of experiments entirely authorize the arrangement's practicability as well as efficiency. One weakness of the strategy, however, was its reliance on a predetermined universal set.

Blockchain and AI were integrated by Rajesh Kumar et al. [26] to enable safe data transfer and CT image detection for hospitals. The developed technique performs numerous critical functions: (i) It provides a way to enhance medical data security by transferring only the learned deep learning model's weights through a smart contract. (ii) To accept heterogeneous Computed Tomography (CT) pictures of differing sizes from numerous sources, it incorporates the Bat approach as well as data augmentation in the global learning model to limit overfitting and noise. (iii) For training a global model, the local deep learning model weights were disseminated through a decentralized blockchain network. (iv) For evaluation of the Region of Interest (ROI) within CT images, a Recurrent Convolutional Neural Network (RCNN) was developed. Generally observed analysis has been carried out to validate the efficacy of this newly created strategy in improving early-stage cancer prediction. The major goal of merging blockchain and deep neural networks was to utilize distributed network patient data to diagnose specific health issues based on low-dose CT scans or radiology images. A DNN model examines medical photos including information about cancer nodules that have been stored and

processed within the blockchain distributed network. Furthermore, DL models require a considerable amount of resources to train as computational power.

Mengji Chen et al. [27] developed the blockchain enabled healthcare system for detection of diabetes. Blockchain, the Interplanetary File System (IPFS), and symptom-based illness prediction are combined in the EHR's transfer architecture to gather patient health data via wearable sensor devices. The user commences the registration procedure in the first phase of this system to establish connectivity with a blockchain network. The EHRs Manager, which was kept within an authentication unit, was utilized to verify user identity. Information from patients and medical professionals, such as doctors, was gathered by the Registration Centre (RC), which was tasked with safely storing it in a database. Machine learning algorithms for detecting diabetes in patients and securely transferring the results to healthcare practitioners were demonstrated. It was assumed by the system that all storage nodes were IPFS-based, and that hospitals and other healthcare providers had collaborated to build and maintain the IPFS system. It utilizes a content addressing approach, which derives addresses from the file content. This established system was intended to assist the healthcare sector in securely storing, processing, and transferring patient health information. It was also intended to help doctors diagnose diabetes more accurately. However, the suggested approach was required to develop an advanced blockchain based model to prevent blockchain attacks.

Desire Ngabo et al. [28] developed the blockchain-based security procedure for the medical data at fog computing framework of IoT. To support a distributed ledger database (server), a security mechanism for a public-permissioned blockchain has been devised, employing Elliptic Curve Cryptography (ECC) digital signatures. The goals of this system's design were to guarantee complete security, guarantee transaction transparency, and guard against tampering with patient records inside the Internet of Things fog layer. The main goal of this security procedure is to ensure optimal data security while addressing fog layer latency issues by

implementing an immutable security solution for medical data within the IoT fog layer. Blockchain adoption was prompted by flaws in existing security measures for Wireless Sensor Network-based IoT (WSN-IoT), which suffer from computational complexity, memory constraints, power consumption of high processors, latency, susceptibility to social attacks, and further issues. The blockchain solution also helps to minimize centralization, latency, and scalability difficulties inside the fog concept. To assess the system's performance, data recovery size was weighed against the efficiency of digital certificates in terms of time in ms, resulting in a data retrieval rate of around 180 ms. Also, testing was carried out and findings for data retrieval latency, size, and key generation time were provided. But in order to create unique decentralised software that enables a facility to open and view health documents without the need for private keys, the suggested approach was necessary.

Ibrahim Abunadi et al. [29] suggested the blockchain security framework for EHR of patients. This framework provides doctors, patients, and insurance agents with a safe and efficient way to attain medical information while protecting patient data. The goal of this work was to evaluate how the developed framework fulfils the security desires of patients, doctors, and third parties, as well as safety and privacy apprehensions in healthcare. Patients may manage, download, and exchange their EHRs autonomously through BSF-EHR system. The BSF-EHR structure was made up of five important players: the patient, the doctor, the insurance agent, the data verifier, and the EHR server. The process begins with the patient seeing the physician and getting treatment, and then the EHR system server serves as a blockchain network node. It gathers EHRs from transactions and arranges them into blocks, much like a miner. The outcomes demonstrate how well BSF-EHR facilitates safe data exchange between users. Protecting critical EHRs from outside threats is effectively achieved by using the BSF-EHR access control system. Furthermore, the BSF-EHR framework offers lightweight EHR transfer with the least amount of time consumption when compared to conventional centralised storage solutions. But in order to apply this framework to a variety of industries,

including the supply chain, IoT, education, logistics, finance, banking, agriculture, and accounting, a developed method was needed.

By combining edge devices with blockchain technology and ECC, Mary Subaja Christo et al. [30] implemented a system that ensures better security for medical data. The developed system uses a 512-bit key to encrypt and decrypt data as part of a robust data authentication mechanism. To ensure data secrecy, it employs blockchain ledger technology, limiting access to only authorized individuals. The encrypted data was subsequently kept on edge devices, which utilized edge computing technologies to enable quick data access within the edge network. Only authorised users could quickly decrypt and process the data. Following processing, the altered data was stored on a cloud server and in the blockchain. This algorithm utilizes the encryption key to secure data and then decrypt it. Data from end users was efficiently kept on cloud architecture, providing greater flexibility for accessing medical data at any time. Safe storage and retrieval of medical reports and data is guaranteed by the existing system. Furthermore, the system includes ground-level edge servers for efficient data processing and storage within cloud servers. The study emphasizes data security while emphasizing data confidentiality and authenticity through data processing and storage on a blockchain ledger.

Jasleen Kaur et al. [31] presented the blockchain-based framework for the privacy preservation of EHR. The Hyperledger Fabric (HLF), Identity-Based Proxy Re-Encryption (IB-PRE), and Interplanetary Distributed File System (IPFS) techniques were all utilized in the framework's thorough implementation. The blockchain network was established utilizing HLF. IPFS was utilized to manage EHRs on the blockchain, with the actual massive, encrypted data residing off-chain and their associated hash values maintained on the blockchain. Furthermore, the IB-PRE method was critical in facilitating safe EHR transfer, with a proxy node receiving requested data from IPFS, re-encrypting it, as well as then returning it to a requester, preserving user privacy, and data integrity. Smart Contracts (SCs) were created with the Go programming language to provide patients complete control

over their records by giving or denying authorization to requesters. Every transaction was painstakingly documented on the blockchain's immutable and distributed ledger. A Hyperledger Caliper tool was utilized to initialize a performance test to measure technique performance as latency and throughput. Enhancements to the framework's capabilities were required to ensure rapid query replies by reducing latency, cost consumption and response time.

Chandramohan Dhasarathan et al. [32] developed the user privacy prevention model utilizing a supervised federated learning-based blockchain approach for the Internet of Medical Things (IoMT). The suggested technique efficiently manages the large amount of data created by IoMT by applying blockchain for IoMT (BIoMT) technology to protect sensitive clinical information. This method employs a combination of encryption techniques to enhance the privacy protection of patient and health records. Furthermore, BIoMT guarantees secure and long-term supply chain management through a highly confidential decentralized structure enabled by blockchain-based smart contracts, reducing the danger of data loss. Furthermore, a framework that leverages a hybrid hashing technique, incorporating homomorphically encrypted algorithms, has been built to allow smart contracts for decentralized applications. The BIoMT method was tested and compared to comparable preventative measures. This study employs smart contracts with distributed consensus characteristics to develop a privacy protection method that serves as a strong deterrent to potential assaults at all transaction levels. The created solution performs particularly well in real-time settings for tackling critical infrastructure security. However, blockchain has highlighted the limitations of this system in terms of data privacy, emphasizing the need to ensure the integrity of information within a distributed ecosystem.

A healthcare system based on blockchain was developed by Kanika Agarwal et al. [33] with compact gas consumption, execution cost, transaction cost, and bandwidth utilisation, along with triple-layered security enhancements. Professionals and patients were initially registered to establish identity access

management. Following that, the owners issued authorization to each registered entity. Finally, a doctor-patient relationship was developed at the third level, with the hospital's owner assigning patients to specific doctors. Data was protected from unauthorized access and kept secure between the doctor and the patient. In addition, the established method utilizes a smart contract to record seven distinct diagnostic parameters by physicians and 15 different parameters by pathologists to speed up various hospital management activities. A system's performance was assessed by simulating and implementing the smart contract on the IPFS as well as evaluating metrics such as gas consumption, transaction fees, execution costs, and bandwidth utilization. As the several users increases, a method demonstrates lower gas consumption costs and maintains constant performance across multiple operations. This adaptive system concept has the potential for future growth and might handle a growing user population.

Using blockchain and IPFS, Deepa Rani et al. [34] proposed a secure framework for IoT-based healthcare. After storing the raw data from IoT-enabled medical devices on the IPFS, the system distributes it to healthcare providers. A dual-layer security approach, one based on blockchain technology and the other on powerful AES encryption technologies, was used to safeguard the data. Several implementation protocols are included in the designed framework. Because of the high expense of keeping files on the blockchain, IPFS was utilized as an off-chain data storage solution. The system utilizes the Proof of Authority (PoA) consensus technique to provide efficiency and scalability. This comprehensive solution employs distributed blockchain to assure data security, IPFS for storage and transfer, and Distributed Applications (DApps) for data collecting and blockchain connectivity, all of which are protected by encryption. The AES encryption algorithm was utilized to encrypt the data. IPFS acts as an off-chain storage mechanism for data, generating Content Identifiers (CIDs) that are then registered on the blockchain. A smart contract, which evaluates access rights and offers the CID for encrypted data, might be utilized by medical practitioners to seek access to patient data. As a result, this framework offers a strong two-tier security solution

for IoT-enabled healthcare infrastructure. However, this technique was initially created to transfer data with the medical team, hence, this method required to extend the framework with data analysis capabilities, which may lessen the data analysis efforts of the medical team.

Amal Abid et al. [35] developed the blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates (NovidChain). NovidChain incorporates numerous emerging concepts: i) utilizing blockchain to secure the integrity and stability of data. ii) Adopting self-sovereign identification principles, which provide people with ultimate control over their data. iii) Adherence to the W3C verifiable credentials standard, allowing for faster verification of COVID-19 proof. iv) The concept of selective disclosure was introduced, allowing users to share certain information with trusted partners. As a result, NovidChain has been painstakingly built to guarantee a high level of personal data safety while adhering to GDPR and KYC standards. It enables user self-sovereignty while also guaranteeing public safety and respecting individual privacy rights. The developed NovidChain platform includes a full technical description, a proof-of-concept implementation, multiple research studies, and a comparative evaluation to validate its security and effectiveness. However, the created NovidChain needed to be improved by including Fog/Cloud structure and Machine Learning techniques for vaccine prioritizing approaches.

Wenkang Liu et al. [36] developed the privacy protection framework for IoMT based on blockchain and federated learning. By combining blockchain, differential privacy, and Generative Adversarial Networks, a unique privacy protection framework for decentralized Federated Learning (FL) has been built. This unique design efficiently handles a variety of issues, including reducing the danger of a single point of failure and strengthening defences against inference attacks. Furthermore, the BFG framework successfully alleviates the blockchain's storage burden by finding a balance between privacy protection and global model accuracy. It also demonstrates resistance to the potentially negative consequences of node

withdrawal. Additionally, Differential Privacy (DP) was employed to inject noise into model updates, shielding against inference assaults while maintaining an equilibrium between privacy protection and accuracy. The approach utilizes Generative Adversarial Networks (GANs) to rebuild training data on specific local devices, resulting in auditing datasets. This approach creates a distributed defence against poisoning attempts, boosting privacy protection even further. The BFG framework takes advantage of these benefits to successfully protect sensitive healthcare data acquired from a diverse set of heterogeneous and resource-constrained IoMT devices. It enables healthcare practitioners to make more accurate and efficient clinical judgments by facilitating the secure transfer of patient healthcare data. Due to IPFS, the technique takes longer than typical FL methods, but it has the potential to solve several complex problems in the healthcare industry.

The Blockchain-Based Zero Knowledge Proof (BKZP) was created by Hasan Al-Aswad et al. [37] to improve healthcare security in Bahrain's IoT smart cities and reduce COVID-19 risk. The model developed was intended to establish a strong and scalable architecture for data exchange, with a focus on protecting sensitive data privacy while assuring consistent accessibility. It also affords robust trust and data truth by utilizing the stable properties of blockchain. Pre-approved blockchain access tokens served as the foundation for Bahrain's ZKP system, which successfully addresses privacy and accountability issues in Bahrain's smart cities. As a result, the model provides various stakeholders with a safe and dependable way to exchange patient data. This technique maintains a balance between trust, privacy, and high availability. A combination of ZKP with smart contracts enables programmable actions, allowing for the decentralized automation of prescription dispensing in secure pharmacies with a huge level of confidence. The usage of blockchain improves healthcare data accessible, even when network connectivity to the internet is lost. In such circumstances, nodes could resort to their locally trusted data, avoiding the need for duplicate checks and saving precious time and resources. The adoption of blockchain necessitates an increased understanding of

the critical role that an organization plays in guaranteeing the proper utilize of the trusted structure.

Shixiong Yao et al. [38] presented a blockchain based multi-dimension observable privacy-preserving prevention and control scheme of COVID-19. To support non-contact security audits, a unique blockchain-based health code system dubbed Auditable and Privacy Preserving Health QR Code (APHC) was developed. This method allows for the efficient auditing and tracing of personal information pertaining to confirmed cases and their close relationships, hence helping to successful epidemic prevention and control. The secure information of residents was safeguarded by utilizing Attribute-Based Encryption, which also allows for fine-grained access control, securing the privacy information buried within the Health Code (HC). Searchable encryption has been introduced into the system to facilitate multi-dimensional traceability by epidemic prevention and control authorities. Comprehensive security analysis and performance evaluation were carried out in order to confirm the viability and practical significance of this approach. In addition, an example approach based on the HLF blockchain was created, and its viability was confirmed by a performance comparison study. An analysis of existing close contact tracing and information exchange systems revealed serious deficiencies in current health code privacy-protection and auditing systems.

Shujiang Xu et al. [39] suggested a privacy-preserving and efficient data transfer scheme with trust authentication based on blockchain for mobile healthcare (mHealth). The usage of blockchain-based access rights authentication guarantees highly trustworthy authentication results. Furthermore, in the context of mobile health (mHealth), the implementation of effective encryption and decryption algorithms caters to the user-friendliness of IoT device users. Throughout the key creation and encryption stages, this method incorporates an offline strategy to improve mHealth efficiency. Furthermore, the technique was designed to mask access policies in part, protecting user privacy. Utilizing blockchain enables a

decentralized and trustworthy authentication system for data access rights. This approach conceals attributes within access policies to safeguard user privacy in addition to offering granular access control for mHealth contexts. The demonstration of security proofs and the findings of the experiment made it abundantly evident that this method offers more security and efficiency. The possibility of malevolent individuals exploiting keys within user groups with similar properties was noted in real-world application scenarios. To address this risk, measures were required to track down and remove malicious users from the mHealth system.

For Internet of Things (IoT)-based healthcare systems, Maryam Nasr Esfahani et al. [40] proposed a blockchain-based end-to-end privacy protection framework. To safeguard patient data and location privacy against potential risks from both internal and external attackers, a three-layered hierarchical blockchain architecture employing ZKP and the ring signature technique was used. Furthermore, a technique provides unidentified authorization, authentication, and scalability, that were critical qualities in healthcare approaches. Both intuitive and formal security evaluations proved a scheme's robustness in contrast to a variety of attacks, including DoS, data tampering, mining, illegal storage, and replay attacks. A considerable percentage of the computational overhead was offloaded to Gateways (GWs) and Access Points (APs) to ease the computational burden on resource-constrained sensors. Furthermore, the intuitive security analysis emphasizes that this solution meets the system's critical security needs of confidentiality, integrity, and availability. It also emphasizes the method's ability to guarantee end-to-end privacy in healthcare systems through authentication, authorization, anonymity, and scalability. Importantly, the security analysis emphasizes the approach's resistance to numerous threats, such as DoS, data tampering, mining, illegal storage, and replay assaults. Furthermore, the presented method has the potential to be generalized to additional IoT applications with similar privacy concerns, perhaps extending to contexts such as smart city applications. However, the established

solution was required to reduce the GWs' overhead by utilizing a lighter ZKP system and providing flexibility in privacy necessities.

Lavanya Settipalli et al. [41] suggested the Extended Lightweight Blockchain (ELB) based integrated healthcare system for fraud prevention. A developed approach of integrated technique employs an ELB transformation for healthcare establishments, drawing inspiration from the lightweight blockchain concept. This solution efficiently attacks the issues that public blockchain networks frequently experience, such as computation overhead and excessive energy consumption. The ELB architecture, which functions as a decentralized authority, allows collaboration across multiple healthcare institutions. It was created on a consortium blockchain, defined as an authorized blockchain with numerous entities. This ELB design successfully integrates the advantages of lightweight and consortium blockchain, constructing a network with distributed authority while decreasing processing overhead. This framework has been systematically designed as an authorized network with numerous authorities, effectively mitigating problems associated with both single-authority networks like unauthorized networks, and potential data breaches, which may incur significant communication and computation overheads. The main objective of this framework is to avoid any kind of frustration in healthcare by implementing efficient smart contracts that start in real-time in further analysis.

Maddila Suresh Kumar et al. [42] developed the security of strong healthcare data transfer by utilizing blockchain based privacy. The developed method introduces Blockchain based Privacy Preserving and Robust Healthcare Data (BPPRH) for patient data management. The security of medical data delivered to patients via the internet is enhanced by this strategy. A hypervisor and Virtual Machines (VMs) were utilized to represent the cloud infrastructure. Various security concerns, including ransomware, malware injection attacks, Man-in-the-Middle attacks, hostile insiders, as well as Denial-of-Service assaults (DoS), may occur within the network during data transit or storage in the cloud. To address these issues,

Modified Fuzzy Particle Swarm Optimization (MFPSO) technique for threat identification was presented. When probable attackers were detected, an Edge-Cloud-based Collaborative System (ECCS) was utilized to protect data. To minimize these dangers, ECCS employs models such as Inverse Network, Regularized Maximum Likelihood Estimation, as well as Shadow Model Reconstruction. The results were evaluated utilizing important parameters such as false-positive rate, attack detection rate, CPU consumption, false-negative rate, and execution time. The results show that simulation performance improves significantly. The developed method improves privacy efficiency by ensuring system compatibility with minimal error rate and execution time while maximising the success rate.

P. Suganthi and R. Kavitha [43] used blockchain technology in conjunction with encoder-elliptic curve deep neural networks and quaternion-based neural networks to establish security and privacy for healthcare data in a cloud environment. The Advancement Data Security Architecture in Healthcare Environment (ADSAH) was a comprehensive system that integrates Elliptical Curve Cryptography (ECC) with blockchain and makes utilize of a Deep Fuzzy-Based Neural Network (DFBNN) to enhance the security of health data stored in the cloud. The method begins by encoding input medical data with an encoder and then employs ECC algorithms for data encryption. The secret encryption key was safely held within a blockchain architecture, increasing security even further. To enhance security, this key was smartly divided into blocks, and the SHA algorithm was utilized to identify important events inside these blocks. Authorized patients or physicians could access medical data by decrypting and retrieving the appropriate information utilizing the secret key. The established cryptographic approach streamlines complexity and reduces processing time by simplifying key generation, encryption, and decryption operations.

Usharani Chelladurai et al. [44] developed a new blockchain based EHR automation technique for healthcare. The established structure's main goal was to

facilitate the transfer of health information within a blockchain platform, thereby helping to establish a sophisticated e-health system. Several health models have been presented, including the utilisation of a Modified MT data structure to create immutable patient logs. This framework ensured that health records were securely stored and easily accessible. Furthermore, the system supports the update of medical data, the transmission of health information across multiple providers, and the creation of viewership contracts on a peer-to-peer blockchain network. This allows patients to easily access their EHR through healthcare professionals. This system's robust security and data integrity, accomplished through the utilize of cryptographic hash functions, were critical components. To evaluate the performance of the developed system, a series of experiments were carried out, directed at transaction response time, throughput, latency, and resource consumption. Outcomes showed that the blockchain method augments system throughput, performance, and network latency while utilizing fewer resources. However, the developed method was required to analyze and adopt the novel modified Merkle Tree data structure to ensure the integrity of the content.

Raghav et al. [45] presented the privacy protecting cloud data transfer for healthcare approaches with hybrid blockchain. This approach combines two independent schemes: Oblivious Transfer-Based Re-Encryption (OTRE) as well as Keyword-Based Re-Encryption (KRE), resulting in a hybrid blockchain system for safe health data exchange. KRE was developed to protect patient data privacy while providing keyword-based access with low-key management costs. OTRE extends KRE by utilizing Oblivious Transfer to protect user data and accommodate numerous data exchange scenarios. Both methods resisted attempts at collaboration by both honest but involved cloud and evil users. The hybrid blockchain architecture does away with the necessity for a only trusted authority and permits secure, significant data transfer. Furthermore, by utilizing smart contracts, blockchain supports end-user authentication and data verifiability on the cloud. A privacy provisioning phase in the OTRE approach adds some time overhead. With formal security proofs, an existing architecture for both KRE and OTRE was

described, ensuring indistinct below selected plaintext attacks within a random oracle model. Security analysis demonstrates which privacy of data was maintained though exchanging data and protects against collaboration between an authentic but interested cloud and bad users. For small data, the encryption-re-encryption-decryption process was completed in milliseconds, with sublinear time scaling as data size increased, all while retaining low consensus times. The hybrid blockchain's high throughput indicates the feasibility and efficiency of both the KRE and OTRE schemes. However, the developed approach was required to enhance the blockchain with deep to secure more privacy protection for health data transmission.

Erukala Suresh Babu et al. [46] suggested the secure exchanging of EHRS by utilizing trust-based blockchain network with privacy. Hyperledger Fabric of permissioned blockchain was utilized in the developed solutions to provide a safe and trusted network for all stakeholders. This protects the truth of protected health data while also ensuring the validity and robustness of health access control. An ECDSA cryptosystem was utilized within the healthcare blockchain network to provide secure and anonymous interactions among nodes for the seamless transfer of healthcare data in a data-transfer network. To address data privacy concerns, the designed healthcare blockchain method incorporates an Online/Offline structure. This structure has two separate modes of operation: i) Online-Chain: Because it does not involve substantial computations and involves less record data directly saved on the blockchain network. This speeds up block processing. ii) Offline-Chain: Data was stored in local databases, with offline data connections and indexes published on the blockchain. Two major objectives are achieved by this method: it guarantees the safe retention of medical records and speeds up the verification procedure. Complete supply chain traceability, fewer redundant tests and needless services, more accountability, the protection of important records, a restriction on the unauthorised transfer of EHR documents, and decreased costs for all types of care are further benefits of an all-inclusive system. However, the created method

was necessary to give healthcare providers access to EHRs and to offer great flexibility, low operating costs, etc.

Youyang Qu et al. [47] suggested privacy-aware and trustworthy data transfer by utilizing blockchain for edge intelligence. To protect secure health data, a tailored differential privacy model was developed, taking into consideration user trust levels. To accomplish individualized privacy protection, the model utilized a modified link community algorithm, with a significant change in the final step requiring users to belong to a single community. Within the context of differential privacy, trust levels were assessed based on a given community density, and the matching privacy protection level was connected with adjustable randomized noise limits. A noise correlation decoupling technique was carefully built utilizing a Markov Stochastic procedure to prevent linkage assaults in personalized differential privacy. In addition, a blockchain-based community architecture was developed to reduce the risk of poisoning assaults during differentially secure data transmission through Secure Health Networks (SHNs). Extensive testing and analysis on real-world datasets confirmed the efficacy of the developed approach, which beat previous research in terms of privacy protection and overall efficiency. Community detection was a crucial procedure in the established technique, but it was difficult to manage the granularity.

Omaji Samuel et al. [48] developed the COVID-19 healthcare system driven by federated learning and blockchain. Initially, a FL system was developed to address the issues of data privacy and COVID-19 prediction inefficiency. Following that, blockchain was implemented to assure entity trust, data immutability, availability, and information security. To build blocks and select miners, the blockchain system utilized a novel consensus process based on the reinforcing addition game. In addition, an epidemiological model was created to account for the influence of blockchain on COVID-19 control and prevention. Privacy and security evaluations illustrate that the built privacy structure was resistant to data security associated threats. For securing identification of CDC, security parameters for calculating a

computational logarithm in the finite field difficulties were developed, and a multilateral procedure based on bilinear maps was applied. Furthermore, developed infrastructure model solves technological limits in public communication. It also explains how to encourage public health policies throughout global health crises like COVID-19 pandemic. However, the presented technique requires real-time applicability and scalability for definite implementation.

Lokesh Lodha et al. [49] suggested the blockchain-based secured system through the IoMT network for e-healthcare monitoring. A Blockchain-based IoMT Security System (BC-IoMT-SS) was presented, which utilizes a blockchain approach within IoMT to enhance patient privacy, security, and administration. In order to satisfy the stringent privacy and security requirements needed for medical data management in IoMT devices, the created framework was successfully deployed. The healthcare application system was created to ensure that an individual's health data may safely trigger alarms utilizing blockchain keys validated by healthcare practitioners. Once patients were enrolled and authenticated, transactions including patient information and device details were carried out within the IoMT network, and this data was securely kept on the blockchain. The framework delivered equal services to authorized peers, with administrative nodes playing a critical role in data processing before transmission. In certain cases, utilizing fog computing's ability to decrease latency emerged as a substantial advantage. Several novel concepts, including software-defined networking, were introduced to the market. IPFS, a secure and distributed storage protocol, was utilized to regulate the needed storage capacity in terms of KB for a certain volume of transactions within the IoMT system. But to make the framework more scalable, off-chain activities had to be done, and as more transactions were made, more storage space was needed to hold the results.

Based on blockchain for e-health applications, Hanan Naser Alsuqaih et al. [50] introduced an effective privacy-preserving control mechanism. The created approach employs an effective access control mechanism, allowing data owners to

require their ideal access controls for sensitive medical data. The developed system makes extensive utilize of blockchain, which stores hashes of individuals' healthcare data and their access control settings. Users could apply their transactions to produce keys, as well as grant or revoke access to authorized doctors. The processing time of this method was extremely fast, clocking in at just 5 seconds, demonstrating its efficiency when compared to standard approaches. The health-chain system's sustainability for integration into smart healthcare systems was demonstrated through investigative data analysis and security assessments. Health-chain also acts as a preventive mechanism against medical conflicts, making it difficult to change or remove IoT data or doctor diagnoses. Extensive analysis validates blockchain's computing efficiency as well as time-saving benefits, as well as its robust capabilities in solving a variety of security requirements. The limitations of the developed approach are in its ability to resist future quantum attacks that could raise problems with the development of quantum computing.

Mohit Kumar et al. [51] developed the blockchain based secure and dependable data transfer framework for cyber-physical healthcare system 4.0. To progress in Healthcare 4.0, the developed system combines technologies such as Tendermint, MongoDB, BigchainDB, IPFS, and AES encryption techniques. Initially, the concept was intended to handle EHR storage and transfer by establishing a decentralized platform that attempted to replace the existing centralized system through the utilisation of blockchain. Following that, the Blockchain-enabled architecture was constructed, integrating Tendermint and IPFS technologies to address common difficulties in existing EHRS systems, such as data leakage, data fragmentation, and unauthorized patient data access. With the utilize of the blockchain-enabled AES-256 algorithm for data protection, the solution effectively retained privacy and security. Furthermore, the solution demonstrated a secure healthcare architecture enabled by blockchain for simplifying record access and management between doctors and patients. The blockchain-based EHR exchange solution was entirely patient-centric, allowing the owner complete data control and

leveraging blockchain to enhance security and privacy. To enhance security and privacy, the developed approach was patient-centric, with data control in the hands of the patient; even system administrators cannot access without user authorization. Nevertheless, the implemented methodology necessitated expansion to transmit voluminous quantities of data via the cloud and oversee intelligent technologies.

Randa Kamal et al. [52] developed the combined healthcare systems based on blockchain for IoMT applications. The advanced method includes medical sensors that allow for the secure transfer of encrypted health information via mobile devices, protecting patient privacy when sharing data with clinicians. The Care4U healthcare system does this by combining mobile-based encrypted IoMT data transfer, cancellable biometric identification for better security, and blockchain for the safety and integrity of health data. Chain1, Chain2, and Chain3 were three interconnected consortium blockchains that make up the blockchain layer, each of these chains provides a distinct function. Chain1 was in charge of keeping revocable biometric credentials, with each organization wishing to record the method needed to supply a facial image for authentication. Chain2 was focused on recording doctor's prescriptions and recommendations based on a patient's health data. Chain 3 contains information about the procedures involved in the provision of prescription medicines by pharmacists, which was critical for care providers to understand. These three consortium blockchains were developed to optimize transaction load distribution and reduce transaction latency. These blockchains collectively store system entity credentials, hospital prescriptions, and recommendations based on data provided over mobile and medical treatment. Additionally, the use of reversible biometrics enhances security and strengthens authentication in well-established medical procedures. But the created Care4U model needed to be expanded to cover a number of other healthcare systems, such as secure real-time health monitoring systems in the context of smart cities and video and speech data management.

Sarath Sabu et al. [53] presented the application of secure and privacy-aware e-health records and IoT data transfer utilizing blockchain. The developed method was designed through the parameter of General Data Protection and Regulation (GDPR). The concern organization was a procedure which attains a difficulty or concern that provider approaches of tracking over issues addressing phases. It was an authorized framework that established directions for the privacy of individual data of people who exist in in European Union (EU). Concern management was a technique for identifying and addressing challenges or concerns using an organized problem-solving approach. This system's employs of blockchain technology acts as a secure and decentralized record-keeping mechanism. It stores data in a distributed database in which records are saved in blocks associated together to form a chain, also known as a blockchain. The Medical Health Record Chain (MHR Chain) was the name given to the intermediary platform in this scenario. Patients commence their involvement in this model by enrolling on the platform and giving the essential information. Patients can contribute their medical record details, including PDF or image record files once they have registered. These records were kept in a dispersed setting. The utilization of IPFS, an open-source file system that provides a decentralized platform for storing data and files through high integrity and robustness, was an essential component of this system. Here, it will be first uploaded in the IPFS when a patient uploads a medical record. The medical record system has limits since it allows doctors or hospitals to access patient records, which has an impact on the healthcare industry.

Yuan Liu et al. [54] introduced the blockchain-empowered Federated Learning (FL) in healthcare-based CPS. A unique record was sustained by the Task Force Committee assembled by representatives of hospitals performing FL tasks. Secure FL task model training-based permission procedure was designed to assure data consistency, resulting in the development of coherent data blocks. In addition, a contribution point-based incentive procedure was developed to evenly recompense FL participants for providing their local data. A voting-based task list generating technique was developed specifically to obtain a consensus on tasks between FL-

TAC. The creation of new data blocks resulted in the creation of trained models based on a secure mapping matrix, with all hospitals taking part in model validation and block verification. Finally, FL participants' Shapley-based contributions were calculated, and CPs for specific tasks were distributed correspondingly. Hospitals that contributed significantly received more CPs, increasing their voting weight. The created system's efficiency was evaluated using actual healthcare data, and the numerical results proved its capacity to accomplish honesty in FL model combination and efficacy in delivering incentives to FL participants. However, to analyze the impact of various parameters, the proposed method required numerous numerical evaluations to analyze the number of K-hospitals, and l-data dimension.

Guangjun Wu et al. [55] suggested a blockchain-based smart healthcare classification through the protection of fine-grained privacy for reliable data replacement and transfer between various users. The blockchain-enabled dynamic access control structure integrated through Local Differential Policy (LDP) approaches was designed to protect attribute-based privacy in transaction systems. The many types of smart contracts used in architecture were created to assess and meet the needs of anonymous transactions, public data evaluation in an open network, dynamic access control, and advantageous matching judgements. Sensitive EMR attributes were divided into multiple phases and allocated different privacy budgets to randomly assign the attributes before data publication and ensure fine-grained privacy protection. Also, a function of data quality was designed for representing a disturbance acquired by LDP-based privacy preferences at requester view, and currently appropriate several matching results between participants for valuable transactions. The prototype system accomplishes configuration of individual-centric privacy formation at patient position though offering error definite data at the requester site. However, the created approach needed to simultaneously address difficult IoMT challenges and increase the flexibility of access control opinions as privacy security.

Table 2.1 Literature Review Overview

Authors	Methodology	Privacy Preservation	Scalability	Efficiency	Security Features	Limitations
G. Amudha [18]	DTARM for information retrieval	Moderate	Moderate	Improved retrieval rate	Authentication techniques, trimming tree	Requires blockchain update for transactions
Ti-Wang et al. [19]	DP-ABE for secure transfer	High	Moderate	High	Attribute-based encryption, CCA security	Time complexity issue
Ruyan Liu et al. [20]	Trusted data storage	High	High	High	LDPC codes, STM-Tree, sharding	Requires coded computation for transactions
Da-Yu-Jia et al. [21]	SE-Chain model	High	Moderate	High	AB-M Tree, reliability validation	Storage decreases as data grows
Duo Zhang et al. [22]	Secure data transfer	High	Moderate	Moderate	Smart contracts, access control	IoT security in human domain
Xu Yuan et al. [23]	EBRC consensus	Low	Moderate	Moderate	Byzantine fault tolerance, reputation-	Reliance on universal set

					based system	
Renpeng Zou et al. [24]	Medical data transfer	High	High	Moderate	Proxy re-encryption, reputation system	Requires improved throughput
Xu Ma et al. [25]	Trusted data transfer	High	Moderate	High	CP-ABE, searchable encryption	Reliance on universal set
Rajesh Kumar et al. [26]	AI & Blockchain for CT image	High	Low	Low	Smart contracts, encryption	High computational power needed
Mengji Chen et al. [27]	Blockchain for diabetes detection	High	Moderate	Moderate	IPFS, symptom-based diagnosis	Needs an advanced attack-resistant model
Desire Ngabo et al. [28]	Medical data security	High	Moderate	Moderate	ECC digital signatures	Requires keyless decentralized access
Ibrahim Abunadi et al. [29]	EHR security framework	High	Moderate	High	Access control, lightweight transfer	Needs industry-wide adaptation
Mary Subaja Christo et al. [30]	ECC-based security for healthcare	High	High	High	ECC encryption, edge computing	Needs deep learning enhancement for ECC

Jasleen Kaur et al. [31]	EHR privacy with IB-PRE	High	Moderate	Moderate	IB-PRE, IPFS, smart contracts	Needs faster query replies
Chandra mohan Dhasarathan et al. [32]	Federated learning-based privacy	High	Low	Moderate	Smart contracts, encryption	Needs improved data privacy
Kanika Agarwal et al. [33]	MyEasyHealthcare system	High	High	High	Triple-layered security, smart contracts	High growth potential
Deepa Rani et al. [34]	IoT-based healthcare framework	Moderate	Low	High	AES encryption, PoA consensus	Needs data analysis features
Amal Abid et al. [35]	NovidChain for COVID-19	High	Low	Moderate	Self-sovereign identity, selective disclosure	Needs Fog/ML integration for scalability
Wenkang Liu et al. [36]	Privacy protection for IoMT	High	Moderate	Moderate	Federated learning, differential privacy	Slower than traditional FL techniques
Hasan Al-Aswad et al. [37]	ZKP-based healthcare security	High	Moderate	High	Zero-knowledge proof, smart contracts	Requires better organizational understanding

Shixiong Yao et al. [38]	Privacy-preserving health code	High	Low	Moderate	Attribute-based encryption, searchable encryption	Deficiencies in privacy and auditing systems
Shujiang Xu et al.[39]	mHealth data transmission	High	Low	Moderate	Trust-based authentication	Vulnerable to malicious key exploits
Maryam Nasr Esfahani et al. [40]	End-to-end privacy protection	High	Moderate	High	ZKP, ring signature	Requires lighter ZKP system for scalability
Lavanya Settipalli et al. [41]	ELB-based healthcare system	High	High	High	Lightweight blockchain, smart contracts	Real-time smart contracts needed
Maddila Suresh Kumar et al. [42]	Privacy-preserving healthcare data	High	Moderate	Moderate	MFPSO, edge-cloud system	Needs better success rate
P. Suganthi and R. Kavitha [43]	Neural network-based privacy	High	Low	Moderate	Quaternion neural network, ECC	Complexity reduction needed
Usharani Chelladurai et al. [44]	EHR automation	High	Low	Moderate	Modified Merkle Tree	Needs improved Merkle Tree adoption

Raghav et al. [45]	Hybrid blockchain for data transfer	High	Moderate	Moderate	OTRE, KRE, smart contracts	Needs deeper blockchain privacy
Erukala Suresh Babu et al. [46]	Trust-based EHR exchange	High	Low	High	ECDSA, Hyperledger Fabric	Requires better EHR availability
Youyang Qu et al. [47]	Blockchain for edge intelligence	High	Low	Moderate	Differential privacy, noise correlation decoupling	Difficult granularity management
Omaji Samuel et al. [48]	Federated learning for COVID-19	High	Low	Moderate	Blockchain-based FL, smart contracts	Needs real-time applicability
Lokesh Lodha et al. [49]	IoMT security system	High	Moderate	Moderate	Blockchain keys, IPFS	Needs off-chain operations for scaling
Hanan Naser Alsuqaih et al. [50]	Privacy-preserving e-health control	High	Low	Moderate	Access control, blockchain ledger	Vulnerable to quantum attacks
Mohit Kumar et al. [51]	Cyber-physical healthcare 4.0	High	Low	Moderate	AES encryption, IPFS, Tendermint	Needs scalability for large data transfers
Randa Kamal et al. [52]	IoMT healthcare system	High	Low	Moderate	Cancellable biometrics,	Requires extension to

					blockchain layers	real-time systems
Sarath Sabu et al. [53]	GDPR-compliant e-health records	High	Moderate	Moderate	IPFS, smart contracts	Limited access for other providers
Yuan Liu et al. [54]	Federated learning in CPS	High	Moderate	Moderate	Voting-based FL, Shapley-based rewards	Needs more evaluations on hospital data
Guangjun Wu et al. [55]	Privacy-preserving smart healthcare	High	Moderate	High	Differential privacy, LDP	Complex IoMT security challenges

2.2 PROBLEM STATEMENT

The integration of blockchain technology into healthcare systems has shown promise in addressing critical challenges such as data security, privacy concerns, and efficient data transfer in the realm of the Internet of Medical Things (IoMT). However, despite the advancements outlined in the literature, several significant issues persist, warranting further exploration and solution-building:

- **Privacy Concerns and Data Security**: Existing blockchain-based healthcare systems offer improved data security through decentralized record-keeping mechanisms. Nevertheless, these systems still encounter challenges in ensuring robust patient privacy and controlling access to sensitive medical records. Moreover, concerns remain regarding the secure transfer and storage of large volumes of medical data, particularly in real-time settings and during data transmission between healthcare providers.

- **Scalability and Efficiency**: While blockchain technology provides inherent security benefits, concerns regarding scalability persist, especially when accommodating the vast amount of data generated by IoMT devices. Current systems face challenges in efficiently managing and processing this data, impacting system performance, transaction speed, and computational overhead, particularly in scenarios with increasing numbers of users.

- **Interoperability and Integration**: Blockchain struggles to connect smoothly with existing healthcare systems, making it hard to share patient records efficiently.

- **Usability and Adaptability**: The practical implementation and user-friendliness of blockchain-based healthcare systems require further enhancement. Solutions need to focus on user accessibility, ease of data exchange, and adaptability to diverse healthcare environments while ensuring compliance with regulatory standards such as GDPR.

- **Optimization of Data Processing**: Efficient utilization of distributed ledger technology (DLT) in healthcare demands optimization strategies to balance data processing, storage requirements, and computational costs. Addressing these aspects becomes crucial for the successful deployment of blockchain solutions within the healthcare ecosystem.

2.3 OBJECTIVES

The objective of research is to propose an efficient data sharing and retrieval approach in blockchain for smart healthcare.

Sub-objectives

1. To propose an efficient data sharing scheme in a blockchain.
2. To design an efficient data retrieval algorithm for the data sharing mechanism.

3. To measure the performance of the proposed algorithm using parameter such as transaction throughput, storage cost, and security.

2.4 SUMMARY

When data exchange is essential during treatment, the process of storing and accessing scattered health information of patients across numerous medical centres can be exceedingly time-consuming and resource intensive. Medical data can be stored in the cloud for several reasons, including scalability, low cost, quick access times, high availability, and flexible capabilities for tasks such as patient health diagnosis, monitoring, e-healthcare models, and m-healthcare models. However, these alternatives frequently demand more robust encryption mechanisms, secure storage techniques and effective access controls. Blockchain secures IoT data by preventing duplicates and attacks. Each block is processed to find what's needed. In IoT environments, blockchains are utilized to get critical information from several blocks. As a result, blockchain-based approaches within IoT-based healthcare systems that can secure patient privacy are lacking, particularly in circumstances when all system performers are deemed undependable.

CHAPTER 3
A BLOCKCHAIN-BASED SOLUTION FOR EFFICIENT AND SECURE HEALTHCARE MANAGEMENT

Healthcare becoming an essential and rapidly changing field, demands advanced technologies for handling medical information and ensuring data security. The research developed a blockchain-based healthcare management system that addresses the critical difficulties of secure medical data sharing. The approach employs the Zero-Trust concept and blockchain technology to ensure compliance with medical records and to promote secure data interchange between research institutions, servers, and patients. In this research, the DZTBS is developed for storing and encoding data to improve the retrieval of secure data. The developed approach efficiently meets the integrity, availability, and confidentiality security and privacy requirements. Particularly, as compared to standard systems, DZTBS delivers a better reduction in overall execution and block-generation time. Additionally, when compared to the existing encryption approaches such as the AES and the ECDSA, the developed approach achieves better encryption and decryption time. These outcomes indicate that the developed DZTBS achieved enhanced security and efficiency in healthcare management.

3.1 INTRODUCTION

The healthcare sector is vital because it provides essential medical services and continually works to improve patient outcomes through technological developments, novel treatments, and public health efforts. Despite these advances, preserving the security and privacy of patient data remains an important concern in the healthcare industry [56]. The standard healthcare system manually keeps the patient's health data, which results in inaccuracies and misconceptions about human health. As a result, health-related data from patients must be preserved in the form of EMRs [57]. With the constant development of information technology in the medical field, EMRs are highly regarded and widely utilized for efficient and superior e-healthcare services [58]. Due to the large volume of various kinds of

health records, providers face numerous challenges in verifying, securing, and storing health records [59]. Because patient data is managed by a third party and accessible without the patient's authorization may lead to security issues [60]. In comparison to traditional paper-based medical records, EMRs provide more efficient sharing between numerous institutions, secure data loss prevention, enhanced traceability, and a variety of other superior features [61, 62].

EHR security can be improved further by utilizing the technology of blockchain, which allows for the development of an open and dispersed online data folder including data list configurations that are related to one another [63]. Presently, blockchain is regarded as one of the most recent extremely secure and transparent innovative approaches for ensuring data and system security, privacy, and accuracy [64, 65]. As a result, blockchain has emerged as an essential approach for evolving healthcare standards [66]. Numerous industries have benefited from the advancement and efficacy of blockchain technology. It can be employed to maintain an unalterable log of the events that a product or service goes through from its origin to its current condition [67, 68]. Outsider adversaries are typically prevented by encryption and authentication mechanisms, but the major problem arises from malicious acts that generate attacks, such as eavesdropping, Denial of Services (DoS), and replay attacks [69]. The blockchain ensures that users maintain ownership and control over their data. The system recognizes that the user owns the data and provides access to healthcare providers only after the user's approval. Access control is fine-grained which improves compliance with data privacy and security [70].

3.2 CONTRIBUTION

Various contributions of the research are mentioned below:

- The DZTBS approach is developed for storing and encoding data to improve the retrieval of secure data that efficiently meets the integrity, availability, confidentiality, security and privacy requirements.

- The technology of blockchain is combined with zero-trust principles to create an efficient healthcare management system that enables the secure sharing of EHRs.
- The developed approach is evaluated using various performance metrics like block production time, blockchain memory, total transaction time, time spent on execution, proof generation, evidence verification, and key generation.

3.3 PROPOSED METHODOLOGY

In this research, the DZTBS approach is developed to secure and efficient healthcare management. Generally, patients' medical information is transmitted and maintained in the healthcare system via the technology of blockchain by clinicians, physicians, and diagnostic laboratories. In this situation, blockchain technology is effectively used to detect errors in medical data. Due to there being no owners in the technology of blockchain, the data must be secured via an effective cryptographic approach while the data flows across a network [71]. Figure 3.1 indicates the block diagram of a healthcare management system.

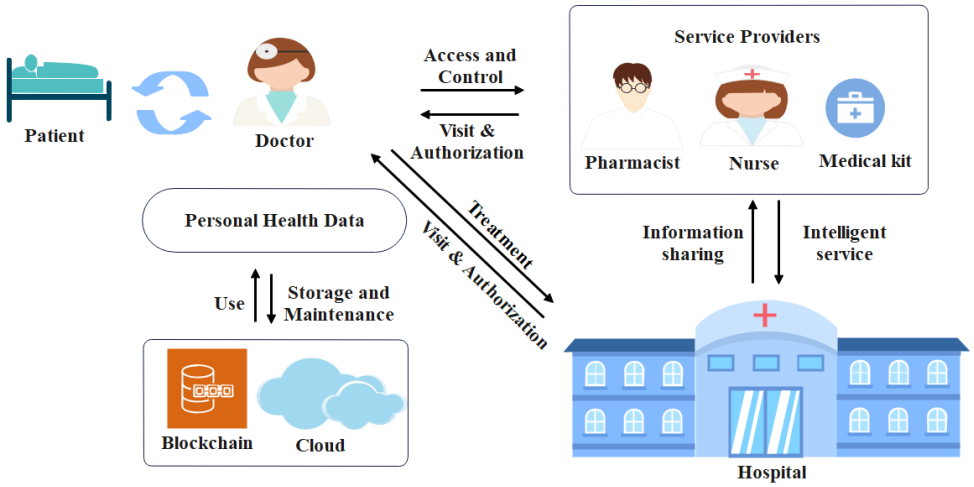

Figure 3.1Block diagram of a healthcare management system

3.3.1 PERSONAL HEALTH DATA

The personal health data is the medical information about patients they gather and maintain. The laboratory and test outcomes, medical history, treatment analysis, mental health condition reports, and insurance data are examples of health data. Personal health data allows the ability to privacy with the demands of organizations and individuals providing healthcare services to collect, use, and disclose.

3.3.2 SERVICE PROVIDER

Healthcare data is provided by nursing homes, hospitals, physicians, clinics, and other healthcare facilities. The data contains the health enhancement, disease prevention, diagnosis, and treatment procedure [72, 73]. Health data provides positive effects on development, economic progress, and both individual and public health.

3.3.3 CLOUD PLATFORM

Using a cloud platform increases the healthcare management system's efficiency while decreasing its cost. The cloud platform manages telehealth apps, maintenance, backend support functions, high security, and simple sharing of medical data. The cloud-based healthcare management solution decreases operational procedures while assessing improved services through personalization. The most effective health services are provided through an efficient process. Cloud computing has disaster recovery solutions, but in the event of a breach, healthcare providers' data is not lost [74].

The cloud-based system is versatile, inexpensive in terms of computing, and obtains better financial approaches. The key benefit of having an EHR platform [75, 76] in the cloud is the reduction in having to carry medical records while going to the hospital to meet with a doctor. The cloud platform enables improved data exchange, allows doctors to monitor consultations with hospital staff, and allows for data sharing.

3.3.4 BLOCKCHAIN TECHNOLOGY

The storage of patient's medical data within the healthcare management system generated accurate medical results by employing the technology of blockchain, which effectively addresses challenges associated with deception in clinical trials. Blockchain technology enables the access of longitudinal healthcare records [77, 78]. Furthermore, blockchain technology enables doctors to seek patient information across several systems, thus solving the issue of interoperability.

In the current environment, blockchain technology is employed for transferring and storing digital data, but the information cannot be modified. Furthermore, immutable ledgers and transaction records cannot be identified, removed, or deleted [79]. A drawback of employing blockchain technology is the cost of storing large numbers of medical records, and also the complexity of querying statistical data [80-82]. As a result, blockchain technology is being employed with artificial intelligence approaches to improve healthcare system quality, reduce costs, and thus make healthcare cheaper and more accessible. Patients can also upload EHRs to the medical blockchain, which hospitals can access with their consent. Figure 3.2 illustrates the EHR on a medical blockchain.

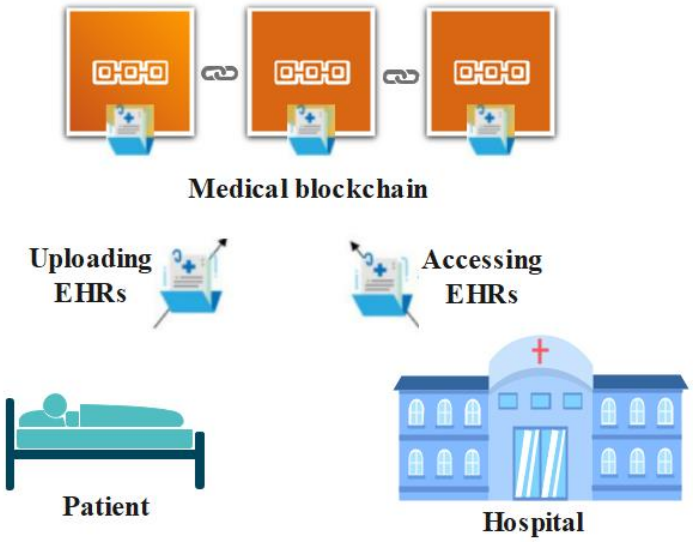

Figure 3.2 EHR on a medical blockchain

3.3.5 DISTRIBUTED ZERO TRUST-BASED BLOCKCHAIN STRUCTURE (DZTBS)

The DZTBS provides data security and user verification in this application by accomplishing different levels. The transmitter securely communicates vital EHRs to the receiver via three security layers like health parameter checking layer, the login layer, and the encryption layer.

Login layer: Initially, the login layer offers the greatest security and involves sender authentication via the end device using login credentials like username and password. In this case, the medical equipment is linked to personal computers.

Health parameter-checking layer: This layer validates the health parameters provided by the sender devices. The health parameter-checking layer determines whether the healthcare devices have recent protection and security updates. These procedures protect medical devices from being hacked.

Encryption: It is the third level of protection and it encrypts data. The data obtained by the health parameter-checking layer is encrypted using the receiver's public key. Only authorized personnel have access to the encrypted data in this case.

The receiver then examines the data by creating a web page or an application that includes three security layers: Two-Factor Authentication (2FA), a login layer, and the decryption layer.

Login layer: It is the highest security layer, and it includes receiver authentication using login credentials such as password and username, although it lacks immediate access.

2FA layer: For establishing the system, the 2FA layer requires two-step authentication. Third-party attackers are unable to access an online account or an individual's device since the authentication application produces a code for gaining access. In this case, the 2FA includes another layer of security to the system of healthcare management.

Decryption layer: Data decryption is performed in the decryption layer. In this layer, the receiver can access the encrypted data that has been passed to them after decrypting it using the private key (only authorized receivers can read the data).

The basics of blockchain technology and zero trust principles are integrated with DZTBS. In this case, zero-trust concepts are used for authorization and access control, while the technology of blockchain is used to ensure data decentralization and immutability. The following are the DZTBS's functionalities:

1st step: The smart contract examines the authorization roles and sender's privileges after the sender accomplished the login and health-parameter checking layers of security. If the request is available, the sender can process it and transfer the files (EHRs).

2nd step: The file is encrypted and stored in IPFS employing a symmetric key. The hash of the file is produced instantly, and it is known as ipfs-hash which indicates the file location in IPFS.

3rd step: The produced ipfs-hash is digitally signed with the sender's private key. Furthermore, the EHRs are encrypted using the receiver's public key.

4th step: After the receiver has passed through the login and 2FA stages of security, the smart contract compares the authorization tasks and the receiver's privileges. If the files are available, the receiver requests that they be extracted.

5th step: When the receiver's request has the right private key, the encrypted ipfs-hash is extracted from the blockchain. It is also decrypted and validated using the sender's public key.

6th step: Finally, the encrypted file can be obtained from IPFS employing the ipfs-hash and symmetric key. The user can view the requested file on the end device and the DZTBS algorithm is explained below.

Algorithm 3.1: DZTBS

Goal: Trust based Verifiable Blockchain based Hospital Information Software System with Secure Key Generation

Outcome: Blockchain Storage of Electronic Health Records

Step 1: Begin

Step 2: Initialize the key parameters

Step 3: Key generation: (Output: key generation point S_K)

3.1 Generate private key and public key pairs for user and server

3.2 U_k=User key & S_k=Server key

3.3 Share the public key between user and server

3.4 Compute the key generation point

Step 4: Encryption: (Input: documents, Output: encrypted-blocks)

4.1 Select the documents that need to be uploaded

4.2 Partition the documents into dissimilar data blocks

4.3 Encrypt every block using S_K

4.4 For every block, create a tag index

4.5 Store the data in blockchain storage

Step 5: Decryption: (Input: encrypted-documents, Output: decrypted-documents)

5.1 Choose the documents that need to be retrieved from blockchain storage

5.2 Retrieve all blocks of file from the block storage

5.3 Decrypt every block using S_K

5.4 Integrate all blocks and download as a single file

5.5 Save the data

Step 6: Blockchain server: (Input: documents and data block number, output: integrity check and recover original data)

6.1 Choose the file to verify

6.2 Select the block and enter the metadata length

6.3 Challenge the block for modification

6.4 If (ciphertext symbol missing)

Proof fails

Else

Proof verified

End

As demonstrated in Algorithm 3.1, the DZTBS algorithm aims to securely manage electronic health records using a trust-based verifiable blockchain system. The process begins with key generation in Step 3, ensuring that both the user and server possess their respective keys. Following this, Step 4 details the encryption process, where documents are partitioned, encrypted, and stored in blockchain format. Decryption, outlined in Step 5, ensures users can retrieve their documents securely. Finally, Step 6 involves the blockchain server performing integrity checks to confirm that the stored data remains unaltered.

3.4 EXPERIMENTAL RESULTS

In this research, the DZTBS approach is simulated using the Python 3.9 software tool with 64-bit Pycharm professional edition, version 2023. The DZTBS experimental research executes on a computer with a Windows operating system, 16 GB of RAM, and an i7 Intel core 12^{th} generation processor. The effectiveness of the DZTBS is evaluated using various performance metrics like block production time, blockchain memory, total transaction time, time spent on execution, proof generation, evidence verification, and key generation.

3.4.1 QUALITATIVE AND QUANTITATIVE ANALYSIS

The efficacy of the DZTBS is initially assessed using blockchain memory, total execution time, and block generation time. Table 3.1 demonstrates the performance of DZTBS in terms of blockchain memory, block generation, and total execution time. The blockchain memory ranges between 0.28 and 0.31 MB and the memory usage increases significantly as the number of blocks increases, although the overall difference is minimal. Furthermore, the block generation time is reliable around 0.99 seconds across all data points. This demonstrates that the system as a whole is still producing new blocks at a fairly steady rate. Total execution time grows

linearly with block size until it reaches 350 blocks. Following that, it experiences a dramatic jump due to resource constraints or system behaviour. The remaining data points 400-500 blocks execute at an average time of about 317 seconds. Figure 3.3 shows the graphical representation of DZTBS performance in terms of block generation, and total execution time. Figure 3.4 illustrates the graphical representation of DZTBS performance in terms of blockchain memory. When compared to conventional healthcare systems, the developed DZTBS effectively improves EHRs' trust level and security. Furthermore, the developed DZTBS provided greatly secure data transmission while consuming less energy, execution time, and memory usage.

Table 3.1 Performance of DZTBS in terms of block generation time and total execution time

Performance Measures		Blockchain memory (MB)	Block generation Time (seconds)	Total execution time (Seconds)
No. of blocks	10	0.28	0.99	40.88
	25	0.29	0.99	68.81
	50	0.29	0.99	97.73
	75	0.28	0.99	127.65
	100	0.29	0.99	157.57
	150	0.28	0.99	189.49
	200	0.28	0.99	210.43
	250	0.29	0.99	227.39
	300	0.28	0.99	277.25
	350	0.29	0.99	317.14
	400	0.3	1	317.15
	450	0.3	1.01	317.16

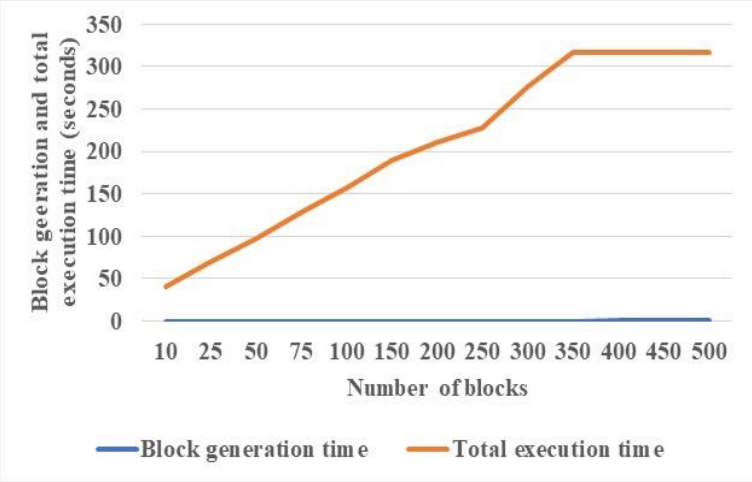

Figure 3.3 DZTBS performance in terms of block generation and total execution time

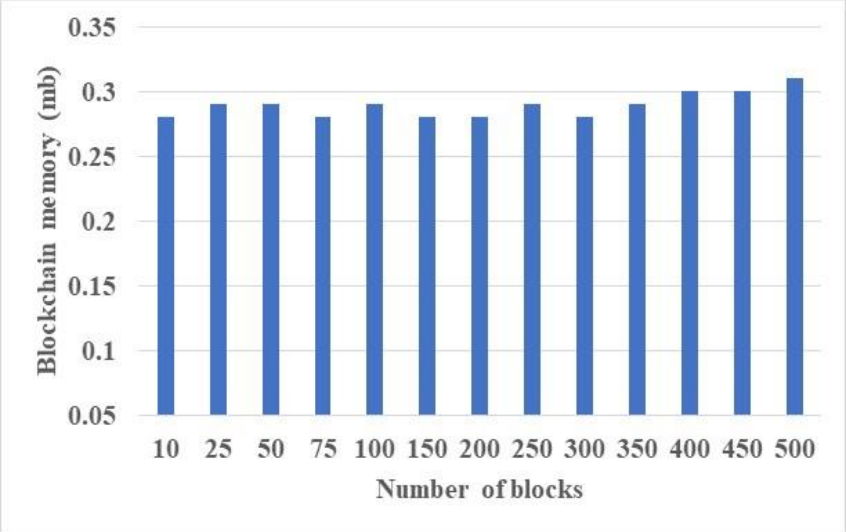

Figure 3.4 DZTBS performance in terms of blockchain memory

The combination of zero trust principles with the technology of blockchain substantially reduced the memory space and key management to store the user keys. Table 3.2 shows the performance of DZTBS in terms of key, proof generation, and proof verification. By enhancing the number of input/health records from 100 to 1000, the time of key generation is generally enhanced. The developed DZTBS scalability is improved by decreasing the time to produce key pairs. Furthermore,

the proof generation time is reduced linearly from 55 seconds to 50 seconds by increasing the number of inputs. However, increasing the number of inputs increases the proof verification time from 0.10 to 0.55 seconds. Figure 3.5 illustrates the graphical representation of DZTBS performance in terms of key and proof generation time. Figure 3.6 shows the graphical representation of DZTBS performance in terms of proof verification time. In general, the verification and key generation time increases as the number of input blocks grows due to the rise of data and patients. Since the decentralized architecture of DZTBS, the proof generation time remains constant.

Table 3.2 Performance of DZTBS in terms of key, proof generation, and proof verification time

Performance Measures (seconds)	**Number of inputs**				
	100	250	500	750	1000
Key generation time	15.50	16.10	16.60	16.70	17.20
Proof generation time	55	54	51	50	50
Proof verification time	0.10	0.18	0.31	0.49	0.55

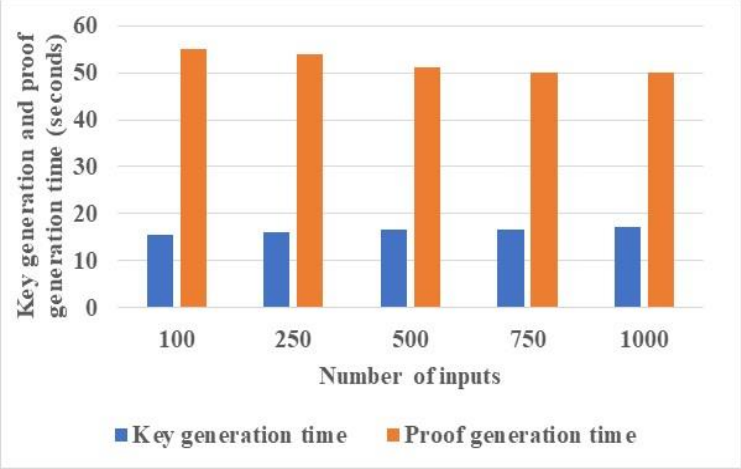

Figure 3.5 DZTBS performance in terms of key and proof generation time

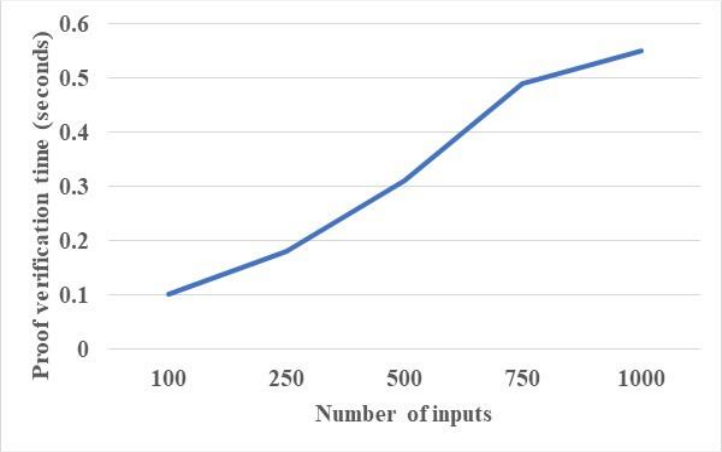

Figure 3.6 DZTBS performance in terms of proof verification time

Table 3.3 shows the performance of DZTBS in terms of proving key size, verification size, and proof size. By increasing the number of input/health records from 100 to 1000, the DZTBS proof size increases from 0.15 kb to 0.58 kb, the verification size drops from 59 kb to 54 kb, and the proving key size increases from 15.80 kb to 18.60 kb. Figure 3.7 illustrates the graphical representation of DZTBS performance in terms of proving key size and verification size. Figure 3.8 shows the graphical representation of DZTBS performance in terms of proof size. The proving key size, verification size, and proof size are direct implications of the number of inputs, and the experimental findings are within the range.

Table 3.3 Performance of DZTBS in terms of proving key size, verification, and proof size

Performance Measures (kb)	**Number of inputs**				
	100	**250**	**500**	**750**	**1000**
Proving key size	15.80	16.50	17	17.90	18.60
Verification size	59	56	56	56	54
Proof size	0.15	0.23	0.33	0.54	0.58

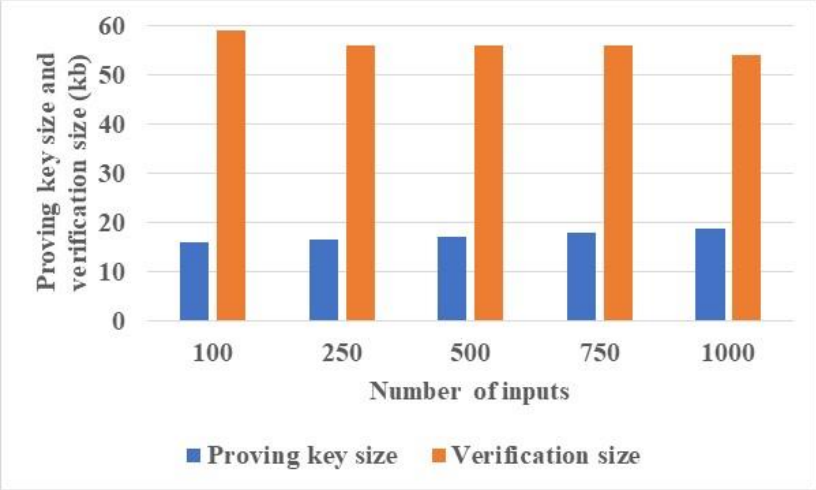

Figure 3.7 DZTBS performance in terms of proving key size and verification size

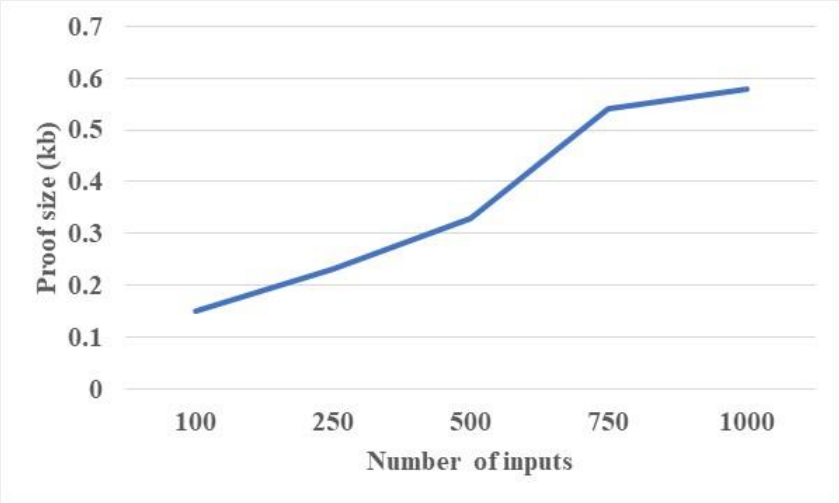

Figure 3.8 DZTBS performance in terms of proof size

Table 3.4 represents the evaluation of time overhead performance by utilizing access transaction, store transaction query-based, and store transaction time period. The performance of ZTA, ZTX, and ZTNA are measured and matched with the developed DZTBS. Figure 3.9 indicates the graphical representation of the time overhead performance with developed DZTBS. The obtained result shows that the developed DZTBS approach attains a greater store transaction time period, query-based, and access transaction which is better when compared to similar methods.

Table 3.4 Evaluation of Time Overhead Performance

Methods	Store Transaction time period	Store Transaction Query-Based	Access Transaction
ZTA	23	46	12
ZTX	29	52	14
ZTNA	31	55	16
Proposed DZTBS	35	60	18

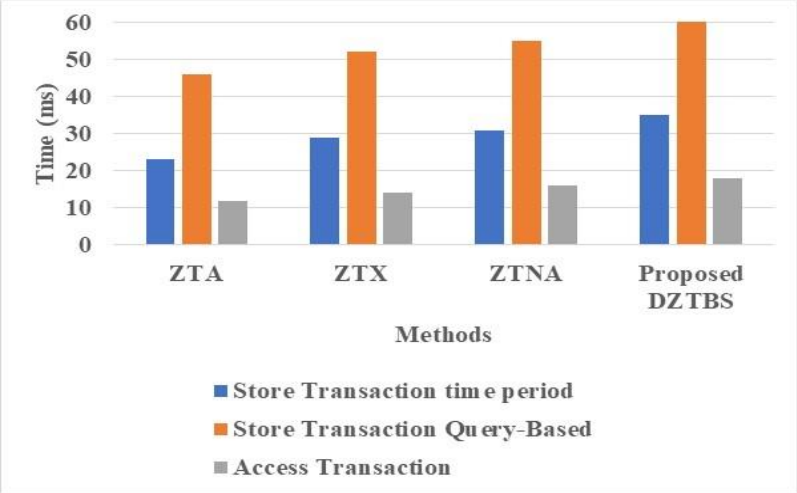

Figure 3.9 Time overhead performance

Table 3.5 represents the evaluation of energy consumption performance by utilizing access transaction, store transaction query-based, and store transaction time period. The performance of ZTA, ZTX, and ZTNA are measured and matched with the developed DZTBS. Figure 3.10 indicates the graphical representation of the energy consumption performance with developed DZTBS. The obtained result shows that the developed DZTBS approach attains a greater store transaction time period, query-based, and access transaction which is better when compared to similar methods.

Table 3.5 Evaluation of Energy Consumption

Methods	Access Transaction	Store Transaction Query-Based	Store Transaction time period
ZTA	`39.39	40.63	41.90
ZTX	45.07	49.19	49.99
ZTNA	50.78	51.20	50.25
Proposed DZTBS	56.41	56.45	56.49

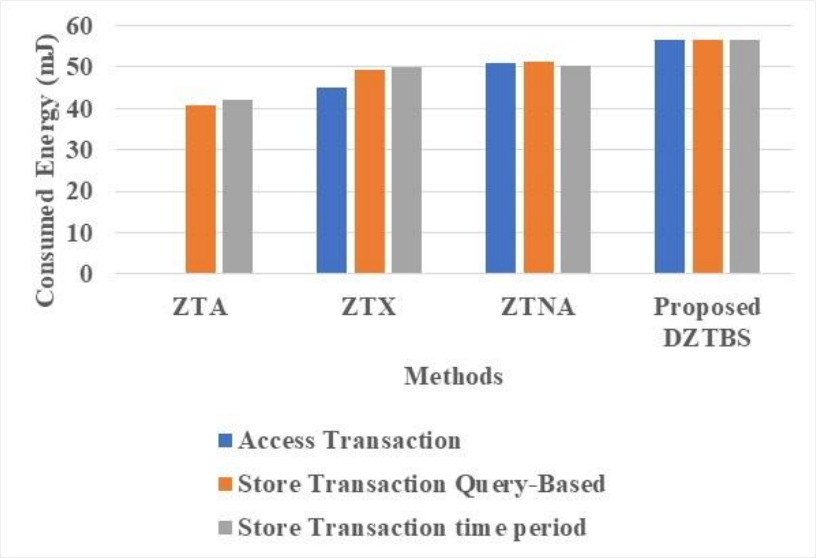

Figure 3.10 Energy Consumption performance

Table 3.6 represents the evaluation of packet overhead performance by utilizing a number of Overlay Block Managers (OBM). The performance of ZTA, ZTX, and ZTNA are measured and matched with the developed DZTBS. Figure 3.11 indicates the graphical representation of the packet overhead performance with developed DZTBS. The obtained result shows that the developed DZTBS approach attains a greater packet overhead which is better when compared to similar methods.

Table 3.6 Evaluation of packet overhead

Methods	**Number of OBMs**						
	0	7	10	13	15	17	20
ZTA	500	620	1500	2500	3200	3900	4900
ZTX	600	700	2200	3100	3700	5000	6000
ZTNA	750	850	2900	3500	4850	6260	7500
Proposed DZTBS	850	1020	3200	4700	5600	7100	9200

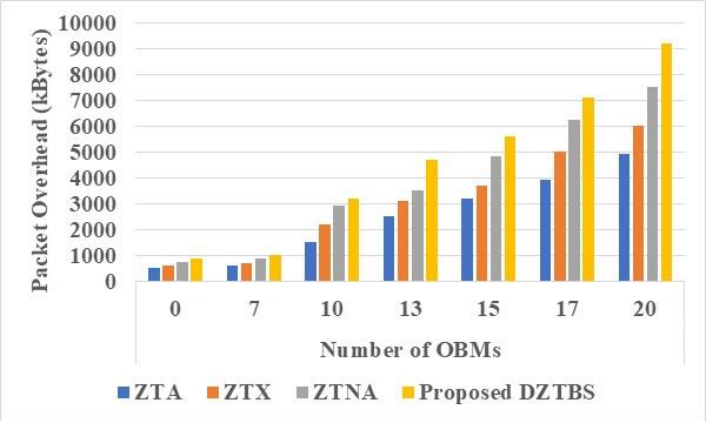

Figure 3.11 Packet overhead performance

Table 3.7 represents the evaluation of delay performance by utilizing the number of Overlay Block Managers (OBM). The performance of ZTA, ZTX, and ZTNA are measured and matched with the developed DZTBS. Figure 3.12 indicates the graphical representation of the delay performance with developed DZTBS. The obtained result shows that the developed DZTBS approach attains a less delay which is better when compared to similar methods.

Table 3.7 Evaluation of delay

Methods	Number of OBMs						
	0	7	10	13	15	17	20
ZTA	0.5	0.75	1.25	1.4	1.8	1.11	2.0
ZTX	0.45	0.71	1.2	1.25	1.75	1.10	2.2
ZTNA	0.3	0.65	1.0	1.2	1.7	1.9	2.3
Proposed DZTBS	0.2	0.5	0.9	1.0	1.5	1.8	2.4

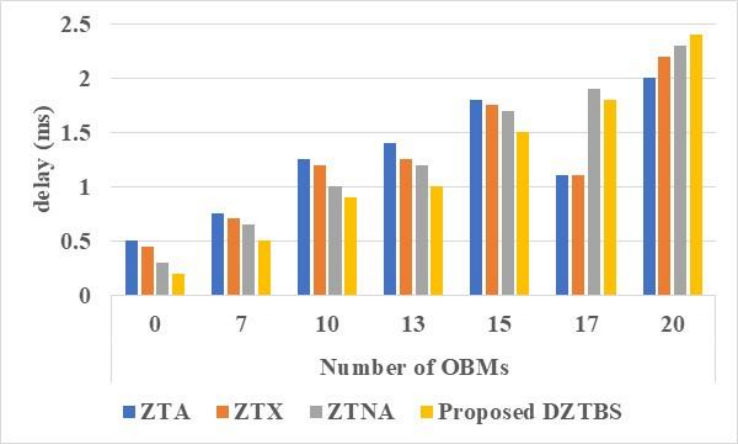

Figure 3.12 Delay performance Comparison

3.4.2 COMPARATIVE ANALYSIS

This section provides a comparative analysis of the developed DZTBS approach with a Max time, Min time, and Mean time which is shown in Table 3.8. The developed DZTBS has a minimal mean encryption and decryption time of 0.001053 seconds and 0.00365 seconds respectively. These times are slightly greater than those of the cryptographic approaches created by Chakraborthy et al. [83], which are higher than the AES but lower than the ECDSA. Figure 3.13 illustrates the graphical representation of comparative analysis with the DZTBS approach. Despite the slight reduction in processing time, the DZTBS achieves significant benefits with respect to functionality, overall efficiency, and security.

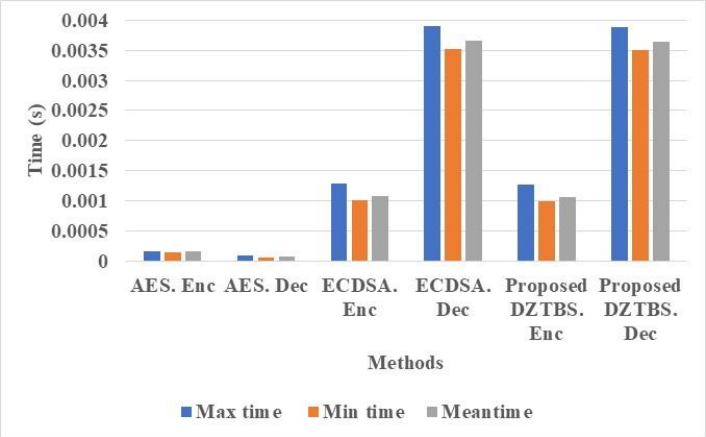

Figure 3.13 Comparative analysis with developed DZTBS approach

Table 3.8 Comparative analysis of existing method with developed DZTBS approach

Algorithm	Max time (s)	Min time (s)	Meantime (s)
AES. Enc	0.000160	0.000146	0.000158
AES. Dec	0.000083	0.000063	0.000077
ECDSA. Enc	0.001280	0.001011	0.001070
ECDSA. Dec	0.003902	0.003526	0.003669
Proposed DZTBS. Enc	0.001268	0.000993	0.001053
Proposed DZTBS. Dec	0.003886	0.003508	0.00365

3.4.3 DISCUSSION

The goal of this research is to improve the retrieval of secure data for storing and encoding data. Generally, patients' medical information is transmitted and maintained in the healthcare system via the technology of blockchain by clinicians, physicians, and diagnostic laboratories. In this situation, blockchain technology is effectively used to detect errors in medical data. Due to there being no owners in

the technology of blockchain, the data must be secured via an effective cryptographic approach while the data flows across a network. There are some limitations to a secure healthcare system such as the BOA having a data imbalance issue that needs to be solved to improve the security performance. When securing EHRs against external threads, the system of data-sharing and privacy-preserving public blockchain challenges issues like limited scalability and poor efficiency. However, the Proof of Work (PoW) consensus algorithm faces issues with energy-intensive and resource inefficiency for improving the security in the healthcare management system. The developed DZTBS overcomes this limitation in healthcare systems. The developed approach provides numerous benefits with respect to overall efficiency, integrity, confidentiality security, and privacy requirements. Particularly, as compared to standard systems, DZTBS delivers a better reduction in overall execution and block-generation time.

3.5 SUMMARY

Healthcare becoming an essential and rapidly changing field, demands advanced technologies for handling medical information and ensuring data security. In this research, the DZTBS approach is developed for secure data sharing and integrates smart contracts with a zero-trust approach and blockchain. The developed approach addresses two issues that are secure data sharing of EHRs and the privacy protection of medical records shared from various sources. When the medical records exceed requirements without sharing the patient's privacy, the zero-trust principle provides smart contracts. The developed approach provides numerous benefits with respect to overall efficiency, integrity, confidentiality security, and privacy requirements. DZTBS delivers a better reduction in overall execution and block-generation time. Additionally, when compared to the existing encryption approaches like the AES and the ECDSA, the developed approach achieves better encryption and decryption time. These outcomes indicate that the developed DZTBS achieved enhanced security and efficiency in the system of healthcare management.

CHAPTER 4
BLOCKCHAIN FOR PATIENT DATA INTEGRITY: DECENTRALISED STORAGE AND RETRIEVAL IN MODERN HEALTHCARE SYSTEMS

Information technology advancements and the rising demand for individualised, data-centric care are driving a digital revolution in the healthcare sector [84]. This has led to an unprecedented surge in healthcare information, including electronic health records (EHRs), medical images, wearable device data, and sensor data [85]. However, managing, securely sharing, and retrieving this data remains a challenge [86].

Traditional centralised data storage and management systems pose numerous risks, such as a single point of failure, data silos, and potential privacy breaches [86]. Blockchain technology offers a promising solution with its decentralised architecture and immutable, transparent, and trustworthy data-sharing capabilities [87]. In the context of smart healthcare, an efficient data exchange and retrieval system on the blockchain is essential [88]. Rapid access to comprehensive and accurate patient data can significantly impact clinical decision-making, treatment outcomes, and medical research [89].

4.1 CONTRIBUTION

This chapter proposes a comprehensive approach to addressing two primary objectives:

- Developing an innovative data-sharing system that harnesses the parallel and distributed computing capabilities of the blockchain network; and
- Proposing a robust data retrieval algorithm that locates specific healthcare data on the blockchain quickly and precisely.

We intend to leverage sharding and parallel processing to enhance data availability, sharing efficiency, and transaction speeds.

4.2 PROPOSED METHODOLOGY

In this chapter, we delineate two primary objectives: optimize data management and accessibility within the blockchain network.

Our initial focus is on the formulation of a data sharing scheme that exploits distributed and parallel computing capabilities. By harnessing these advanced techniques, we anticipate significant enhancements in data-sharing efficiency, increased data availability, and accelerated transaction speeds. This proposed framework integrates advanced consensus mechanisms, strategic sharding methodologies, and cutting-edge parallel processing algorithms. Through this integrative approach, we aim to optimize data distribution and dissemination across the blockchain network. Additionally, a pivotal component of our investigation encompasses privacy preservation to ensure that sensitive healthcare data is securely maintained, granting access solely to authorized entities.

Subsequently, we pivot towards the development of a robust data retrieval algorithm tailored for swift and precise access to specific healthcare information on the blockchain. With rapidly increasing data volume on the network, efficient data retrieval is crucial. This objective will entail the exploration of methods including, but not limited to, advanced indexing techniques, caching strategies, and refined search algorithms. Such a comprehensive approach will expedite the retrieval of pertinent patient records, medical documentation, and research data. Concurrently, our methodology addresses data privacy during retrieval, integrating stringent access control mechanisms to uphold patient confidentiality.

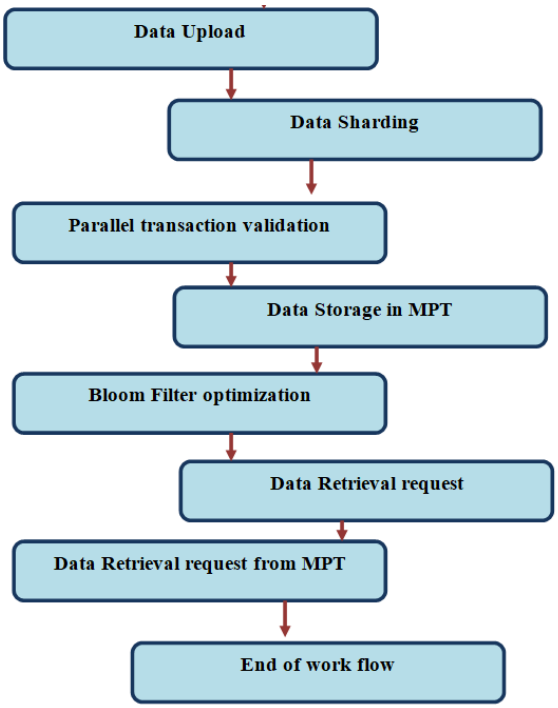

Figure 4.1 Proposed Workflow

In pursuit of these objectives, we endeavour to redefine data management paradigms within the blockchain infrastructure, promoting enhanced efficiency and security in healthcare applications. The culmination of this research is the design of the 'sHealthCareBlockchain' framework, as depicted in Figure 4.1, with its detailed mechanics discussed in subsequent sections.

4.2.1 PROPOSED DATA SHARING SCHEME

The chapter introduces a novel data sharing scheme in the blockchain for smart healthcare, leveraging a unique combination of distributed and parallel computing techniques. The proposed approach aims to optimize data sharing efficiency, scalability, and security while accommodating the unique requirements of healthcare data management. The new approach improves data accessibility, speeds up transactions, and promotes a smooth and safe data sharing environment for smart healthcare applications by utilizing both distributed and parallel computing within the blockchain network.

- **Dynamic Sharding Algorithm**

This chapter proposes an adaptable and novel dynamic sharding technique for a blockchain-based intelligent healthcare system. This method improves data sharing, scalability, and load balancing by dynamically adjusting the number of shards and their composition to changing network conditions and data distribution. Unlike other algorithms, this one can rapidly adapt to changes in network traffic, transaction volumes, and processing resources. This ensures optimal network performance and data accessibility for the intelligent healthcare blockchain.

Adaptive Dynamic Sharding Algorithm

The adaptive dynamic sharding technique adjusts the number of shards based on variables such as network size, transaction volume, and computational resources. Consider the following:

N : Nodes in the blockchain network as a whole.

T : Total volume of network transactions.

S : Number of Shards

S_min : Shard count that must be met for the system.

S_max : The most shards that can be present in the system.

The following equation illustrates how the adaptive dynamic sharding algorithm works. Equations 4.1 and 4.2 are used for computing the *Shard_Size* and *Transaction_Per_Shard* respectively.

$$Shard\_Size = N / S \tag{4.1}$$

$$Transaction\_Per\_Shard = T / S \tag{4.2}$$

We consider the transaction load per shard and track its variation to dynamically modify the number of shards. If the transaction load per shard,

Transaction_Per_Shard, exceeds a predefined threshold, *Transaction_Threshold*, we increase the number of shards to reduce the load on each shard and improve data sharing efficiency as shown in equation 4.3.

if *Transaction_Per_Shard* > *Transaction_Threshold* :

$$S = \min (S\_max, S * 2) \tag{4.3}$$

On the other hand, if the transaction load per shard drops below another predefined threshold, *Empty_Shard_Threshold*, we decrease the number of shards to consolidate data and optimize resource utilization as shown in equation 4.4.

if Transaction_Per_Shard < Empty_Shard_Threshold：

$$S = \max (S\_min, S / 2) \tag{4.4}$$

By continually monitoring the transaction load and dynamically adjusting the number of shards, the adaptive dynamic sharding algorithm ensures that the smart healthcare blockchain network remains scalable and responsive to changing demands.

Load Balancing Mechanism

To address load imbalance among shards, the algorithm employs a load balancing mechanism. To uniformly share the workload of transaction processing, this technique redistributes transactions among shards. Let:

Shard_Transaction_Counts: A list of transaction counts for each Shard

The following is a representation of the load balancing mechanism. Average number of transactions, *Calculate_Average_Transaction*,is computed using equation 4.5 as:

$$Calculate\_Average\_Transaction = \text{sum} (Shard\_Transaction\_Counts) / S \tag{4.5}$$

For each shard in *Shard_Transaction_Counts*, if the transaction count exceeds the average (*Calculate_Average_Transaction*), the system initiates load balancing. This process redistributes excess transactions to other shards, ensuring an even workload. The goal is to optimize performance and prevent any single shard from being overloaded. Equation 4.6 is used to show the load balancing criteria.

for each shard in *Shard_Transaction_Counts*:

if *Shard_Transaction_Counts* [*shard*] > *Calculate_Average_Transaction*:

Perform *Load balancing* (4.6)

Load Balance Factor

Redistribute transactions initially from (shard) to additional underloaded shards. The Load_Balance_Factor is a parameter that establishes how much redistribution of transactions is required for balancing. The technique makes sure that there is an equitable load distribution and reduces processing bottlenecks by periodically reviewing the transaction counts in each shard and redistributing transactions as necessary.

A highly flexible, scalable, and effective data sharing strategy for the blockchain for smart healthcare is produced by combining the adaptive dynamic sharding algorithm with the load balancing mechanism. This algorithm's dynamic nature enables the network to adjust to shifting circumstances and transaction volumes, resulting in increased performance for patients, researchers, and healthcare professionals as well as optimal data sharing efficiency.

- **Parallel Transaction Validation**

This study proposes an approach for parallel transaction validation in blockchain-based smart healthcare systems, utilising the Heinit method. This would enhance the efficiency of data sharing. The Heinit criterion refers to a mathematical approach utilised in the optimisation of parallel tasks. This method employs the utilisation of processing units to dynamically allocate resources for transaction validation. The utilisation of the Heinit criterion allows for the efficient distribution of transaction workloads among the available processing units. This facilitates the acceleration and equitable distribution of transaction validation. The implementation of this novel approach enhances the overall performance of the intelligent healthcare blockchain network and augments the utility of data sharing.

Heinit Criterion for Load Balancing

By distributing the workload across the available processing units, the *Heinit_Criterion* is a mathematical formula for optimizing parallel processing workloads. Let:

W: Each transaction's workload, expressed in computing units.

N: total volume of transactions that need to be verified.

P: number of processor units dedicated to parallel validation.

The following is a representation of the load balancing Heinit criterion:

$$Heinit\_Criterion = \sum(W_i) / P \tag{4.7}$$

where $\sum(W_i)$ indicates the total work done by all transactions.

To ensure the most effective parallel transaction validation, it establishes the appropriate workload distribution across processing units. By dynamically distributing transactions to processing units so that the workload is evenly distributed, the algorithm seeks to minimise the value.

Heinit-based Parallel Transaction Validation

The Heinit-based parallel transaction validation technique utilises the Heinit_Criterion to dynamically allocate transactions to available processing units. Let:

Transactions: List of incoming transactions.

P: Number of processing units allocated for parallel validation.

The Heinit-based parallel transaction validation technique can be represented as follows:

Step 1: Calculate the workload of each transaction, W_i, in the Transactions list.

Step 2: Calculate the Heinit_Criterion = $\sum(W_i) / P$

Step 3: Divide Transactions into *P* partitions while aiming to minimize the difference in workload sum across partitions, ensuring each partition has a workload close to the *Heinit_Criterion* value.

Step 4: Distribute each partition of transactions to the corresponding processing unit for parallel validation.

By using the *Heinit_Criterion* to dynamically allocate transactions among processing units, the technique ensures equitable distribution of transaction workloads, minimizing processing bottlenecks, and maximising resource utilization.

Parallel Transaction Validation Time with Heinit

The research proposes a revised equation to calculate the parallel transaction validation time considering the dynamically allocated processing units based on the *Heinit_Criterion*. Let:

V: Number of transactions to be validated.

P: Number of processing units allocated for parallel validation.

Heinit_Criterion: The calculated Heinit criterion value.

The parallel transaction validation time with Heinit can be represented as follows:

$$Validation\_Time\_Parallel\_Heinit = V / (P * Heinit\_Criterion) \quad (4.8)$$

In equation 4.8, the time taken to validate V transactions in parallel using *P* processing units, considering the *Heinit_Criterion*, ensures that each processing unit handles an optimized workload. This results in faster and more balanced transaction processing within the blockchain network.

The integration of the Heinit-based parallel transaction validation technique leads to a highly efficient, balanced, and responsive data sharing ecosystem in the blockchain based smart healthcare system. The use of the Heinit_Criterion optimises workload distribution, reduces processing disparities, and enhances overall performance, contributing to improved data sharing efficiency for healthcare providers, researchers, and patients.

- **Consensus-Driven Data Propagation**

To address data availability concerns, the proposed research introduces a consensus-driven data propagation mechanism. Let:

C: Consensus threshold required for data propagation

V: Number of validators in the network

The Data Propagation Time can be calculated as shown in equation 4.9:

$$Data\_Propagation\_Time = Time\ taken\ to\ achieve\ consensus\ among\ C\ out\ of\ V\ Validators \quad (4.9)$$

By requiring agreement among a predetermined number of validators, the research ensures that data is safely transferred around the network before being added to the blockchain. This approach lowers the possibility of data forks and makes data more accessible for efficient retrieval.

The research's objective is to create an innovative and effective blockchain ecosystem for smart healthcare by incorporating these cutting-edge techniques into the data sharing framework. A strong and scalable infrastructure will be created by combining dynamic sharding, parallel transaction validation, and consensus-driven data propagation to meet the requirements for data sharing of contemporary healthcare applications while maintaining data security and integrity.

4.2.2 PROPOSED DATA RETRIEVAL SCHEME

The study suggests a highly original and effective data retrieval technique for the blockchain-based smart healthcare data exchange mechanism. The innovative approach uses Merkle-Patricia Trie (MPT) and Bloom filters in tandem to retrieve data quickly and precisely while maximizing memory consumption. This cutting-edge method gives healthcare professionals and researchers seamless access to particular patient records and medical data within the blockchain, improving patient care, medical research, and analytics.

- **Merkle-Patricia Trie (MPT) Indexing**

The data recorded in the blockchain is indexed and organized using the Merkle-Patricia Trie (MPT) data structure in the research. The MPT is a modified Merkle tree designed specifically for storing and retrieving data quickly in a distributed system like the blockchain. Let:

H(x): Hash function to produce the data's hash value 'x'.

The following is a representation of the MPT indexing algorithm:

$$MPT\_Insert(data) \rightarrow root\_hash \tag{4.10}$$

$$\text{MPT\_Retrieve}(root\_hash, key) \rightarrow data \quad (4.11)$$

The functions *MPT_Insert* and *MPT_Retrieve* in the equations 4.10 and 4.11 are used to enter data into the MPT and to retrieve specific data using the MPT's root hash and a special key associated with the data, respectively. As each state of the MPT generates a distinct root hash, any changes to the data will result in a new root hash, allowing for quick data retrieval while preserving data integrity in the blockchain.

- **Bloom Filters for Efficient Key Lookup**

The suggested approach uses Bloom filters to quicken key lookup operations in order to better optimise data retrieval efficiency. A probabilistic data structure called a bloom filter effectively checks if an element is present in a set. Let:

K : Number of elements in the set (keys in the MPT).

The Bloom filter algorithm can be represented as follows:

$$Bloom\_Insert(key) \rightarrow Bloom\_filter \quad (4.12)$$

$$Bloom\_Lookup(Bloom\_filter, target\_key) \rightarrow \text{Boolean} \quad (4.13)$$

Here, the Boolean value in Eq. 4.13 will be true if target_key is likely in the set and false otherwise.

The *Bloom_Insert* function as shown in equation 4.12 is used to add keys to the Bloom filter, and *Bloom_Lookup* function in equation 4.13 is employed to check the probable existence of a target key in the filter. By using Bloom filters, the algorithm reduces the need for extensive disk or memory access for key lookup, thereby accelerating data retrieval operations.

- **Efficient Data Retrieval Algorithm**

The proposed research integrates the MPT indexing and Bloom filters into an efficient data retrieval algorithm that allows healthcare providers and researchers to quickly access specific patient records and medical data within the blockchain.

Algorithm 4.1: Data_Retrieval

Input: root_hash, target key
Outcome: Data associated with the target key (if present)
Step 1: Initialize an empty Bloom filter (Bloom filter)
Step 2: Load the Merkle Patricia Tree (MPT) with the given root_hash
Step 3: Traverse the MPT to populate the Bloom filter with keys
Step 4: Check if the target key exists in the Bloom filter using Bloom_Lookup
Step 4.1: If Bloom_Lookup returns True, perform MPT_Retrieve(root_hash,target key) to retrieve the data associated with the target key.
Step 4.2: If Bloom_Lookup returns False, the data associated with the target key is not present in the blockchain.

As outlined in algorithm 4.1, the Data_Retrieval algorithm is designed to efficiently check for the presence of a target key in a blockchain's Merkle Patricia Tree (MPT). The process begins by initializing an empty Bloom filter in Step 1. In Step 2, the algorithm loads the MPT using the provided root_hash. Step 3 involves traversing the MPT to fill the Bloom filter with available keys. Then, in Step 4, the algorithm checks for the existence of the target key through the Bloom_Lookup. Depending on the result, it either retrieves the associated data using MPT_Retrieve or indicates that the key is not present.

By combining the MPT indexing and Bloom filters, the data retrieval algorithm significantly reduces the time and resources required to fetch specific healthcare data from the blockchain. The unique properties of the MPT ensure data integrity,

while bloom filters provide a space-efficient approach for rapid key lookup, making the proposed algorithm highly unique and efficient for data retrieval in the blockchain based smart healthcare system.

4.3 RESULTS AND DISCUSSION

To evaluate our proposed decentralized storage and retrieval algorithms, we used synthetic healthcare records designed to emulate a real-world healthcare database. This ensured that patient privacy remained uncompromised. The records were encrypted before being distributed across the network nodes. Our tests were facilitated by libraries and tools optimized for structured data generation. As a result, our synthetic dataset incorporated crucial aspects of healthcare records, such as patient ID, medications, medical history, lab results, and more. The following subsections detail the findings and their implications.

Tables 4.1 and 4.2 showcase the results of evaluating "Merkle-Patricia Trie (MPT) EHR Retrieval", "B+ tree EHR Retrieval," and "Traditional Block Retrieval" mechanisms in a smart healthcare blockchain system. Table 4.1 corresponds to a block size of 1200, while Table 4.2 relates to a block size of 2400. The evaluation assessed data upload and download times for varying user counts (5, 10, 15, 20, 25 and 30) in seconds.

Table 4.1 Upload and Download time (s) for block size 1200

No. of Users	Proposed MPT EHR retrieval		B+ tree EHR retrieval		Traditional block retrieval	
	Upload time	Download time	Upload time	Download time	Upload time	Download time
5	15	14	18	17	26	25
10	18	16	22	21	31	30
15	20	19	25	26	39	40
20	22	20	28	28	45	42
25	25	23	31	30	51	50
30	30	27	35	39	55	55

Table 4.2 Upload and download time (s) for block size 2400

No. of Users	Proposed MPT EHR retrieval		B+ tree EHR retrieval		Traditional block retrieval	
	Upload time	Download time	Upload time	Download time	Upload time	Download time
5	28	27	37	34	50	47
10	35	33	45	43	58	57
15	41	40	52	50	68	70
20	45	44	57	56	83	86
25	49	48	65	63	91	94
30	58	56	71	69	102	105

The data upload times demonstrate the efficacy of various data retrieval mechanisms in a blockchain-based smart healthcare system. Table 4.1 (block size 1200) and Table 4.2 (block size 2400) provide insight into the time required to upload healthcare data for user counts ranging from 5 to 30. The data upload times demonstrate that the "Proposed MPT EHR Retrieval" consistently demonstrates the quickest upload times across all user scenarios. These results demonstrate the efficacy of the "Proposed MPT EHR Retrieval" mechanism, which consistently outperforms other methods, emphasizing its capacity to upload healthcare data quickly.

Both the "Proposed MPT EHR Retrieval" and the "B+ tree EHR Retrieval" methods perform similarly in terms of data download times, with MPT slightly outperforming B+ tree. Both strategies make use of efficient indexing and caching methods, which speed up the retrieval of information. However, the proposed approaches' enhanced indexing and caching features make "Traditional Block Retrieval" slower to download.

- **Comparative Analysis**

In the following, we compare the performance metrics of our proposed sHealthCare blockchain with those of a traditional blockchain (without MPT & Bloom). To determine how well the proposed approach works in the context of smart healthcare applications, we conducted a comprehensive evaluation. The findings shed light on the expanded potential of the proposed blockchain architecture.

Table 4.3 Evaluation of proposed blockchain for EHR

Metric	Proposed sHealthCareBlockchain	Traditional Blockchain (without MPT & Bloom)
Throughput (transactions / Second)	185	168
Latency (ms)	584	653
Delay (ms)	115	138
Response Time (ms)	200	242

Values from Table 4.3 provide valuable insights into the enhanced capabilities of our proposed blockchain framework. Notably, our sHealthCareBlockchain outperforms the traditional blockchain in several aspects. It achieves a significantly higher throughput of 185 transactions per second, demonstrating its efficiency in handling a substantial transaction load. Furthermore, our blockchain exhibits lower latency and delay, with 584 ms and 115 ms, respectively, indicating prompt transaction processing and improved data-sharing efficiency. The proposed sHealthCareBlockchain exhibits a superior response time of 200 ms, thereby ensuring efficient and responsive data sharing in comparison to the conventional blockchain. The obtained results validate the efficacy of our novel data sharing and retrieval mechanisms, establishing our blockchain technology as a promising solution for the optimisation and security of smart healthcare applications.

4.4 SUMMARY

In this chapter, the 'sHealthCareBlockchain' framework is designed for efficient data management in the blockchain infrastructure. The proposed data sharing scheme leverages dynamic sharding algorithms, adaptive dynamic sharding, and parallel transaction validation for improved efficiency, scalability, and load balancing. Privacy preservation is a pivotal focus, ensuring secure access only to authorized entities.

In the realm of data retrieval, the study introduces a novel technique combining Merkle-Patricia Trie (MPT) indexing and Bloom filters. This method significantly reduces data retrieval time by efficiently organizing and quickly accessing specific healthcare data within the blockchain. The results of synthetic healthcare records evaluation demonstrate the superior performance of the proposed MPT-based EHR retrieval mechanism over traditional methods. Comparative analysis with a traditional blockchain highlights the efficiency of the proposed sHealthCareBlockchain. It exhibits superior throughput, lower latency, delay, and response time, validating the effectiveness of the innovative data-sharing and retrieval mechanisms. The study concludes that the proposed framework has the potential to optimize and secure smart healthcare applications, addressing current challenges in data management and retrieval.

CHAPTER 5

AN EFFICIENT DATA SHARING SCHEME USING MULTI-TRANSACTION MODE CONSORTIUM BLOCKCHAIN FOR SMART HEALTHCARE

To address the security and transparency issues associated with EHRs, new standards must be developed. Blockchain technology has shown to be an exciting option for enhancing EHR security within the context of smart healthcare systems. However, issues in privacy and scalability remain, particularly in the context of managing off-chain transactions. To address these issues, this work proposes a solution that uses a Multi-Transaction Mode Consortium Blockchain (MTMCB) running on Redis to improve EHR retrieval speed by implementing an Adaptive Balanced Merkle (AB-M) tree. This innovative approach combines binary tree efficiency with Merkle tree robustness. In addition, to ensure the secure storage and retrieval of patient EHRs, it uses a lattice-based ring signature technique. The method produces superior outcomes, demonstrating a significant improvement in both upload and download times when compared to existing methodologies, which provides a potential solution to the widespread difficulties with EHR access and security.

5.1 INTRODUCTION

In today's ever-changing healthcare context, the need for secure, efficient, and transparent data sharing has never been greater. The development of EHRs has transformed the way patient information is stored and accessed, potentially improving patient care and healthcare system efficiency. However, these developments present new challenges, particularly in terms of data security, privacy, and scalability [90]. The present section explores an innovative approach to addressing these issues, focusing on the design and implementation of an MTMCB specifically designed for smart healthcare systems. The healthcare sector has long struggled with the difficult balance between data accessibility and security [91]. Medical data, which is frequently regarded as one of the most sensitive types of information, must be easily accessible to authorised healthcare workers while

being resistant to unauthorised access or modification [92]. EHRs have become an essential component of modern healthcare, centralising patient data and allowing physicians to provide more personalised and prompt care. However, due to the vulnerability of centralised EHR systems to hacking attempts and the inherent privacy problems they create, the way things are now has been re-evaluated.

Blockchain technology, popularised originally by cryptocurrencies, has emerged as a possible revolution in the healthcare industry. Its inherent characteristics, such as decentralisation, immutability, and transparency, are perfectly aligned with the fundamental goals of EHR management [93]. This section investigates the use of a consortium blockchain, a private, authorised blockchain managed by a group of trusted organisations, in this context. This multi-transaction consortium blockchain has the potential to overcome the constraints of typical single-transaction blockchain. The usage of Redis as the underlying architecture for our MTMCB, an open-source in-memory data store, has various benefits, including high performance and fault tolerance. The robust basis of the information transfer method is Redis, which is well-known for its storage and retrieval of data capabilities. It can develop a flexible and effective data management system by utilising Redis, which is critical in the rapidly changing field of healthcare.

The development of an AB-M tree for EHR retrieval is one of the key advancements discussed in this section [94]. The AB-M tree is a unique work of binary tree efficiency with Merkle tree cryptographic robustness. This structure improves EHR retrieval performance, which is crucial in the dynamic world of healthcare, where rapid access to patient data can be the difference between life and death [95]. Furthermore, to maintain the security and privacy of patient data, this approach includes a lattice-based ring identification mechanism for EHR storage and retrieval. The use of ring authorization, a cryptographic technique, provides for the anonymous authentication of a message sender's authenticity within a group [96, 97]. This guarantees that EHRs are kept and retrieved securely, protecting patients' sensitive information while allowing authorised healthcare professionals

access to the data they require. It will offer actual evidence throughout the portion demonstrating the significant improvements in upload and download times achieved as compared to traditional EHR data sharing strategies. The outcomes of our novel technique provide a potential address to the long-standing problems associated with EHR access and security in smart healthcare systems [98, 99]. Hence, this research aims to investigate and construct an innovative data sharing system based on a multi-transaction mode consortium blockchain augmented by Redis and the Adaptive Balanced Merkle tree. This not only tackles the security and scalability issues inherent in EHR management, but it also lays the way for a more efficient and secure future for smart healthcare systems. The concepts and technologies addressed here have the potential to transform how healthcare data is managed and shared, thereby improving the quality of treatment provided to patients while protecting their sensitive information.

5.2 CONTRIBUTION

The contributions of the research are as follows,

- This research suggested a blockchain-based healthcare model that improves EHR retrieval efficiency by using an AB-M tree, an optimised Redis cache, and a lattice-based ring signature technique.
- The developed model has been evaluated on testing across different node and user counts, calculating block upload and download times as performance metrics.
- It evaluated the lattice-based ring signature schemes within the proposed system in terms of encryption and decryption times, comparing them to contemporary cryptographic techniques.

5.3 PROPOSED METHODOLOGY

In this research, an EHR retrieval method was suggested that utilizes the ABM Tree and Redis Cache, enabling efficient and secure data sharing in smart healthcare systems, as illustrated in Figure 4.1. Furthermore, it included the Lattice-Based

Ring Signature technique, which improves sender privacy by making transaction signers computationally difficult to determine. It suggests using an MTMCB for creating a robust smart healthcare system, with Redis Cache playing a critical role in block building.

To increase retrieval while minimising data processing, an effective in-memory indexing system for each block file saved on the disc is required, optimising the amount of disc reads and writes. Redis technology, which includes features like key lifespan and subscription interest, appears as a viable tool for this purpose. Redis saves infrequently updated data in memory, decreasing dataset searches, improving response times, and increasing throughput. Furthermore, Redis supports packed records as a data format, allowing for more efficient data storage and encoding inside a single memory region. The flow of this technique is illustrated in Figure 5.1, which depicts the health record retrieval process.

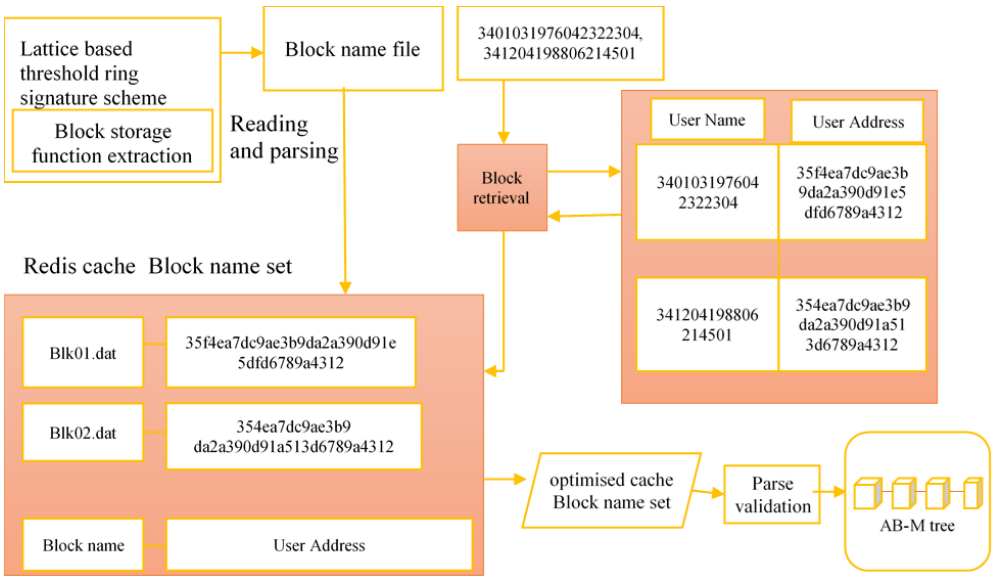

Figure 5.1 Health record retrieval technique

To optimise both data verification speed and retrieval efficiency, it used the AB-M tree to reorganise the client and block name capacity within the Redis store. This AB-M tree combines the benefits of Merkle trees, which are well-known for their rapid data validation, with the speed of binary trees in data retrieval. The Merkle

tree's capacity to validate data quickly is leveraged by the binary tree's short look-up time, resulting in the AB-M tree's combined benefits. Furthermore, user privacy is protected by an effective ring signing system that allows a 'ring' of signers to securely sign communications. This novel approach assures that message signatures can be validated without the verifier knowing which ring member applied the signature. Furthermore, signatures from two separate signers remain unlinkable, allowing individuals to securely share their healthcare records while maintaining their privacy. When numerous sites are active at the same time, this system systematically checks all block files. It finds the matching crossover blocks between the two sites in the user brick file. Following that, within the user file, a number of parallel destinations are located, allowing all respective users to participate together. The below recommended retrieval approach is comprised of a set of well-defined procedures that ensure a fast and secure process for accessing healthcare records while protecting user privacy.

5.3.1 MULTI-TRANSACTION MODE CONSORTIUM BLOCKCHAIN (MTMCB) ARCHITECTURE

The Multi-Transaction Mode Consortium Blockchain (MTMCB) technology incorporates critical components of modern blockchain technology, including distributed storage, decentralisation, point-to-point connection, and robust encryption. This innovation defines the traditional concept of electronic cash transactions, transforming it into a more comprehensive term that encompasses the entire process and resolution of event handling. It improves the functionality of both the transaction verification system and the block distribution mechanism. The architectural representation of MTMCB, as shown in Figure 5.2, demonstrates the presence of two critical components: the Transaction Node and the Regulatory Node System (RNS).

Within this architecture, the RNS is in charge of server initialization, transaction processing, and auditing. Transaction nodes, which are represented by devices such as PCs, smartphones, and ATMs, serve as system access gateways. The User File

is initiated by several user types following authorization, including patients, doctors, hospital administrators, and insurance agents, each with distinct roles within the smart healthcare system. The Regulatory Node takes authority of the MTMCB's User File, which contains user names and 10-character business deal addresses. Users' privacy is protected by using their unique addresses for retrieval and future transaction data. Figure 5.3 depicts the complicated structure of the MTMCB and the integration of transaction nodes with the regulatory node system.

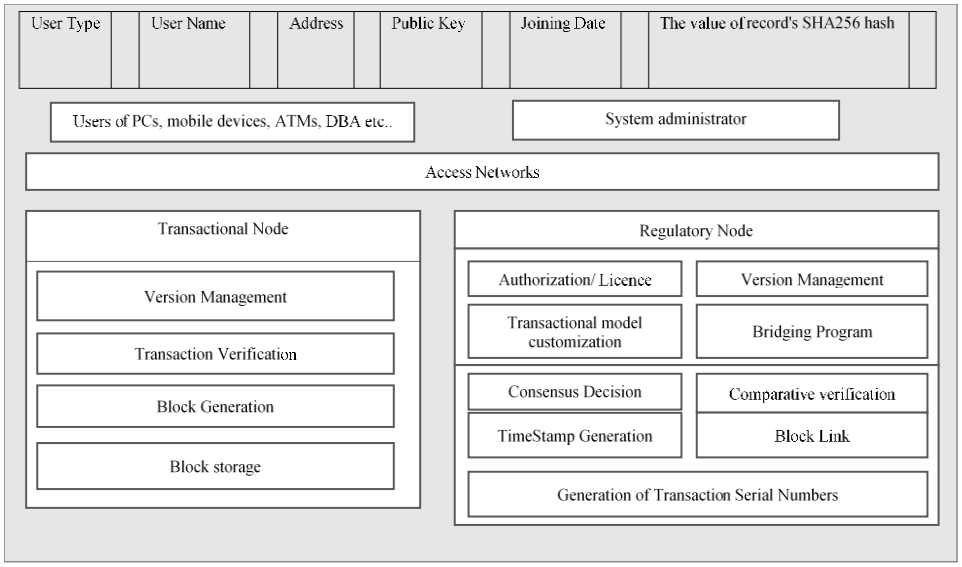

Figure 5.2 Architecture of MTMCB

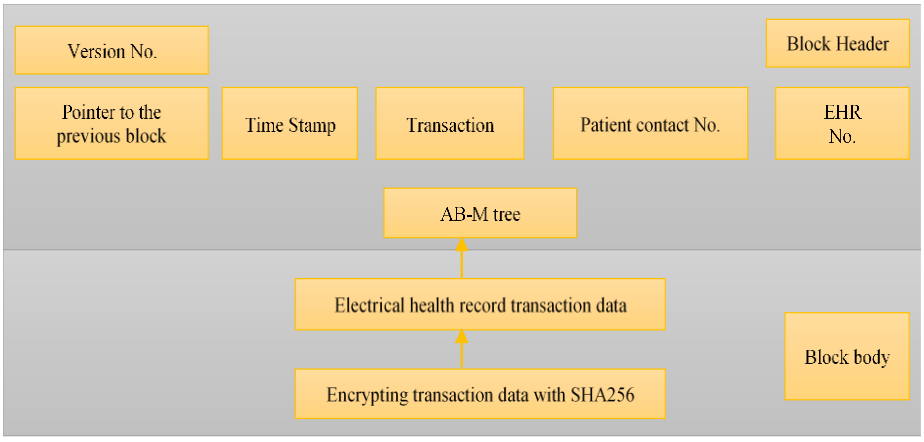

Figure 5.3 Block diagram of the constructed MTMCB

Figure 5.3 depicts the block's body and header. The hash values are critical in determining the hash of the preceding block, which serves as the block header and is the initial block on the blockchain. Except for the genesis block, each successive block maintains the hash value of its previous one. Two crucial components are retained within the network head file, a system file: a Word document representing the network head frame's database equivalent and the hash value of the block. These interconnected blocks comprise the blockchain, allowing for the preservation and update of the chain's tail block contents. Using the hash value of the preceding block, a sequential progression from the 'tail' to the 'head' inside the blockchain's hierarchical structure can be made, maintaining the integrity and continuity of the blockchain data records.

5.3.2 OPTIMISED REDIS CACHE TECHNOLOGY

This work utilizes Optimized Redis Cache, an open-source caching service that allows query, insertion, updating, and removal of key/value pairs as illustrated in the Equation (5.1-5.4).

$$B(T_i) = B.B_i.Query(T_1, T_2, \dots, T_n) \tag{5.1}$$

$$B(T_i) = B.B_i.Insert(T_{i+1}) \tag{5.2}$$

$$B(T_{i+1})_n = B.B_i^{"}.Update(T_{i+1}) \tag{5.3}$$

$$B^{"}(T_{i+1}) = B.Delete(T_{i+1}) \tag{5.4}$$

In the context of this discussion, $B(T_i)$ represents the transaction database, where B represents the database and B_i represents the collections. The operations Query, Insert, Update, and Delete represent the equivalent NoSQL functions, and $B\ (T_{i+1})$ represents the updated database once the transactions are processed.

When dealing with transaction data, especially searching, the usage of Redis cache technology could create issues, especially when dealing with large amounts of data.

To address this, a novel method is proposed that is inspired by the feeding and migratory behaviour of flamingo birds and is included in the Redis storage architecture. The Flamingo Search algorithm is designed to optimise the arrangement within the search zone. However, the method encounters unpredictability in the maximum search distance due to random modifications, resulting in a significant failure rate in identifying key characteristics.

Equation (5.5) describes analogous to how a flamingo's nose is calculated during hunting operations, emphasising the necessity to adjust and fine-tune the algorithm to improve its efficacy in recognising significant characteristics within the data.

$$\left|\eta_1 \times \lambda T_{bj} + \varepsilon_2 \times T_{ij}\right| \tag{5.5}$$

Xavier initialization includes assessing a random number that is determined by the Euclidean distance and aligns with a multivariate normal distribution. A typical assumption is applied once to simulate flamingo screening behaviour during bill examination, taking into consideration the range of flamingo snout positioning is calculated as Equation (5.6):

$$\eta_2 \times \left|\eta_1 \times \lambda T_{bj} + \varepsilon_2 \times T_{ij}\right| \tag{5.6}$$

It is frequently used to improve the feeding range of flamingos and investigate variations in individuals' selection behaviours. In summary, as mentioned in equation (5.7), the detection range of a flamingo's beak adds to the stride length of the flamingo's foraging movement, which normally occurs during the twelfth cycle.

$$b_{ij}^{t} = \varepsilon_1 \times \lambda T_{bj}^{t} + \eta_2 \times \left|\eta_1 \times \lambda T_{bj}^{t} + \varepsilon_2 \times T_{ij}^{t}\right| \tag{5.7}$$

Enhanced by Xavier initialization, provided by the following Equation (5.8):

$$V(\varepsilon_1, \varepsilon_2) = U\left[-\frac{1}{\sqrt{T_n}}, \frac{1}{\sqrt{T_n}}\right] \tag{5.8}$$

The following Equation (5.9) refers to the location of flamingo foraging behaviour.

$$T_{ij}^{T+1} = \left(T_{ij}^{t} + \varepsilon_1 \times \lambda T_{jb}^{t} + \eta_2 \times \left|\eta_1 \times \lambda T_{jb}^{t} + \varepsilon_2 \times T_{jb}^{t}\right)/k \right. \quad (5.9)$$

In equation (5.9), T_{ij}^{t+1} shows the area jth estimation of the general cycle, and Γ_{ij}^{t} demonstrates the area course of the flamingo people, separately.

In the context of the t cycle, λT_{bj} refers to the parameter addressing the jth characteristic within the population. The variable K, denoted as $k(n)$, represents a random variable characterized by an irregular number with n degrees of choice, following a chi-square distribution. This extension of the range and the incorporation of inherent uncertainty contribute to enhancing its overall validity through the exploration of functions. Additionally, $\eta_1 = n(0,1)$ and $\eta_2 = n(0,1)$ represent two random values drawn from a standard normal distribution, while ε1 and ε2 are manipulated by either -1 or 1.

$$T_{ij}^{T+1} = T_{ij}^{t} + \Im \times \left(\lambda T_{jb}^{t} - T_{ij}^{t}\right) \quad (5.10)$$

In Equation (5.10), T_{ij}^{t+1} denotes the coordinates of the ith dimension and jth dimension, primarily signifying the position of the flamingo's feet within the population. During a specific migration process, the flamingo with the highest fitness in the t iteration is located at λT_{jb}^{t} in the jth dimension. This intricate movement pattern contributes to an exceptionally efficient search strategy for queuing transaction data. Additionally, algorithm 5.1 illustrate the optimized Redis cache technology. The proposed Optimised Redis Cache Technology algorithm utilizes a flamingo population for efficient data retrieval. The algorithm begins by initializing the flamingo population in Step 1. It then iterates through each member of the population to evaluate fitness in Step 2, where fitness is calculated based on specified parameters. Depending on the count of flamingos, the algorithm updates their positions using either a standard or alternative formula. In Step 2.1.3, the positions of the flamingos are determined, and if a satisfactory search outcome is achieved, the optimal solution is returned. If not, the algorithm reverts to the fitness evaluation process.

Algorithm 5.1. Proposed Optimised Redis Cache Technology

Input: $B(T_i) = B.B_i.Query(T_1, T_2, \ldots\ldots T_n)$

Output: Data retrieval

Begin

Step 1: Initialize the flamingo population T_{ij}

Step 2: For i=1 to n

Step 2.1 **For** j=1 to m

Step 2.1.1 **Evaluate** the fitness of the population

$$b_{ij}^{t} = \varepsilon_1 \times \lambda T_{jb}^{t} + \eta_2 \times \left|\eta_1 \times \lambda T_{bj}^{t} + \varepsilon_2 \times T_{ij}^{t}\right|$$

Step 2.1.2 **If** countT_{ij} >1

Update the flamingo position using,

$$T_{ij}^{t+1} = \left(T_{ij}^{t} + \varepsilon_1 \times \lambda T_{jb}^{t} + \eta_2 \times \left|\eta_1 \times \lambda T_{bj}^{t} + \varepsilon_2 \times T_{ij}^{t}\right|\right)/k$$

Else

Update the flamingo position using,

$$T_{ij}^{t+1} = T_{ij}^{t} + \Im \times \left(\lambda T_{jb}^{t} - T_{ij}^{t}\right)$$

End if

Step 2.1.3 **Determine** the position of each flamingo

$$\left|\eta_1 \times \lambda T_{bj} + \varepsilon_2 \times T_{ij}\right|$$

$$\eta_2 \times \left|\eta_1 \times \lambda T_{bj} + \varepsilon_2 \times T_{ij}\right|$$

Step 2.1.4 **If** search is obtained

Return the optimal search solution

Else

Return to fitness evaluation

End if

End for

End for

End begin

Redis caching technology is critical for improving the performance and efficiency of data storage and retrieval procedures. As recorded values in this system, any.NET object serializable to JSON can be used, assuring flexibility and compatibility.

When data is received from the cache, it is deserialized from JSON to the proper data format, making it easier to access and use. A memory index is created using Redis cache technology to accelerate the retrieval of disk-stored block files. Redis is a high-performance database, ideal for high-concurrency relational databases. Its in-memory operations improve read and write performance significantly. Redis supports a wide range of data structures, such as connected records, strings, sets, and sorted sets ($Zset$). It conducts atomic operations and includes features like unions, intersections, complements, and sorting, making it a versatile and powerful data management tool. One of Redis's significant characteristics is its broad set of application programming interfaces (APIs), which support a variety of programming languages such as Java, Python, PHP, Ruby, and others. Redis also has features like publish/subscribe, notifications, and key expiration. Redis, as a business cache, helps to reduce database load, improve response times, and increase throughput by maintaining often accessed but infrequently updated data in memory. Additionally, Redis supports the storing of compressed lists, which helps in memory conservation and ensures efficient data encoding and storage, particularly in fields with recognised time limitations and difficult reading conditions. Because of Redis's varying role, it is an essential component for efficient and high-performance data management [100].

The Redis caching system is an essential component of the smart healthcare infrastructure, operating independently of the primary application framework. Its key function is to make expanding the smart healthcare system across several instances easier while keeping data consistency. This method is especially useful when network load balancers route users to different smart healthcare system instances, ensuring that cached data is consistent across all instances. Data access

is significantly accelerated when the Redis cache is strategically located within the same data centre as the blockchain services since the cache maintains data in memory, reducing the need for time-consuming disc reads. Through its basic, standard, and premium tiers, the Redis cache solution provides versatility. Basic tiers are less expensive but lack Service Level Agreements (SLAs) and replication failover features, which means that using basic instances in a production environment risks data loss if the hosting Virtual Machine (VM) is reused. The standard and premium tiers are suggested for production tasks because it provide the required reliability and functionality for robust and high-performance operations.

The base tier of Redis cache offers a robust service with a 99.9% Service Level Agreement (SLA) for availability. It has redundancy and automated failover features in case the primary node fails. The premium tier, on the other hand, inherits all of the capabilities of the standard tier, such as the ability to scale via a Redis cluster, disaster recovery cache snapshots, and enhanced throughput. Patients generate an increasing volume of EHR daily in the changing environment of smart healthcare systems. The explosion in data contributes to an exponential increase in computational complexity. Redis Cache is critical in the development of smart healthcare applications because it preserves session information for many web front ends and efficiently caches permanent data. Consider an instance in which a programme routinely requests costly data from persistent storage, such as an access control list. This information can be saved in the Redis cache to speed up web application access. It is critical to carefully evaluate the cache's data retention period, especially when using a lazy loading strategy to construct it. If any changes to the cached data occur inside the application, it is critical to ensure that redundant data is either updated or removed from the cache, ensuring data consistency and accuracy in the dynamic smart healthcare environment.

5.3.3 TRADITIONAL MERKLE TREE STRUCTURE

The traditional Merkle tree is a binary tree structure employed to store multiple hash values. In Figure 5.4, a five-layer Merkle tree is illustrated, comprising a root node $K_{4,1}$, a set of middle nodes $K_{3,m}$ for $m = 1, 2,3,4$ and an array of leaf nodes (1, 2, ..., 8) at the base.

The following can be used to demonstrate the $K_{4,1}$ root node computation process:

Initially, consider $S_i$as the *i*-th input data $Data_i$, , where i = 1, 2,….8, k (.), and k(.) represents a hash function. The leaf nodes denoted as k_i, are generated by hashing the input data S_i using K(.), and their values can be determined through the following Equation (5.11).

$$K_i = K(S_i), i = 1, \dots 8 \tag{5.11}$$

Second, leaf nodes Ki denote the next layer and processing elements may be calculated as shown in equations (5.12), (5.13) and (5.14) as:

$$K_{2,i} = K(K_{2i-1}, K_{2i}), i = 1, \dots 4 \tag{5.12}$$

Finally,

$$K_{3,m} = K\left(K_{2,2m-1}, K_{2,2m}\right), m = 1,2 \tag{5.13}$$

Ultimately, the results of the root node can be described from

$$K_{4,1} = K\left(K_{3,1}, K_{3,2}\right) \tag{5.14}$$

Ultimately, the result of the root node can be derived from the following analysis as illustrated in Figure 5.4.

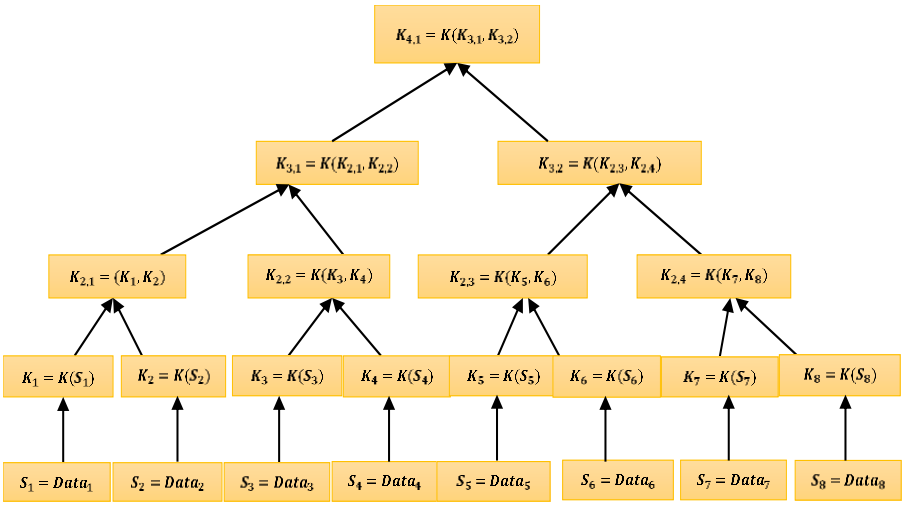

Figure 5.4 Merkle tree structure

The cryptographic hash of a certain dataset is typically kept in the leaf nodes of a Merkle tree. The intermediary nodes, on the other hand, maintain hash values derived from the data of their lowest three interconnected child nodes. Furthermore, the root node stores the highest-level hash function, which integrates data from the previous two layers. The interconnected structure of the nodes ensures that each change in the value of a leaf node causes corresponding changes in its parent nodes, resulting in a cascading impact of changes. For example, if the 'Data' represented by S_4 in Figure 5.4 changes, major changes will occur in the root node, $K_{4,1}$ as well as the intermediary nodes, propagating throughout the tree.

5.3.4 ADAPTIVE BALANCED MERKLE TREE (AB-M TREE)

An Adaptive Balanced Merkle (AB-M) tree balances efficiency in terms of quick data retrieval from a binary tree with quick data verification from a Merkle tree [101]. This section introduces AB-M trees and describes how to set a query demand threshold for an optimised smart healthcare blockchain system. Layers are determined in the adaptive AB-M tree construction process using threshold-based calculations. To simplify data organisation and retrieval, it employs a two-tier data structure with a hybrid top level and a Merkle tree at the bottom level.

Each upper node in the AB-M tree structure plays an important function in preserving important information. It saves the maximum (Max) and minimum (Min) exchange initiator promotion addresses for the leaf nodes with which it is linked. It also keeps the exchange initiator's address (K) and the left and right pointers (L1 and R1), which point to the appropriate leaf node. The AB-M tree, unlike the Merkle tree, keeps the maximum and minimum values within its nodes. This distinguishing characteristic eliminates the need to traverse every block during a query demand, greatly increasing the efficiency of collecting the essential information. By directly accessing nodes, the system already has the necessary results. The logical binary tree structure of the AB-M tree permits rapid data location without the need to traverse the full block, thereby speeding the retrieval process.

When constructing AB-M trees, the thresholding mechanism encapsulates the smart healthcare blockchain system's query requirements. Thresholding is determined as follows: The initial value for the period can be utilized according to requirements. N_t represents the total transaction count in the last fixed period, and N_q is the previous period's thresholding value, denoted as T_p , which is utilized to compute the current period's thresholding *T* and is shown as equation (5.15).

$$T = min\left\{\left[T_p + \omega\left[\frac{N_q}{N_t - 1}\right]\right], 1\right\} \tag{5.15}$$

where ω implies query thresholding coefficient that could be changed, *T* Signifies minimum of [$T_P + \omega\left(\frac{N_q}{N_t} - 1\right)$] and 1. If T = 1, it implies that inquiry demand is high. Thresholding is determined by evaluating data from the previous block, considering in the knowledge that current and future applications may differ. Because blockchain data is append-only, it is not possible to change query criteria for confirmed blocks. New blocks can only be evaluated using 5.2 or the evaluation parameters expanded. Equation (5.16) describes a method for calculating the total amount of leaf node levels in H_i, helping in a flexible data structure.

$$H_i = H(1 - T) \tag{5.16}$$

where H is the total number of layers in the balanced tree. When T = 1 and $H_i = 0$, all nodes continue to function. Algorithm 5.2 produces AB-M trees.

Algorithm 5.2: Algorithm to Generate AB-M tree

Input: Data transaction array, Thresholding T.

Output: An AB-M tree

Step 1: Verify transaction data within a timeframe;

Step 2: Create a balanced binary tree based on every transaction initiator's address (the first layer contains L neaf nodes);

Step 3: Compute a thresholding T and layer count H_i from (5.15) and (5.16)

Step 4: Generate Merkel trees beneath $(H_i + 1)^{th}$ layer nodes

Step 5: for

Step 5.1: Merge every $(H_i + 1)^{th}$ layer nodes' hash value with their left leaf node;

Step 5.2: Combine the result with the right leaf nodes' hash

Step 5.3: Record the Maximum, Minimum and i value of every $(H_i + 1)^{th}$ node {where L_1 indicates left leaf node, R_1 right leaf node}

Step 5.4: $H_i = H_i + 1$

Step 6: end for

Step 7: The combined result is stored in block head as an AB-M tree.

In Algorithm 5.2, the process starts with verifying transaction data within a specified timeframe in Step 1. A balanced binary tree is then created based on the transaction initiators' addresses in Step 2, resulting in L leaf nodes at the first layer. In Step 3, the threshold T and layer count H_i are computed using provided equations. Step 4 involves generating Merkle trees beneath the $(H_i + 1)^{th}$ layer nodes. The algorithm then iterates through these nodes, merging hash values with their corresponding leaf nodes and recording key metrics such as maximum and

minimum values in Step 5. Finally, the combined result is stored in the block header as an AB-M tree in Step 7.

5.3.5 TRESHOLDING RING SIGNATURE SCHEME

The suggested thresholding ring signatures are based on the concept that a threshold of t users within a group of N users can collectively sign a message on behalf of the entire group. Additionally, the recipient can confirm the authenticity of the signature without having to identify the exact signers. This approach is known as an $A\ (t, N)$, t$<$ N thresholding ring signature system, consists of three essential algorithms: Verify, Sign, and KeyGen, which allow for secure and efficient message authentication.

KeyGen: produces N pairs of private and public keys for N users using a probability algorithm (x_i, A_i) … … $\left(x_{N,} A_N\right)$ $with\ i \in 0, \ldots N-1$.

Sign: A set of N public keys and t private keys $(A_i, \ldots . A_N)$, $(x_{i1}, \ldots . x_{it})$, with $\{i_i, \ldots . i_i\}$ $\{1 \ldots . N\}$ and m is a message, are inputs for the probabilistic interactive protocol sign, where 'm' represents the message, it generates a (t, N) - minimum signature required for that message.

Verify: Determine if the algorithm is predictable with message inputs , a signature, and an N public key pair $(A_i, \ldots . A_N)$ It produces a result of 1 if σ the signature form is a fair (t, N), thresholding signature concerning the public keys $(A_i, \ldots . A_N)$ and a result of 0 if it is not.

The first step of developing a (t, N) -message thresholding signature is to choose a leader from among the *t* participants. This leader is in charge of interacting with the verifier and the remaining $t-1$ users to establish a (t, N) -thresholding signature. The security criteria for (t, N) -thresholding ring signature system include qualities such as accuracy, tamper resistance, and reference. $A\ (t, N)$ −thresholding signature scheme is considered acceptable if the verifying party acknowledges any combination of message and signature (m, σ) obtained using suitably formed public-private key pairs and the Sign algorithm with a probability of 1. The

unforgeability property claims that it is impossible to generate a legitimate (t, N)-thresholding signature without knowledge of at least *t* private keys. Furthermore, the source-hiding attribute assures that identifying t-subsets of signers who contributed to the creation of a given (t, N)thresholding signature and message (m, σ) remains difficult.

5.3.6 LATTICE-BASED THRESHOLDING RING SIGNATURE SCHEME

This approach is used to create a storage protocol for maintaining EHR securely within a smart healthcare ecosystem. To protect user privacy, it is intended for incorporation into the predicted smart healthcare consortium blockchain environment [102]. The system consists of four basic algorithms: setup, key creation, signature, and verification.

The setup procedure, as described below, derives $n, m, and\ q$ parameters from the security parameter k, allowing the formation of lattices and associated operations necessary for data security and privacy.

"For $i = 1, \ldots . n$ if a user i has N pairs of public and private keys(x_i, A_i), with $i \in 0, \ldots . N - 1$. All private keys are binary vectors with Hamming weight $m/2 +$ 1m/2 + 1 and solve $A_i x_i = 0\, mod\, q\, .\, i \in Z_q^{(n\times(m+1))}$ are public keys.

Modifying fundamental RSA is a difficult issue. Allow $L_m: \{0,1\}^* \rightarrow KN_i$ to work. Let L be the arrangement of all open keys of the Nclients. Let χ be two times the piece biggest q_i andN_i, for$1 \leq i \leq N$.

Over-simplification, assume client Θ, for$1 \leq \Theta \leq t$, are partaking endorsers and the client j, for $1 \leq j \leq n$, are non-taking part underwriters. To produce an $\{t, n\}$ edge ring mark t partaking underwriters complete the accompanying advances."

The signing algorithm

1. The process of lattice key pair is shown in equation 5.17,

$$Z_i = G_i^{Si} Y_i^{Ci} \text{mod} \chi_i\ if\ user\ i\ has\ a\ lattice\ based\ key\ pair \qquad (5.17)$$

2. Using equation 5.18 the process to randomly select values for each participating user j, for j=1…t…pick $\Re_j \epsilon_R Z_R$, is computed as:

$$Z_i = G_i^{Si} \text{mod} \chi_i \; if \; user \; j \; has \; a \; lattice \; based \; key \; pair \quad (5.18)$$

3. Equation 5.19 is used to compute the degree or complexity $D(E)$ of the function initial value of the function $E(0)$ and to assign the challenge values $E(i)$ as

$$D(E) = N - t, E(0) = C_0 \; and \; E(i) = C_i, for \; t + 1 \leq i \leq N \quad (5.19)$$

4. For i=1,…..n, figure $C_i = E(i)$, as shown in equation 5.20:

$$Z_i' = G_i^{Si} Y_i^{Ci} \text{mod} \chi_i \; if \; user \; i \; has \; a \; lattice \; based \; key \; pair \quad (5.20)$$

5. The mark yield for M and L as $\sigma = (S_1, \ldots . S_{N,} E)$

Algorithm for verification:

A verifier can validate a signature $\sigma = (S_1, \ldots . S_{N,} E)$ as follows:

1. Check if $deg\ (E)$ = N-t. If so, go ahead. If not, dismiss.

2. For i= 1,…n, compute challenge values $C_i = E(i)$ for all users (equation 5.21) as:

$$Z_i' = G_i^{Si} Y_i^{Ci} \text{mod} \chi_i \; if \; user \; i \; has \; a \; lattice \; based \; key \; pair \quad (5.21)$$

3. Check whether $E(0)$ = g (L, t, M, Z,…Z_n). Accept if yes

Reject in all other scenarios; this extensive arrangement simplifies concurrent integration for enhanced efficiency and effectiveness.

5.3.7 BLOCK RETRIEVAL ALGORITHM

To ensure the integrity of the blockchain, each newly connected block includes the hash value of its predecessor, producing a chain of interconnected blocks. However,

due to the unidirectional nature of the blockchain, direct access to previous blocks is often limited to the most recent block. Prior blocks are frequently retrieved by exploring a series of linked hash values from the end-of-chain block and going backwards. The number of blocks on the blockchain increases over time, potentially making sequential retrieval methods less effective and presenting a barrier to long-term system efficiency.

To address this issue, the MTMCB Regulatory Node System uses the MTMCB network's partially centralised structure to produce block names, optimising efficiency and limiting any performance degradation. A Redis cache indexes user files and blocks within this architecture, allowing for rapid searches for block names and content locations. The block retrieval process is divided into four independent stages, resulting in a more streamlined and effective method of retrieving blockchain data.

Algorithm 5.3: Block Retrieval Algorithm

Input: User transaction ID

Output: User-related block file

Step 1: Utilizing a user set, the retrieval technique identifies the user's transaction ID.

Step 2: By employing the AB-M tree, we can extract the user address key from the user block set, enabling the precise identification of all user block file name records.

Step 3: If not, all suitable block file names are located, repeat Step 2.

Step 4: Steps 2 and 3 generate a user-related block file as the query’s target file.

Algorithm 5.3 outlines the process for retrieving user-related block files within a blockchain framework. The algorithm begins with Step 1, where it utilizes a user set to identify the user's transaction ID through a retrieval technique. This step is crucial as it establishes the foundation for accessing the relevant block data.

In Step 2, the algorithm employs the AB-M tree structure to extract the user address key from the user block set. This extraction is essential, as it allows for the precise

identification of all associated user block file name records, ensuring that the retrieval process targets the correct data.

If the initial search does not yield any user block file names, Step 3 instructs the algorithm to locate all suitable block file names and repeat the extraction process outlined in Step 2. This iterative approach enhances the algorithm's effectiveness by ensuring that no potential matches are overlooked.

Finally, in Step 4, the results from Steps 2 and 3 are consolidated to generate a user-related block file, which serves as the target file for the user's query. This structured process not only improves the accuracy of block retrieval but also contributes to the overall efficiency of accessing blockchain data.

Figure 5.5 depicts the architecture used for EHR search, which uses the MTMCB block name file to hold block names and patient addresses. The structure of this file is an important component of the logical storage system for block names. The file's key consists of a user transaction identifier, represented by a 20-byte hexadecimal integer encapsulating the data of the transaction participants, followed by a separator ";". In addition, a 32-byte SHA 256 value is inserted to protect data integrity, which is followed by the "#" sign.

In circumstances where user and block name files are often accessed, relying exclusively on traditional disc storage may fall short of meeting the expectations of efficient retrieval. During startup, users must read, semantically process, and store data, while Redis clusters are used for caching and replicating data. The identification of frequently accessed memory data adds to shorter query times. In contrast to relational databases, Redis uses logical mode conversion to key-value pairs. The structure of Redis keys is critical, and its cache design considerably improves query speed while consuming less memory. However, as the number of users and transactions increases, retrieving EHR data from the Redis cache may become increasingly difficult. The AB-M-tree is efficiently linked with the Redis cache, ushering in a harmonic approach to data management and retrieval.

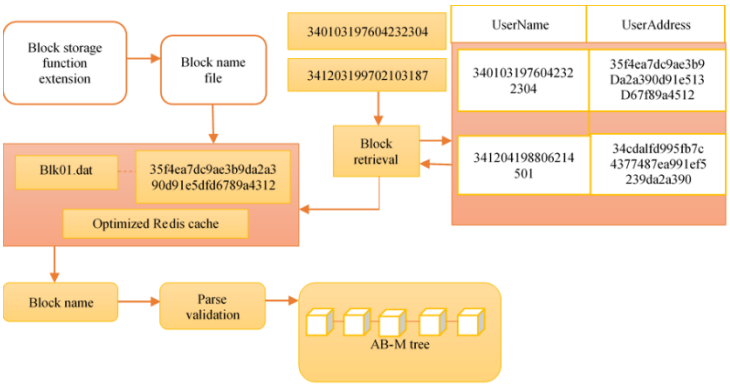

Figure 5.5 Architecture of EHR retrieval

The financial transactions are considered as $T = \{T_1, T_2, T_3, \dots T_N\}$. To generate a polynomial $F(Z)$, the transaction hash is evaluated initially using $\hbar(T) = \hbar\{T_1, T_2, T_3, \dots T_N\}$, with order of N, such as $F\left(\hbar(T_1)\right) - 0, u \in \{1,2,3,4, \dots, N\}$. A polynomial is generated next as given by Eq. (5.22)

$$(Z) = \left(Z - \hbar(T_1)\right)\left(Z - \hbar(T_2) \dots \dots \left(Z - \hbar(T_N)\right)\right) \tag{5.22}$$

The condition 1 is then concluded further as given by Eq. (5.23)

$$F(Z) = ZN + CM^{-1}ZM^{-1} + \cdots + C^{-1}Z + C_0 \tag{5.23}$$

Where the coefficients are denoted by $[CM^{-1}, CM^{-2}, \dots, C_0]$. The above equation is then calculated as shown in Eq. (5.24) when $F(Z) = 0$

$$ZN + CM^{-1}ZM^{-1} + \cdots + C^{-1}Z + C_0 \tag{5.24}$$

Additionally, the condition 2 is divided by $-C_0$ on both sides and obtained Equation (5.25) and Equation (5.26).

$$ZN + CM^{-1}ZM^{-1} + \cdots + C^{-1}Z + C_0 \tag{5.25}$$

$$\frac{-1}{C_0}Z^M + \frac{-C^{M-1}}{C_0}Z^{M-1} + \cdots + \frac{-C_1}{C_0}Z \tag{5.26}$$

It is considered that $R_m = \frac{-1}{C_0} Z^M$, $R_m - 1 = \frac{-C^{M-1}}{C_0} Z^{M-1} + \cdots + R_1 = \frac{-C_1}{-A_0}$ generates polynomials.

$$W(Z) = R_M Z^M + R_{M-1} Z^{M-1} + \cdots + R_1 Z \tag{5.27}$$

Finally, it is concluded as given by Equation (5.28)

$$W\big(\hbar(T)\big) = 1 \tag{5.28}$$

Where, $T_U \in T$

Further, the vector Φ is determined as $\{\Phi_1, \Phi_2, \Phi_3, \ldots \Phi_{M-1}, \Phi_M\}$ and $\hbar s_j$ is the other vector which is represented as given by Equation (5.29)

$$\hbar s_j = [\hbar_1(T_u), \hbar_1(T_u)^2, \hbar_1(T_u)^{M-1}, \hbar_1(T_u)^M\ ] \tag{5.29}$$

Where the product obtained from both the vectors Φ and $\hbar s_j$ is given as $\Phi \hbar s_j = 1$. The consensus vector Φ is thoroughly checked, whenever a new block index is generated in the network. This is to ensure that there are no false positives to occur.

At present, the data layer assesses to ensure that a hub's inquiry has been completed. If the hub is fully occupied, data is obtained from local sources. When dealing with a light hub, on the other hand, it searches for a fully populated hub or even the entire secure blockchain to fulfil the request. The inquiry procedure starts with the most recent block and works its way down to the nearest B block header. Because the root typically contains the maximum and minimum leaf hub initiator addresses, when the broker combines transaction data into this block, it is organised correctly. The procedure includes a step to ensure that is K_1 outside the given range. If K_1 falls inside the predefined range, the system searches the AB-M tree. The scanning procedure within the AB-M tree determines the layer node storage structure.

Queries are processed via a balanced binary tree search, with the lookup node receiving information from a Merkle tree. When the AB-M tree scan is finished, the system moves on to the next block search. Importantly, the hash values derived from the leaf nodes are present in the higher nodes of the AB-M tree, essentially making the AB-M tree resistant to manipulation. Any change, whether in the upper or lower contents, results in a change in the block header hash value, exposing any malicious manipulation. The proposed technique for retrieving EHRs was created to connect the 'user block collection' and the 'user set,' hence eliminating the requirement for a block name file. To obtain a patient's medical records, it is necessary to query the smart healthcare system's block files. Service providers can easily access doctors' (users') block files, and if a patient's EHR is contained in the user file, the patient's block file names can be obtained directly from the user block file, reducing retrieval time.

5.4 RESULTS AND DISCUSSION

The suggested EHR retrieval strategy has been developed in Python and tested on a computer with an Intel(R) i7-8700 CPU running at 3.20GHz and 16 GB of RAM. This method relied heavily on Redis version 6.2.7, with the system running Ubuntu 20.04 64-bit. Unexpectedly, no prior research has been uncovered that integrates the parts of an AB-M tree, Redis caching, and a lattice-based ring signature scheme within a blockchain environment for EHR retrieval. The proposed EHR retrieval technique was evaluated using several criteria, including upload and download timings, encryption and decryption speeds. These characteristics were extensively examined to assess the effectiveness and efficiency of the proposed approach, highlighting its original addition to the area.

The lattice-based ring signature technique effectively built a privacy-focused storage system within the smart healthcare environment. However, it had longer storage and retrieval times, especially when dealing with greater block sizes and a higher number of users. Despite this, when it involves overall system performance, the proposed approach consistently outperforms all other retrieval schemes that

were tested. As shown in Tables 5.1 and 5.2, detailed performance parameters, such as encryption and decryption times, were compared between the lattice-based ring signature scheme and various cryptographic approaches such as RSA, ECC, and ABE.

Table 5.1 Encryption and decryption time (ms) for block size 1200

No of users	LBRSS		RSA		ECC		ABE	
	Encryption time	Decryption time	Encryption time	Decryption time	Encryption time	Decryption time	Encryption time	Decryption time
5	2255	2257	2999	3003	3881	3885	4234	4236
10	2299	2301	3311	3315	3889	3901	4654	4658
15	3245	3248	3356	3359	4001	4006	4765	4768
20	3445	3449	3458	3441	4111	4117	4799	4812

Table 5.2 Encryption and decryption time (ms) for block size 2800

No of users	LBRSS		RSA		ECC		ABE	
	Encryption time	Decryption time	Encryption time	Decryption time	Encryption time	Decryption time	Encryption time	Decryption time
5	2300	2359	3150	3100	3950	3930	4340	4350
10	2360	2454	3400	3410	3950	4000	4780	4746
15	3390	3390	3426	3459	4130	4142	4865	4869
20	3449	3594	3520	3600	4254	4269	4899	4935

Figures 5.6 to 5.9 show that the Lattice-Based Ring Signature Scheme (LBRSS) consistently displayed the fastest encryption and decryption times, surpassing rival schemes such as RSA, ECC, and ABE. Notably, as the number of users increased,

both LBRSS and RSA demonstrated comparable performance levels. However, LBRSS outperformed the other systems in cases with fewer users.

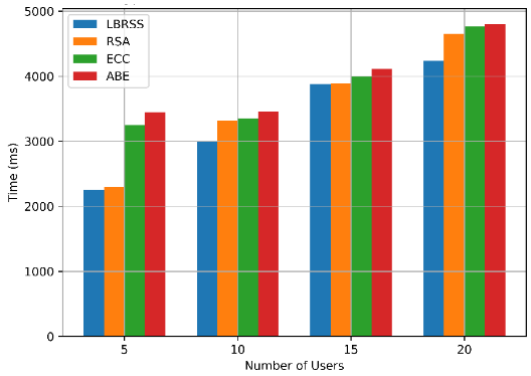

Figure 5.6 Encryption time for block size 1200

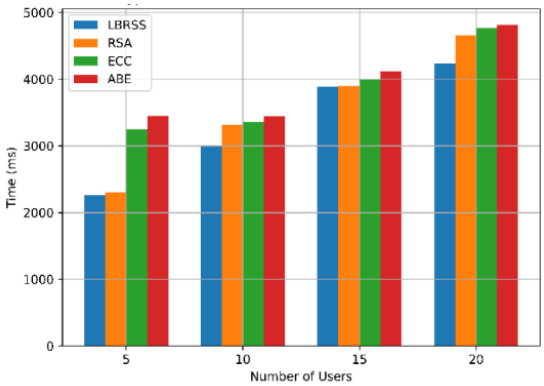

Figure 5.7 Decryption time for block size 1200

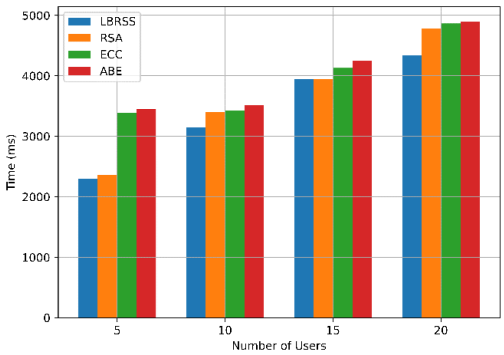

Figure 5.8 Encryption time for block size 2800

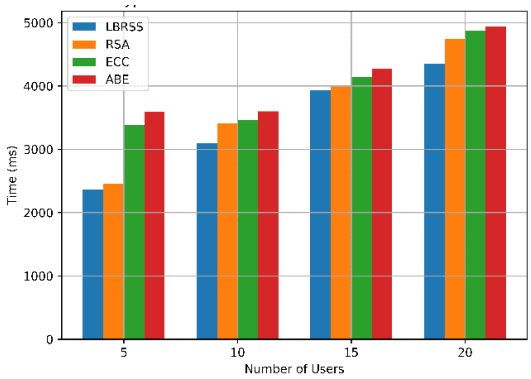

Figure 5.9 Decryption time for block size 2800

The study conducts an evaluation encompassing two distinct block sizes (1200 and 2800) and various user counts (5, 10, 15, and 20). To assess the effectiveness of the proposed EHR retrieval method, it is pitted against EHR retrieval without Redis, the B+ tree EHR retrieval scheme, and the conventional block retrieval system. Comprehensive comparative analyses of these retrieval systems, under varying conditions, are documented in Tables 5.3 and 5.4. Furthermore, visual representations of the results are illustrated in Figures from 5.10 to 5.13.

Table 5.3 Upload and download time (ms) for block size 1200

No of users	Proposed EHR retrieval		Proposed EHR retrieval without Redis		B+ tree EHR retrieval		Traditional block retrieval	
	Upload time	Download time	Upload time	Download time	Upload time	Download time	Upload time	Download time
5	11	11	40	45	43	48	68	73
10	24	28	56	59	65	62	72	88
15	45	49	64	71	81	88	92	96
20	68	71	82	85	91	98	99	104

Table 5.4 Upload and download time (ms) for block size 2800

No of users	Proposed EHR retrieval		Proposed EHR retrieval without Redis		B+ tree EHR retrieval		Traditional block retrieval	
	Upload time	Download time	Upload time	Download time	Upload time	Download time	Upload time	Download time
5	92	94	142	145	183	187	221	224
10	94	97	144	139	189	192	241	243
15	97	98	148	151	192	198	262	265
20	103	110	157	167	196	199	283	288

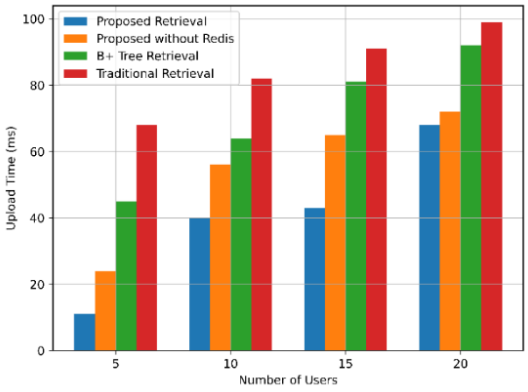

Figure 5.10 Upload time for block size 1200

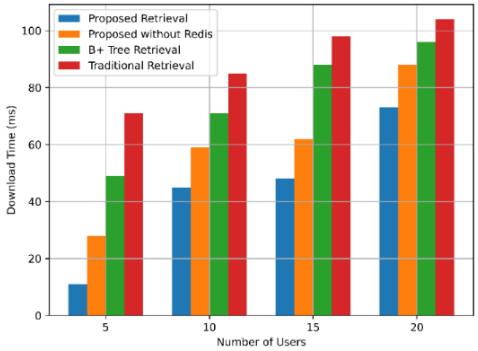

Figure 5.11 Download time for block size 1200

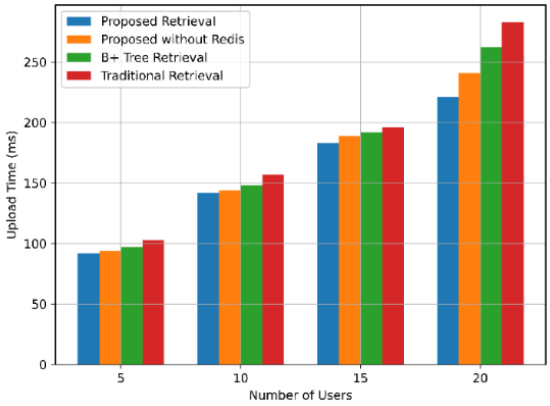

Figure 5.12 Upload time for block size 2800

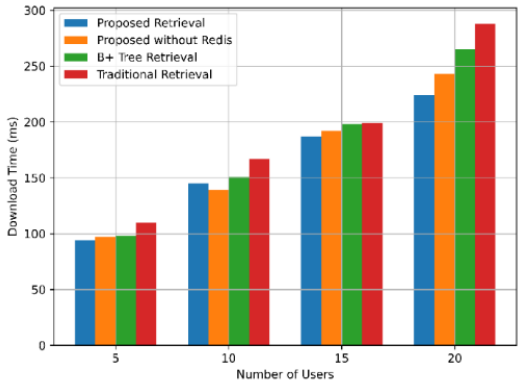

Figure 5.13 Download time for block size 2800

Figures 5.10 and 5.11 show that the suggested EHR retrieval technique achieves the fastest upload times, with upload times of 11 ms for block sizes of 1200 and 2800, respectively. As seen in Figures 5.12 and 5.13, the same system also has the shortest download timings, 11 ms for block size 1200 and 94 ms for block size 2800. These data highlight the large performance gains provided by the proposed retrieval methodology, with or without Redis, when compared to B+ tree retrieval and traditional block retrieval approaches. The addition of the Redis caching mechanism significantly improves system speed.

5.5 SUMMARY

This chapter describes an innovative EHR retrieval approach for a blockchain-based smart healthcare system that makes use of Redis caching, an Adaptive Balanced Merkle (AB-M) tree, and a lattice-based ring signature scheme. These three important components are quickly integrated into the consortium blockchain framework to build a secure and efficient smart healthcare ecosystem. The Redis cache is critical for providing essential caching and NoSQL services, whereas the proposed technique successfully saves data blocks. The approach excels at quick retrieval via a Merkle tree and quick verification through a balanced binary tree. The lattice-based ring signature system helps to develop a reliable storage mechanism. To validate the suggested technique, extensive testing is performed with two alternative block sizes and varying user counts. Comparative analyses are performed, comparing the suggested technique against traditional block retrieval systems, EHR retrieval without Redis, and EHR retrieval using B+ trees. The results support the proposed approach's superiority, as it continuously outperforms other contemporary methods across their respective performance baselines, demonstrating its potential for revolutionary EHR retrieval in the smart healthcare domains.

CHAPTER 6
CONCLUSION AND FUTURE SCOPE

An EHR is a digital repository that holds critical health information and is a subset of the larger Health Record or Medical Record. This digital storage system promotes streamlined collaboration among healthcare providers, facilitates training activities, and generates valuable data for research endeavours. Because EHRs are fundamentally sensitive, it is critical to provide secure sharing among various healthcare bodies. This work proposes the development of a robust system using blockchain technology to address the issues associated with EHR management. Blockchain, known for its decentralized structure, immutability, and non-repudiation guarantee, appears to be a strategic option for increasing the security and integrity of EHRs. Blockchain's decentralized nature ensures that no single authority controls the entire system, resulting in a more resilient and transparent infrastructure. Furthermore, because blockchain technology is immutable, once data is recorded, it cannot be edited or tampered with, establishing a high level of trust in the integrity of the stored medical records. Non-repudiation guarantees an additional layer of accountability, ensuring the legitimacy of transactions and data exchanges within the EHR system. Using these features, the proposed blockchain-based EHR system aims to create a reliable and secure framework for storing and sharing EHRs, ultimately contributing to breakthroughs in healthcare interoperability and data-driven research projects.

A new approach known as DZTBS is developed in the first study to promote secure data sharing by combining smart contracts with a zero-trust framework and blockchain technology. Essentially, the DZTBS strategy focuses on secure data storage and encoding, attempting to facilitate information retrieval while maintaining the integrity, availability, and secrecy required for security and privacy. This new technique addresses two major issues: secure EHR sharing and the preservation of privacy in medical records exchanged from various sources. The

DZTBS solution effectively handles medical records that transcend criteria by utilizing the zero-trust principle through smart contracts. The DZTBS is being evaluated by measuring a variety of performance indicators, including block production time, blockchain memory consumption, total transaction time, execution time, proof generation, evidence verification, and key generation. When compared to existing encryption algorithms such as AES and ECDSA, the DZTBS methodology is significantly more efficient, with mean encryption and decryption times of 0.001053 and 0.00365 seconds, respectively. These findings highlight the DZTBS strategy's increased security and efficiency in the field of healthcare management systems.

The second study focuses on the digital revolution in the healthcare sector driven by information technology advancements and the increasing demand for personalized, data-centric care. Traditional centralized storage systems present risks such as a single point of failure and privacy breaches. The study proposes a comprehensive approach, leveraging blockchain technology's decentralized architecture for efficient data exchange and retrieval in smart healthcare. The primary objectives include developing an innovative data-sharing system using blockchain's parallel and distributed computing capabilities and proposing a robust data retrieval algorithm for quick and precise location of healthcare data on the blockchain. The approach involves sharding, parallel processing, and privacy-preserving techniques. The proposed methodology focuses on optimizing data management and accessibility within the blockchain network, introducing dynamic sharding, adaptive dynamic sharding, load balancing, and parallel transaction validation. The data-sharing mechanism integrates these techniques into the ‘sHealthCareBlockchain’ framework, aiming to enhance efficiency and security in healthcare applications. The study also introduces a data retrieval algorithm using Merkle-Patricia Trie and Bloom filters for quick and precise access to specific healthcare information. The results showcase the proposed system's superiority in terms of data upload times, download times, throughput, latency, delay, and response time compared to a traditional blockchain without the proposed

enhancements. The findings suggest that the ‘sHealthCareBlockchain’ offers an efficient and secure solution for data sharing in smart healthcare applications.

The third study introduces a novel method for accessing EHRs in a blockchain-based smart healthcare system. In the second phase of our research, we propose a novel approach to gaining access to EHRs in a blockchain-based smart healthcare system. This solution includes critical components like Redis caching, an AB-M tree, and a lattice-based ring signature system. These components integrate seamlessly into the consortium blockchain infrastructure, providing a secure and efficient foundation for a smart healthcare ecosystem. Redis caching should be used strategically to provide essential cache and NoSQL services, while the proposed technique effectively saves data blocks. The method is used in rapid retrieval with a Merkle tree and quick verification with a balanced binary tree. The lattice-based ring signature system complements a strong storage mechanism. To validate the efficacy of our proposed technique, we conduct extensive testing with varying block sizes and user counts. The suggested EHR retrieval technique delivers excellent upload times, with only 11 ms required for block sizes of 1200 and 2800, respectively. Similarly, the system has the quickest download times, with 11 ms for block size 1200 and 94 ms for block size 2800. These results demonstrate the significant performance advantages provided by our retrieval methodology, whether or not it uses Redis when compared to B+ tree retrieval and traditional block retrieval methodologies. The use of Redis caching technology significantly improves system performance. Overall, this study firmly establishes the superiority of our proposed technique, consistently outperforming other contemporary methods across multiple performance baselines, demonstrating its potential to revolutionize EHR retrieval in smart healthcare.

6.1 FUTURE SCOPE

Future efforts should be focused on improving the storage protocol and streamlining computational processes. With the dynamic evolution of the healthcare landscape, there is an increased need to investigate the scalability of

blockchain- EHR systems to ensure efficient handling of increasingly large datasets.

Additionally, incorporating advanced ML algorithms to conduct statistical analysis on patient data significantly improves the overall healthcare system. Efforts should be directed toward investigating interoperability standards that allow for the unified exchange of EHRs across diverse healthcare platforms, thereby advancing patient care.

The incorporation of advanced technologies, such as AI-driven NLP, has the potential to transform EHR retrieval methods, making them more intuitive and context-aware. Developing an advanced blockchain system based on DL models seeks to safeguard the healthcare management system against potential blockchain attacks, ensuring patient data integrity and security.

REFERENCES

[1] Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. (2021). The revolution of blockchain: State-of-the-art and research challenges. *Archives of Computational Methods in Engineering*, *28*, 1497-1515.

[2] Javed, I. T., Alharbi, F., Margaria, T., Crespi, N., & Qureshi, K. N. (2021). PETchain: A blockchain-based privacy enhancing technology. *IEEE Access*, 9, 41129-41143.

[3] Baig, M. J. A., Iqbal, M. T., Jamil, M., & Khan, J. (2021). Design and implementation of an open-Source IoT and blockchain-based peer-to-peer energy trading platform using ESP32-S2, Node-Red and, MQTT protocol. *Energy reports*, *7*, 5733-5746.

[4] Rahman, M., & Saifullah, A. (2022). Transparent and Tamper-Proof Event Ordering in the Internet of Things Platforms. *IEEE Internet of Things Journal*, *10*(6), 5335-5348.

[5] Kołodziej, M. (2021). Development factors of blockchain technology within banking sector. In *Contemporary Trends and Challenges in Finance: Proceedings from the 6th Wroclaw International Conference in Finance* (pp. 125-138). Springer International Publishing.

[6] Kaur, M., Khan, M. Z., Gupta, S., Noorwali, A., Chakraborty, C., & Pani, S. K. (2021). MBCP: Performance analysis of large scale mainstream blockchain consensus protocols. *IEEE Access*, *9*, 80931-80944.

[7] Ramani, V. (2023). *Data interoperability and privacy schemes in healthcare data using Blockchain technology* (Master's thesis, V. Ramani).

[8] Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, 68, 1-13.

[9] Hölbl, M., Kompara, M., Kamišalić, A., & Nemec Zlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry*, *10*(10), 470.

[10] Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain technology use cases in healthcare. In *Advances in computers* (Vol. 111, pp. 1-41). Elsevier.

[11] Gnambs, T. (2021). The development of gender differences in information and communication technology (ICT) literacy in middle adolescence. *Computers in Human Behavior*, *114*, 106533.

[12] Nijor, S., Rallis, G., Lad, N., & Gokcen, E. (2022). Patient safety issues from information overload in electronic medical records. *Journal of Patient Safety*, *18*(6), e999-e1003.

[13] Sarwar, E. (2023). Laying an Ethical Foundation in Healthcare in the Era of PM. In *Global Perspectives on Precision Medicine: Ethical, Social and Public Health Implications* (pp. 157-188). Cham: Springer International Publishing.

[14] Amin, S. U., & Hossain, M. S. (2020). Edge intelligence and Internet of Things in healthcare: A survey. *Ieee Access*, *9*, 45-59.

[15] Omar, I. A., Hasan, H. R., Jayaraman, R., Salah, K., & Omar, M. (2021). Implementing decentralized auctions using blockchain smart contracts. *Technological Forecasting and Social Change*, *168*, 120786.

[16] Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., Bukhari, W. A., & Khan, M. I. A. (2022). Blockchain technology in healthcare: A systematic review. *PloS One*, 17(4), e0266462. https://doi.org/10.1371/journal.pone.0266462.

[17] Tomar, K., & Sharma, S. (2024). A proposed artificial intelligence and blockchain technique for solving health insurance challenges. In *Data-Driven Technologies and Artificial Intelligence in Supply Chain* (pp. 31-57). CRC Press.

[18] Amudha, G. (2022). Dilated transaction access and retrieval: Improving the information retrieval of blockchain-assimilated internet of things transactions. *Wireless Personal Communications*, *127*(1), 85-105.

[19] Wang, T., Zhou, Y., Ma, H., & Zhang, R. (2022). Enhanced dual-policy attribute-based encryption for secure data sharing in the cloud. *Security and Communication Networks*, *2022*.

[20] Liu, R., Yu, X., Yuan, Y., & Ren, Y. (2023). BTDSI: A blockchain-based trusted data storage mechanism for Industry 5.0. *Journal of King Saud University-Computer and Information Sciences*, *35*(8), 101674.

[21] Jia, D. Y., Xin, J. C., Wang, Z. Q., Lei, H., & Wang, G. R. (2021). SE-chain: a scalable storage and efficient retrieval model for blockchain. *Journal of Computer Science and Technology*, *36*(3), 693-706.

[22] Zhang, D., Wang, S., Zhang, Y., Zhang, Q., & Zhang, Y. (2022). A secure and privacy-preserving medical data sharing via consortium blockchain. *Security and Communication Networks*, *2022*.

[23] Yuan, X., Luo, F., Haider, M. Z., Chen, Z., & Li, Y. (2021). Efficient Byzantine consensus mechanism based on reputation in IoT blockchain. *Wireless Communications and Mobile Computing*, *2021*, 1-14.

[24] Zou, R., Lv, X., & Zhao, J. (2021). SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system. *Information Processing & Management*, *58*(4), 102604.

[25] Ma, X., Wang, C., & Chen, X. (2021). Trusted data sharing with flexible access control based on blockchain. *Computer Standards & Interfaces*, *78*, 103543.

[26] Kumar, R., Wang, W., Kumar, J., Yang, T., Khan, A., Ali, W., & Ali, I. (2021). An integration of blockchain and AI for secure data sharing and detection of CT images for the hospitals. *Computerized Medical Imaging and Graphics*, *87*, 101812.

[27] Chen, M., Malook, T., Rehman, A. U., Muhammad, Y., Alshehri, M. D., Akbar, A., Bilal, M., & Khan, M. A. (2021). Blockchain-Enabled healthcare

system for detection of diabetes. *Journal of Information Security and Applications*, 58, 102771.

[28] Ngabo, D., Wang, D., Iwendi, C., Anajemba, J. H., Ajao, L. A., & Biamba, C. (2021). Blockchain-based security mechanism for the medical data at fog computing architecture of internet of things. *Electronics*, *10*(17), 2110.

[29] Abunadi, I., & Kumar, R. L. (2021). BSF-EHR: blockchain security framework for electronic health records of patients. *Sensors*, *21*(8), 2865.

[30] Christo, M. S., Jesi, V. E., Priyadarsini, U., Anbarasu, V., Venugopal, H., & Karuppiah, M. (2021). Ensuring improved security in medical data using ecc and blockchain technology with edge devices. *Security and Communication Networks*, *2021*, 1-13.

[31] Kaur, J., Rani, R., & Kalra, N. (2022). A Blockchain-based Framework for Privacy Preservation of Electronic Health Records (EHRs). *Transactions on Emerging Telecommunications Technologies*, *33*(9), e4507.

[32] Dhasarathan, C., Hasan, M. K., Islam, S., Abdullah, S., Khapre, S., Singh, D., Alsulami, A. A., & Alqahtani, A. (2023). User privacy prevention model using supervised federated learning-based block chain approach for internet of Medical Things. *CAAI Transactions on Intelligence Technology*.

[33] Agrawal, K., Aggarwal, M., & Tanwar, S. (2023). MyEasyHealthcare: An efficient and secure three-tier blockchain-based healthcare system. *Security and Privacy*, *6*(6), e314.

[34] Rani, D., Kumar, R., & Chauhan, N. (2024). A secure framework for IoT-based healthcare using blockchain and IPFS. *Security and Privacy*, *7*(2), e348.

[35] Abid, A., Cheikhrouhou, S., Kallel, S., & Jmaiel, M. (2022). NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. *Software: Practice and Experience*, *52*(4), 841-867.

[36] Liu, W., He, Y., Wang, X., Duan, Z., Liang, W., & Liu, Y. (2023). BFG: privacy protection framework for internet of medical things based on blockchain and federated learning. *Connection Science*, *35*(1), 2199951.

[37] Al-Aswad, H., El-Medany, W. M., Balakrishna, C., Ababneh, N., & Curran, K. (2021). BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. *Arab Journal of Basic and Applied Sciences*, *28*(1), 154-171.

[38] Yao, S., Jing, P., Li, P., & Chen, J. (2022). A multi-dimension traceable privacy-preserving prevention and control scheme of the COVID-19 epidemic based on blockchain. *Connection Science*, *34*(1), 1654-1677.

[39] Xu, S., Zhong, J., Wang, L., He, D., Zhang, S., & Shao, W. (2023). A privacy-preserving and efficient data sharing scheme with trust authentication based on blockchain for mHealth. *Connection Science*, *35*(1), 2186316.

[40] Nasr Esfahani, M., Ghahfarokhi, B. S., & Etemadi Borujeni, S. (2024). Blockchain-based end-to-end privacy-preserving scheme for IoT-based healthcare systems. *The Journal of Supercomputing*, *80*(2), 2067-2127.

[41] Settipalli, L., Gangadharan, G. R., & Bellamkonda, S. (2024). An extended lightweight blockchain based collaborative healthcare system for fraud prevention. *Cluster Computing*, *27*(1), 563-573.

[42] Kumar, M. S., & Nagalakshmi, V. (2023). Secure transfer of robust healthcare data using blockchain-based privacy. *Cluster Computing*, 1-17.

[43] Suganthi, P., & Kavitha, R. (2023). Secure and privacy in healthcare data using quaternion based neural network and encoder-elliptic curve deep neural network with blockchain on the cloud environment. *Sādhanā*, *48*(4), 206.

[44] Chelladurai, U., & Pandian, S. (2022). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *13*(1), 693-703.

[45] Raghav, Andola, N., Venkatesan, S., & Verma, S. (2023). Privacy-preserving cloud data sharing for healthcare systems with hybrid blockchain. *Peer-to-Peer Networking and Applications*, *16*(5), 2525-2547.

[46] Babu, E. S., Yadav, B. R. N., Nikhath, A. K., Nayak, S. R., & Alnumay, W. (2023). MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. *Cluster Computing*, *26*(4), 2217-2244.

[47] Qu, Y., Ma, L., Ye, W., Zhai, X., Yu, S., Li, Y., & Smith, D. (2023). Towards Privacy-Aware and Trustworthy Data Sharing Using Blockchain for Edge Intelligence. *Big Data Mining and Analytics*, *6*(4), 443-464.

[48] Samuel, O., Omojo, A. B., Onuja, A. M., Sunday, Y., Tiwari, P., Gupta, D., Hafeez, G., Yahaya, A. S., Fatoba, O. J., & Shamshirband, S. (2023). IoMT: A COVID-19 Healthcare System Driven by Federated Learning and Blockchain. *IEEE Journal of Biomedical and Health Informatics*, 27(2), 823–834.

[49] Lodha, L., Baghela, V. S., Bhuvana, J., & Bhatt, R. (2023). A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring. *Measurement: Sensors*, *30*, 100904.

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

[51] Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. *Internet of Things and Cyber-Physical Systems*, *3*, 309-322.

[52] Kamal, R., Hemdan, E. E. D., & El-Fishway, N. (2023). Care4U: Integrated healthcare systems based on blockchain. *Blockchain: Research and Applications*, *4*(4), 100151.

[53] Sabu, S., Ramalingam, H. M., Vishaka, M., Swapna, H. R., & Hegde, S. (2021). Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain. *Global Transitions Proceedings*, *2*(2), 429-433.

[54] Liu, Y., Yu, W., Ai, Z., Xu, G., Zhao, L., & Tian, Z. (2022). A blockchain-empowered federated learning in healthcare-based cyber physical systems. *IEEE Transactions on Network Science and Engineering*.

[55] Wu, G., Wang, S., Ning, Z., & Zhu, B. (2021). Privacy-preserved electronic medical record exchanging and sharing: A blockchain-based smart healthcare system. *IEEE journal of biomedical and health informatics*, *26*(5), 1917-1927.

[56] Suganthi, P., & Kavitha, R. (2023). Secure and privacy in healthcare data using quaternion based neural network and encoder-elliptic curve deep neural network with blockchain on the cloud environment. *Sādhanā*, *48*(4), 206.

[57] Vidhya, S., & Kalaivani, V. (2023). A blockchain based secure and privacy aware medical data sharing using smart contract and encryption scheme. *Peer-to-Peer Networking and Applications*, *16*(2), 900-913.

[58] Lin, G., Wang, H., Wan, J., Zhang, L., & Huang, J. (2022). A blockchain-based fine-grained data sharing scheme for e-healthcare system. *Journal of Systems Architecture*, *132*, 102731.

[59] Chelladurai, U., & Pandian, S. (2022). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, *13*(1), 693-703.

[60] Raghav, Andola, N., Venkatesan, S., & Verma, S. (2023). Privacy-preserving cloud data sharing for healthcare systems with hybrid blockchain. *Peer-to-Peer Networking and Applications*, *16*(5), 2525-2547.

[61] Liu, J., Fan, Y., Sun, R., Liu, L., Wu, C., & Mumtaz, S. (2023). Blockchain-aided privacy-preserving medical data sharing scheme for e-healthcare system. *IEEE Internet of Things Journal*.

[62] Babu, E. S., Yadav, B. R. N., Nikhath, A. K., Nayak, S. R., & Alnumay, W. (2023). MediBlocks: secure exchanging of electronic health records (EHRs) using trust-based blockchain network with privacy concerns. *Cluster Computing*, *26*(4), 2217-2244.

[63] Maurya, C., & Chaurasiya, V. K. (2023). Collusion-resistant and privacy-preserving data sharing scheme on outsourced data in e-healthcare system. *Multimedia Tools and Applications*, *82*(26), 40443-40472.

[64] Rathee, G., Garg, S., Kaddoum, G., & Hassan, M. M. (2023). A secure emotion aware intelligent system for Internet of healthcare. *Alexandria Engineering Journal*, *75*, 605-614.

[65] Chamola, V., Goyal, A., Sharma, P., Hassija, V., Binh, H. T. T., & Saxena, V. (2023). Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management. *Neural Computing and Applications*, *35*(31), 22959-22969.

[66] Mahajan, H. B., & Junnarkar, A. A. (2023). Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. *Multimedia Tools and Applications*, *82*(28), 44335-44358.

[67] Zakzouk, A., El-Sayed, A., & Hemdan, E. E. D. (2023). A blockchain-based electronic medical records management framework in smart healthcare infrastructure. *Multimedia Tools and Applications*, *82*(23), 35419-35437.

[68] Kumar, M. S., & Nagalakshmi, V. (2023). Secure transfer of robust healthcare data using blockchain-based privacy. *Cluster Computing*, 1-17.

[69] Alruwaili, F. F., Alabduallah, B., Alqahtani, H., Salama, A. S., Mohammed, G. P., & Alneil, A. A. (2023). Blockchain Enabled Smart Healthcare System using Jellyfish Search Optimization with Dual-Pathway Deep Convolutional Neural Network. *IEEE Access*.

[70] Meier, P., Beinke, J. H., Fitte, C., Schulte To Brinke, J., & Teuteberg, F. (2021). Generating design knowledge for blockchain-based access control to personal health records. *Information Systems and e-Business Management*, *19*, 13-41.

[71] Zhao, Y., Liu, L., Qi, Y., Lou, F., Zhang, J., & Ma, W. (2020). Evaluation and design of public health information management system for primary

health care units based on medical and health information. *Journal of infection and public health*, *13*(4), 491-496.

[72] Chanias, S., Myers, M. D., & Hess, T. (2019). Digital transformation strategy making in pre-digital organizations: The case of a financial services provider. *The Journal of Strategic Information Systems*, *28*(1), 17-33.

[73] Aljamal, R., El-Mousa, A., & Jubair, F. (2019, April). A user perspective overview of the top infrastructure as a service and high performance computing cloud service providers. In *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)* (pp. 244-249). IEEE.

[74] Lakhan, A., Mohammed, M. A., Rashid, A. N., Kadry, S., Panityakul, T., Abdulkareem, K. H., & Thinnukool, O. (2021). Smart-contract aware ethereum and client-fog-cloud healthcare system. *Sensors*, *21*(12), 4093.

[75] Liu, Y., Zhang, L., Yang, Y., Zhou, L., Ren, L., Wang, F., Liu, R., Pang, Z., & Deen, M. J. (2019). A Novel Cloud-Based Framework for the Elderly Healthcare Services Using Digital Twin. *IEEE Access*, 7, 49088–49101.

[76] Rajabion, L., Shaltooki, A. A., Taghikhah, M., Ghasemi, A., & Badfar, A. (2019). Healthcare big data processing mechanisms: The role of cloud computing. *International Journal of Information Management*, *49*, 271-289.

[77] Qiu, J., Liang, X., Shetty, S., & Bowden, D. (2018, September). Towards secure and smart healthcare in smart cities using blockchain. In *2018 IEEE international smart cities conference (ISC2)* (pp. 1-4). IEEE.

[78] Hussien, H. M., Yasin, S. M., Udzir, N. I., Ninggal, M. I. H., & Salman, S. (2021). Blockchain technology in the healthcare industry: Trends and opportunities. *Journal of Industrial Information Integration*, *22*, 100217.

[79] Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE access*, *7*, 147782-147795.

[80] Gul, M. J., Subramanian, B., Paul, A., & Kim, J. (2021). Blockchain for public health care in smart society. *Microprocessors and Microsystems*, *80*, 103524.

[81] Rathee, G., Sharma, A., Saini, H., Kumar, R., & Iqbal, R. (2020). A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. *Multimedia Tools and Applications*, *79*(15), 9711-9733.

[82] Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation research part e: Logistics and transportation review*, *142*, 102067.

[83] Chakraborty, S., Aich, S., & Kim, H. C. (2019, February). A secure healthcare system design framework using blockchain technology. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 260-264). IEEE.

[84] Sriram, R. D., & Subrahmanian, E. (2020). Transforming health care through digital revolutions. *Journal of the Indian Institute of Science*, *100*(4), 753-772.

[85] El Majdoubi, D., El Bakkali, H., & Sadki, S. (2021). SmartMedChain: A blockchain-based privacy-preserving smart healthcare framework. *Journal of Healthcare Engineering*, *2021*.

[86] Gupta, S., Sharma, H. K., & Kapoor, M. (2023). *Blockchain for secure healthcare using internet of medical things (IoMT)* (pp. 1-197). Springer.

[87] Kumar, A., Krishnamurthi, R., Nayyar, A., Sharma, K., Grover, V., & Hossain, E. (2020). A novel smart healthcare design, simulation, and implementation using healthcare 4.0 processes. *IEEE access*, *8*, 118433-118471.

[88] Kumar, A., Kumar Sharma, D., Nayyar, A., Singh, S., & Yoon, B. (2020). Lightweight proof of game (lpog): a proof of work (pow)'s extended

lightweight consensus algorithm for wearable kidneys. *Sensors*, *20*(10), 2868.

[89] Wehde, M. (2019). Healthcare 4.0. *IEEE Engineering Management Review*, *47*(3), 24-28.

[90] Tu, J., Zhang, J., Chen, S., Weise, T., & Zou, L. (2020). An improved retrieval method for multi-transaction mode consortium blockchain. *Electronics*, *9*(2), 296.

[91] Ali, A., Pasha, M. F., Fang, O. H., Khan, R., Almaiah, M. A., & K. Al Hwaitat, A. (2022). Big data based smart blockchain for information retrieval in privacy-preserving healthcare system. In *Big Data Intelligence for Smart Applications* (pp. 279-296). Cham: Springer International Publishing.

[92] Dewangan, N. K., & Chandrakar, P. (2021, December). Patient feedback based physician selection in blockchain healthcare using deep learning. In *International Conference on Advanced Network Technologies and Intelligent Computing* (pp. 215-228). Cham: Springer International Publishing.

[93] Bhattacharya, P., Saraswat, D., Dave, A., Acharya, M., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Coalition of 6G and blockchain in AR/VR space: Challenges and future directions. *IEEE Access*, *9*, 168455-168484.

[94] Mardiansyah, V., Muis, A., & Sari, R. F. (2023). Multi-State Merkle Patricia Trie (MSMPT): High-Performance Data Structures for Multi-Query Processing Based on Lightweight Blockchain. *IEEE Access*.

[95] Balobaid, A. S., Alagrash, Y. H., Fadel, A. H., & Hasoon, J. N. (2023). Modeling of blockchain with encryption based secure education record management system. *Egyptian Informatics Journal*, *24*(4), 100411.

[96] Liu, Y., Liu, A., Xia, Y., Hu, B., Liu, J., Wu, Q., & Tiwari, P. (2023). A blockchain-based cross-domain authentication management system for IoT devices. *IEEE Transactions on Network Science and Engineering*.

[97] Bhattacharya, P., Saraswat, D., Dave, A., Acharya, M., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Coalition of 6G and blockchain in AR/VR space: Challenges and future directions. *IEEE Access*, *9*, 168455-168484.

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

[99] Wang, S., Zhang, D., & Zhang, Y. (2019). Blockchain-based personal health records sharing scheme with data integrity verifiable. *IEEE Access*, *7*, 102887-102901.

[100] Sanka, A. I., Chowdhury, M. H., & Cheung, R. C. (2021). Efficient high-performance FPGA-Redis hybrid NoSQL caching system for blockchain scalability. *Computer Communications*, *169*, 81-91.

[101] Jawahar, M., Sabari, A., & Monika, S. (2021). Identity authentication-based load balancing with Merkle hash tree for secured cloud data storage. *International Journal of Business Innovation and Research*, *25*(3), 408-430.

[102] Leevik, A., Davydov, V., & Bezzateev, S. (2023). Threshold Lattice-Based Signature Scheme for Authentication by Wearable Devices. *Cryptography*, *7*(3), 33.

LIST OF PUBLICATIONS

JOURNAL ARTICLES:

1. Deepak Kumar Sharma, Adarsh Kumar. "An Efficient Data Sharing Scheme Using MultiTransaction Mode Consortium Blockchain for Smart Healthcare" in International Journal of System of Systems Engineering. DOI:10.1504/IJSSE.2025.10059329.
2. Deepak Kumar Sharma, Adarsh Kumar. "A Blockchain based Solution for Efficient and Secure Healthcare Management" in International Journal of Critical Infrastructures.DOI:10.1504/IJCIS.2025.10060627.

CONFERENCE PAPER:

1. Deepak Kumar Sharma, Adarsh Kumar. “Blockchain for Patient Data Integrity: Decentralised Storage and Retrieval in Modern Healthcare Systems”. In: Santosh, K., *et al.* Recent Trends in Image Processing and Pattern Recognition. RTIP2R 2023. Communications in Computer and Information Science, vol 2027. Springer, Cham. DOI: 10.1007/978-3-031-53085-2_28

First Page of Plagiarism Report

Thesis v21

ORIGINALITY REPORT

8%	4%	7%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	link.springer.com Internet Source	1%
2	ebin.pub Internet Source	<1%
3	"Blockchain for Biomedical Research and Healthcare", Springer Science and Business Media LLC, 2024 Publication	<1%
4	www2.mdpi.com Internet Source	<1%
5	Da-Yu Jia, Jun-Chang Xin, Zhi-Qiong Wang, Han Lei, Guo-Ren Wang. "SE-Chain: A Scalable Storage and Efficient Retrieval Model for Blockchain", Journal of Computer Science and Technology, 2021 Publication	<1%
6	www.researchgate.net Internet Source	<1%
7	www.inderscience.com Internet Source	<1%