**E-HEALTHCARE SYSTEM IN CLOUD COMPUTING USING BLOCKCHAIN AND MEDCHAIN TECHNOLOGY TO PROTECT USER DATA**

**3.1. Introduction**

Blockchain can share data reliably without third party intervention is a distributed public ledger database maintained by the verifier or nodes and storage invariant block networks. The data, in order to promote the cryptographic signature and consensus, it will be recorded using an algorithm that has been promulgated as a key to the application. To save the data, this feature is a large amount of data is distributed widely exchange, is an important reason to promote health care, the use of medium-blockchain.

In medical industry is the main candidate for the blockchain technology is it has in order to solve the important issues such as possibilities for verification and public health management of automated billing. This technology allow patient own data, who thereby, the ownership and sharing of data, it can choose to deal with the existing concerns, and to share. Conventional data access control technology, because it establish and implement a secure access strategy for having a completely reliable server, it is difficult to get the latest distributed network environment.

By selecting decentralization and trustlessness, blockchain be distributed file system to people, reliable point-to-point transmission provides new concepts consensus mechanisms and encryption algorithms. In recent years, ABE is an important technical means for the security requirements in a cloud computing environment, ABE access control mechanism has been analyzed in extensive computing environment. The encryption mechanism, using the attributes as a public key, the mechanism is, in essence, to link the ciphertext of the user via the attribute. Its flexibility will guarantee a significant cloud data storage security in the form of encryption and access control. The encryption mechanism, using the attributes as a public key, the mechanism is, in essence, to link the ciphertext of the user via the attribute. Its flexibility will guarantee a significant cloud data storage security in the form of encryption and access control.

However, there are still some challenges in the adoption of medical blockchain. Among the major technical obstacles, efficiency is one of the most concern issue. Existing blockchain based solution is inefficient by sharing data streaming from Internet of Things (IOT) devices. First, IoT data of the devices, the serial data is the time of the stream, such as ECG signals. In terms of storage, they are divided into a number of data blocks. The difference of a single medical records, access to the data stream is that it requires access to all of the data block. Existing system design, it can verify the integrity of the record in order to verify the data stream, they need to download the digest of each block, in order to access particularly long stream, and non-efficient it is to check all possible ways. Second, the description of the data can be changed at any time and manage information variables in Blockchain, a new block consumes more storage space or need, than is need to add rewrite the entire Blockchain.

MedChain, hash value of the link that has been created record issue the access to the EMR problem in blockchain, instead of keeping data itself. To access the records, encrypted query link, have access rights, it will be sent over HTTPS to the relevant participants. Therefore, the hash value is not changed during transmission is acquired outside the store blockchain properties to ensure as a hash value is unique to the original document. In order to improve the security, MedChain the link query, key the electronic medical record in a different location than the key. Privacy has been maintained in the MedChain the adoption of smart contract for managing the transaction timeout. In order to improve the security, MedChain the link of the query, key and Electronic Medical Records in a different location. Privacy has been maintained in the MedChain the adoption of smart contract for managing the transaction timeout. Security and access control have been maintained by employing advanced encryption and authentication technologies through Blockchain.

MedChain is used master public key to encrypt the message, related secret key to the have been distributed in a distributed ElGamal re-encryption mode of pieces to set of proxies agent, it has distributed the adoption of private key. Therefore, it will not be able to be able to decrypt the whole message instead it decrypt that message. According ElGamal re-encryption mode, the set of proxy nodes should be configured in a system that has a public key and a unique public / private key pair known to the other proxy node.

In addition, all of the proxy node, a secret key that corresponds to it and has a master public key has been distributed to the proxy node. Each proxy node, blindly use the coefficient of the message dazzling ElGamal homomorphic multiplication random to encrypt, in order to decrypt it, using its own private key. The results of decoding as long as the decoding unblind value message is not determined that it is possible to perform only via a predetermined receiver, in order to create a hidden plaintext will unblind use the original random blind factor.

The MedRec is distributed Electronic Medical Records management system using the blockchain technology. The MedRec, management authority among the participants, is a module designed for sharing authority and data. The access to the outside of their access rights and encryption data of blockchain to the patient's medical record, in order to save hash point, it emphasized the ability of MedRec. It is highly available, scalable, and because there is flexibility in the price, cloud computing is considered a quick solution for sharing medical data storage. However, for medical data sharing of privacy and confidentiality requirements, additional security measures must be applied in order to reduce the risk of cloud procurement of medical and public health fields.

**3.2. Problem identification factors**

S. Wang et al (2018) describes to improve the accuracy of diagnosis and the effectiveness of treatment, a framework of parallel healthcare systems (PHSs) based on the artificial systems computational experiments parallel execution (ACP) approach is proposed then, analyze, and evaluate various treatment plan, to apply the computer experiment in order to realize the parallel execution of decision support and real-time optimization to actual and artificial healthcare process.

A. Omar et al (2021) propose a general framework for the contract process in the healthcare supply chain, including detailed algorithms that explain the various interactions between HCSC stakeholders. Group Purchasing Organizations (GPO) is a key stakeholder in HCSC and offers benefits such as cost savings, volume discounts and supplier selection. However, the current GPO contract process is time consumption and inefficient.

Kumar et al (2020) proposed Blockchain technology has proven to be suitable for almost all areas due to its cryptographic security and immutability. The purpose of this work is to design an intelligent healthcare system, which is found to be possible by combining the integration and interoperability of real-life health care situations.

P. P. Ray et al (2021) describes Internet of Things (IoT) and blockchain technology are widely developed and used in many areas, especially in e-healthcare. In the field of healthcare, IoT devices can provide real-time sensor data from patients for processing and analysis. However, blockchain cannot solve these serious problems by providing decentralized computing and storage for IoT data.

M. Zarour et al (2020) describes Blockchain technology will improve existing IT facilities in many areas technological developments have made significant progress in the healthcare industry. Information security and accessibility are important considerations for integration and communication with electronic medical record (EHR) systems when sharing personal medical information.

P. Li et al (2020) explains the ChainSDI framework uses blockchain technology and rich edge computing resources to manage secure data sharing and computation of sensitive patient data. However, when designing and deploying healthcare applications in heterogeneous home-edge cloud environments, it face the challenges of data interoperability and regulatory compliance.

G. S. Aujla et al (2021) demonstrates in health monitoring sensors can form large Internet of Things (IoT) networks that continuously monitor data and send it to nearby devices and servers. However, connecting these IoT-based sensors to different entities can lead to security vulnerabilities. Security vulnerabilities can be exploited by attackers because of the openness of data. These are major problem, especially in the area of health care where the values of sensor data change.

A. Mazlan et al (2020) describes coordination and validation are simplifying records are designed to be updated on a regular basis, and there is no difference between the databases. It focuses on how blockchain solves scalability challenges and provides solutions in the healthcare sector through the implementation of blockchain technology.

E. Daraghmi et al (2019) proposed the system design based on the blockchain named MedChain has been proposed for managing medical records it aims to improve the existing system. However, more work is needed to better describe, understand, and evaluate blockchain technology applications in the healthcare industry.

T. Muhammed et al (2018) explains Mobile cloud computing can meet future healthcare needs by collecting and analyzing patient data at anytime, anywhere. However, network delay, bandwidth, and reliability are one of the many obstacles to the realization of next-generation healthcare.

S. Abolfazli et al (2014) introduces Cloud-based Mobile Augumentation (CMA) is the most advanced enhancement model that uses near and far clouds to enhance, and optimize the computing power of mobile devices. However, smartphones are miniature, it impose specific limits on computing power and battery life, preventing Resource-intensive Mobile Applications (RMA) from running.

R. Ranchal et al (2020) describes Cloud computing infrastructure includes the ability to continuously retrieve data from multiple heterogeneous sources, efficient data integration, and big data analytics. However, due to the ambiguity, and migrating a medical workload to the cloud is not an easy task.

S. Roy et al (2019) proposed a new solution that offers a combination of fine-grained access control to cloud-based multi-server data and a provable and secure mobile user authentication mechanism for the healthcare industry.

L. A. Tawalbeh et al (2016) describes Big data analytics is to support connected healthcare and mobile cloud computing. With the adoption of cloud computing in health care, the motivation and development of network healthcare applications and systems is also introduced.

Jindal et al (2018) proposed a new patient health information sharing scheme that protects privacy allows HSPs to access and retrieve PHI files in a safe and effective way. However, there are some privacy issues when sharing confidential information.

Xu, N et al (2019) introduces MCC technology is widely deployed in a variety of healthcare applications and specifically describes common architectural and design considerations that need to be considered when designing an MCC for a healthcare scenario.

X. Wang et al (2015) explains Patients can approve doctors by setting up an access tree that supports flexible threshold predicates. Based on this, a new attribute-based, specified verifier signing technology is designed to meet levels of security and privacy requirements. Many methods of access control and anonymous authentication schemes are not directly available.

C. Baktir et al (2018) demonstrates Cloud computing provides an unlimited pool of resources for latency-tolerant services such as machine learning model training. Delayed sensitivity to personalization of healthcare services and ongoing health assessments requires computing infrastructure close to the end user.

S. Yan et al (2021) describes a decentralized cloud computing environment relies on a complex communication and sharing paradigm to facilitate access, information processing, and analytics. A difficult feature of this cloud computing environment is concurrency and accessibility, during both service providers and end users rely on a common shared platform.

**3.3 Materials and methods**

MedRec is a distributed Electronic Medical Records (EMRs) management system that uses blockchain technology. MedRec is a modular design that manages permissions, approvals, and data sharing between participants. Focusing on emphasized the ability of MedRec to encrypt external data it store patient health records and hash pointers to access rights within the blockchain.

EMRs will continue to be stored in the provider's database to reduce the need to store the patient's EMR on the blockchain and utilize existing systems. Since the healthcare provider currently maintains and manages the EMR the patient can only read the data, and provider node is responsible for the blockchain maintenance.

Since all access to EMR is done via the blockchain, a history of these accesses is stored on the blockchain, providing a complete view of all events that have occurred on EMR. The MedChain system uses blockchain technology, which is a set of technologies for creating data chains. With this technology, each new data is linked to the previous data chain via an encrypted hash function. Therefore, it significantly increases the difficulty of attacks and improves the privacy and security of EMR. Since all access to EMR is done via the blockchain, a history of these accesses is stored on the blockchain, providing a complete view of all events that have occurred on EMR.

Decision making based Proof of Authority (PoA) Consensus (DPoAC) algorithm

Medical records DB

DB manager

Validation process

Provider node

DB manager

Validation process

Patient’s node

Super Peer

Advanced encryption techniques

Immutable Information

Mutable Information

**Figure 3.1 Proposed diagram for efficient healthcare using blockchain and medchain**

Figure 3.1 describes MedChain is built on a decentralized network that connects all healthcare providers, including hospitals, medical centers, clinics and healthcare enterprises. It adopt a simple but reasonable peer selection method. The blockchain server maintains a complete blockchain to verify data integrity and audit activity. The directory server maintains a list of healthcare data, maps them to actual storage locations, and manages sessions for data sharing. MedChain does not require the healthcare provider to migrate the actual data to the new system, it provide a reference to the data on the old system for access.

**3.4 Medical records DB**

Medical records stored in a provider database by creating a link to that record. The function of DB Manager is to navigate an existing database and it create a query link for patient medical records. Medical records are stored in the supplier's existing database and the blockchain can be integrated as an access control layer to allow interaction between participants. The medical records in the provider's existing database, as well as the reference addresses and permissions for these records, are stored on the blockchain network.

**3.5 Provider node**

The provider node calculates the degree of association with the provider node in the network. The node order is calculated based on the quantity and quality of EMR stored in the database. Multiple methods and multiple attributes can be used to define the quality of medical records, based on the purpose and perspective of the designed system. Generally speaking, the quality of a medical record should be judged by whether the record meets its intended purpose. The provider node's DB Manager provides an access interface to the existing database and sends the patient's Ethereum address and its "patient" role to the Nodes Consensus Contract (NCC) for verification.

**3.6 Patient’s node**

The patient node sends the provider's ID to its EHR to get the relevant patient record address. After receiving the address, patient node sends the requested record file name and patient Ethereum address to the EHR. The EHR forwards the request to the access control to see if the received Ethereum address has permissions (that is, a "read" access level) on the requested record. If the patient node has permission, access control forwards the patient's encrypted symmetric key to EHR. The EHR forwards the received key and database access information to the patient node in sequence.

**3.7 Block chain and Medchain technology in healthcare**

Based on the blockchain-based EMR system, propose a new incentive mechanism to measure its efforts in maintaining medical records and creating new blocks, and the extent to which provider nodes are used from the perspective of the EMR system. Provider nodes of lower order are more likely to be selected to create new blocks. Therefore, since the hash value is specific to the original document, the hash value stored in the blockchain it ensures that no changes are made outside the blockchain during transmission.

First, the blockchain only stores immutable records however, the actual data location may change. When a URL is modified, a new block containing the new URL must be generated, instead modifying old block. Secondly, their data sharing scheme will not reclaim space after sharing. For additional security, MedChain stores query links, keys and EMRs in different locations. MedChain maintains patient’s privacy by managing your transactions using time-based smart contracts. Security and access control is maintained using advanced encryption and identity verification technology across the blockchain.

**3.8 Decision making based Proof of Authority (PoA) Consensus (DPoAC)**

Decision making based Proof of Authority (PoA) Consensus (DPoAC) is the proposed algorithm in order to provide the patient, interoperable secure and effective access to medical records medical service providers, the existing it is intended to improve the system and other third party is not allowed to access patient's privacy. These methods, to manage the transaction, in order to control access to the regular electronic medical record, it use a smart contract. To maintain the medical records, making full use of the scope of their efforts to create a new block for the medical service providers, and advanced new incentive mechanism to provide additional security to this work it uses an encryption technology.

**3.9 Advanced Encryption Techniques**

After successfully loading the data into the cloud healthcare application, each patient record is encrypted using a secure algorithm. Therefore, individual keys are generated for encryption and decryption. Key generation follows the ECC algorithm and is used for data encryption. The generated key and the corresponding record or database are automatically stored in the cloud database for future verification. The generated keys and encrypted data are variable and immutable information that improve the security level of cloud data. The generated key and the rest of the data are encrypted. The GUI has navigation buttons that help to view the next level of data the patient's record is encrypted and stored in the cloud. If the provider needs to know more about the patient, the record must be decrypted before downloading. The key is very secure in terms of security because it is known only to the data owner and not to other third parties in providing data security.

**3.10 Super peer**

The new block is instantiated and distributed across all super peers in the patient network. When most nodes approve the new block, the system inserts its chain. This provides a global view of the patient's medical history in an efficient, verifiable and permanent way. If the agreement is reached, a fork will be created in the chain, the block will be defined as isolated and will not belong to the main chain.

**3.11 Summary**

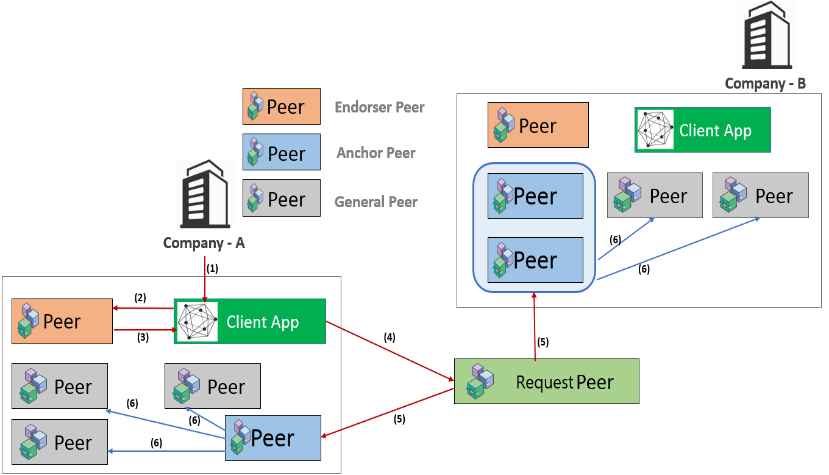
System design based on blockchain MedChain is proposed to manage EMR. MedChain aims to be compatible with existing EMR databases and improve current EMR management systems these are used to provide medical service providers, patients, and third parties with interoperable, secure, and efficient access to EMR while preserving patient privacy. At MedChain, blockchain maintenance, is including the creation, validation, and addition of new blocks, is the responsibility of medical service provider, allowing patients to securely control access to EMR. MedChain's privacy uses time-based smart contracts to manage transactions and monitor the calculations performed by EMR by implementing acceptable usage policies. It use hash technology to ensure data integrity it maintain security and access control by using advanced encryption and identity verification technology across the blockchain. It uses comprehensive logging to provide interoperability, auditability, and accessibility. The proposal is independent of a particular system, the variant of which may be applicable to other similar systems, allowing multiple access to electronic records.

**LINEAR ELLIPTICAL CURVE DIGITAL SIGNATURE (LECDS) WITH BLOCKCHAIN APPROACH FOR ENHANCE THE SECURITY ON CLOUD SERVER**

**4.1. Introduction**

Blockchain is a distributed ledger that records time series transactions. Different centralized general ledger servers maintain the general ledger in the Blockchain network and all nodes on the server update transaction on each participating node. Blockchain enforces trust by doing transaction processing in the validation process (Merkel tree) that has been hashed with transparency and transactions to make it immutable. Blockchain eliminates the risk of a single point of failure because it is distributed in nature, and every network node makes a copy of the transaction data. Blockchain guarantees the integrity of transactions and thus allows for fast transactions between two parties without mediation to provide a guarantee.

There are two main categories of Blockchain technology: Permission less and granting. Permission less Blockchain, commonly referred to as public Blockchain, is open to all users. However, while it has huge potential like Bitcoin, it may not be suitable for business owners who want to control transaction processing systems. Business processes can participate in the complex operations of customized solutions and then limit outsiders to have specific requirements and needs. Permission less Blockchain also likes scalability and is affected by some challenges in regulatory and control evolution. It allows exploring other options like Blockchain that empower companies to have personal control. It only joins the Blockchain network and limits trusted participants. The Blockchain that grants permissions is also called a private Blockchain.



**Figure 4.1 Hyperledger fabric Blockchain architecture**

Figure 4.1 defines Hyperledger fabric Blockchain architecture for trust operators who want them to process and maintain transaction records accurately and securely. Peers in the member organization will receive a customer transaction call request from within the organization. Clients can have specific organizational / business activities for specific application/service portals. Endorser, to check the details of the certificate and other verification transactions. Anchors peers get updates and telecast renovation from other peers within the organization. Orderer peer has been considered as a central communication channel for its Hyperledger fabric network of peers. Since the operation is mainly manual, there is also the possibility of loopholes and fraud in daily transactions. As a result, we cannot guarantee the integrity and reliability of many businesses. Hyperledger is an effort to collaborate on cross-industry Blockchain technologies and create and promote open source. The Hyperledger deployment platform can provide a highly confidential, flexible, and extensible degree to support distributed ledger solutions.

The elliptic curve code is widely used to protect mini automated devices. In secret securitizing and allocation of just text, the images and more of the multimedia content also be secured with LECC. Therefore, LECC-based cryptology research is emerging as an interdisciplinary area and combines with growing mathematics, electronic, electrical and computer science.

**4.2 Problem identification**

J. Ma et al. (2020), the novel discusses the earlier method, presents the blockchain security issues in the cloud, and analyzes the existing methods. Assuming this paper number of n companions and f is the maximum of the malicious nodes, Hyperledger proposes to enable PeerBFT to handle Byzantine failures in the fabric sorting service. The Emergency Access Control Management System (EACMS) proposed this paper clearance management based on Blockchain hyperledger fabric and hyperledger composer R. Rajput et al. (2019). Data Items the organization suggested regarding the use of emergency and term smart contracts may specify certain restrictions to limit patients' health achievement (PHR) permissions and define certain rules. Licensing management of PABC is based on the blockchain international patent application system. Patent applications may be modified or rejected without reliance on the patent office S. Bian et al. (2021). Professional Node's management system in every patent office in a country or region feels contracted for all applications. The literature S. Kakei et al. (2020) proposes a distributed authentication infrastructure called the Meta Indonesian Communist Party, through which multiple Certificate Authorities (CAs) can cross-certify algorithms such as exchange mechanisms.

A dynamic joint consensus project authority verifies and validates event data by new modules without any authority center H. Guo et al. (2020). It conducts numerical analysis and, based on it, proposes a quick leader election algorithm and Hyperledger Cloth Blockchain Network emulator test. A new Blockchain-based Reliable and Intelligent Animal Information Management System (RIVIMS) has been suggested for smart contracts and the use of machine learning technology N. Iqbal et al. (2021). The proposed RIVIMS includes two main modules; Blockchain is based on standard veterinary information management, data and forecast analysis modules. It is necessary to examine two of the four aspects of manufacturing and research systems: distributed ledger, cryptography, consensus protocol, and smart contract B. Huang et al (2020). The data processing workload is the framework for understanding the performance of private blockchains. Common software failures and blockchain-specific software failures T. T. A. Dinh et al. (2018) (e.g., the need for a transaction sender) affect the reliability and integrity of the Smart Contract Index and observations of absolute reliability.

After that, both consumer nodes use electronic energy converters to develop consumer profiles and consumption profiles for smart meters Á. Hajdu et al. (2020) in a real-life situation. Platform collectors use permissions to enable the data owner to ensure that only designated parties can process personal data and use smart contracts and encryption technology to record all data transactions within a standard distributed bargain. Provides a new method G. Sciumè et al. (2020) to address the shortcomings of the existing centralized system. N. B. Truong et al. (2020), the Permit Management Blockchain based on the Hyperledger-based Emission Trading System (HyperETS) is proposed. A measuring instrument used in shared blockchain-based constructions P. Yuan et al. (2019). The conceptual model is compared to the distributed measurement model discussed in the previous measurement tools and previous work.

Z. Lu et al. (2019), the article explores the ongoing multi-party use of private data security supported by the Multi-Party Computation (MPC) Fabric. In our solutions, pioneers use MPC to store their data from the series before encryption and whenever such private data protection is required. The security properties of the sorting mechanism W. S. Melo et al. (2019), and the influence of late authentication messages on the federation's Blockchain protocol. Damage to the attacker can lead to news of honest players who are delayed by subsequent hit evidence. Blockchain F. Benhamouda et al. (2019) degree supplier management inventory sharing facility can design scientific research methods based on the Hyperledger fabric software model.

Then, the smart contract starts to calculate the basics and supports the possibility of adaptive load that can meet the needs of each customer; Blockchain will record customer energy consumption or generation T. Meng et al. (2021). The client-side should be aware of the deployment address of chain code T. Guggenberger et al. (2021) and endorsement policies within the platform. In past releases, this was statically configured on the client-side. Blockchain data integration-based programs can successfully avoid the problem of trusting third-party protocols Y. Manevich et al. (2019), but they must face major computational and overhead communication issues. This low security makes it difficult to provide different types of data classification for sensitive and non-sensitive user information.

The author introduces Merkle Hashing Tree (MHT) method to resolves high communication overhead and dynamic data validation in verifying the integrity of the data stored on the cloud server. Authentication of the server security index information will be merged into the data verification to avoid the attack server H. Wang et al. (2019). Authentication of the server security index information will be merged into the data verification to avoid server attacks. But this method didn't provide proper security for information in cloud storage and didn't improve communication efficiency.

**4.3. Implementation of the proposed method**

The proposed Linear Elliptical Curve Digital Signature (LECDS) with Hyperledger Blockchain framework provides security for sensitive and non-sensitive information from a cloud database. The cloud security method first classifies the user information before cloud storage. Data classification is determined based on the availability, integrity, and confidentiality of the security target and the data classification's sensitivity. Data owners must monitor the data throughout its life cycle and carefully analyze each piece of data to determine the potential impact of unauthorized leakage or destruction of these data. Symmetric key generation to provide a public key for each data for service verification. The non-sensitive data encryption to secure using an RSA method, and sensitive data are encrypted using an LECC method. The user request key and user policy are verified after the information is encrypted.

Sensitive

Non-Sensitive

LECC encryption/ Decryption

Modified Spider search optimization

Database

Key Auditing

Hyperledger Blockchain Authentication

Symmetric Key Generation

RSA encryption/ Decryption

Input file

User

Policy verifier

Linear regression

**Figure 4.2 proposed method block diagram**

The process of the proposed block diagram is present in figure 2. Modified Spider search optimization algorithm help to search the user request query information from the cloud. Once the policy is verified, all user query transactions are stored on a hyperledger, and a private network cloud Blockchain is created to request the user. In this data security framework, authorized users only can access both sensitive and non-sensitive data.

**4.3.1. Linear regression data classification**

The proposed LECC method is used to encrypt sensitive information and RSA methods to encrypt the non-sensitive information. Only the sensitive data is accessible easy to the authorized users. The data can be classified using different categories such as personal, student education, customer, card, information, health and banking, etc. In each category, some data is confidential, and those have been made secure so that non-authorized users won't have access to those data.

**Algorithm steps**

**Input:** User’s medical information

**Output:** Classify the sensitive information and non-sensitive information

Begin

Step 1: To train the subsets sensitive (s) (heart rate, pulse, BP etc.) and non-sensitive (ns) (name, area, and zip code) form dataset (ds)

Step 2: A trees 🡨

Step 3: 🡨{(Train, root)}

While q is not empty do

q🡨

If then

🡨Maxclass (ds)

Else if ds is linearly separable by a classifier then

🡨

Else

🡨 Predict selected by a split procedure split (ds)

Create child class and of

Return

End while

End

This sensitive and non-sensitive data classification using a machine learning method using linear regression. To train the data for cloud system sensitive data and non-sensitive features. Linear regression algorithm is done to classify the user’s medical sensitive information and non-sensitive information for name, area, and zip code.

To train the subsets sensitive, non- sensitive data

A trees 🡨

Predict selected by a split procedure split (ds)

If ds is linearly separable by a classifier

If

No

Yes

No

Yes

**Figure 4.3: Flow diagram for linear regression data classification**

Figure 4.3 illustrates flow diagram for linear regression data classification for split the data into user’s medical information sensitive (heart rate, pulse rate, disease etc.) and non-sensitive data (name, phone number, age etc.).

**4.3.2 Modified Spider Optimization search Algorithm**

MSOA expects the entire query space to be search query information, where all spiders communicate with each other. In this way, each array in space asks about the location of the cloud feature. All inquiries received by the spider are conformity estimates placed by social spider representatives. The updated spider is updated again with the help of Drosophila optimization algorithms to achieve better query selection. Drosophila optimization performed a wide range of user searches and sent food odor information to surrounding Drosophila during the foraging process. This algorithm designs two distinctive inquiry operators (spiders): sensitive and non-sensitive information to update the user query population. Each interaction is operated by various development operators who follow the unique, effective behaviors typically expected within the state. By characterizing the total amount of n-dimensional individuals, characterize the quantity of sensitive and non-sensitive spiders in the whole population F.

(4.1)

Where the User query and user sequence query

n= number of query information

**4.3.3. Fitness Evaluation**

Spider size is the trademark that assesses the individual ability to perform better than its allotted undertakings. Each user (spider) gets a feature (query) which indicates the arrangement quality that compares to the spider i (independent of information) of the populate F. Fit () is the fitness value received by estimating the spider location concerning the objective function F and the values, and are computed utilizing the below expression.

Spider size is a trademark that evaluates an individual's ability to work better than its assigned cause. Each user (spider) gets a feature (query) that indicates the quality of the permutations. It is compared to fill-in. Approximate () If the spider i (independent information) is the fitted value received by estimation, the relative spider position of the objective function F and the values and are using the fitness function.

**4.3.4. Modeling of the vibrations through the communal query**

Public queries are used as a mechanism for sending information between colony members. This information is encoded as a small vibration that is the key to the collective coordination of all individuals in the group. The quality of information depends on the weight and distance of the spiders they are producing. Individuals nearby have a stronger perception of vibrations than those far away, such as distance-induced vibrations and their relatives to the detection components. To reproduce this process, the personal vibration perception i is the result of the information sent by the authorized user j according to the following equation:

(4.2)

Where the is the Euclidian distance between the spiders i and j, such that

(4.3)

The algorithm starts by instating the set F of N spider locations every spider location, and is a dimensional vector consisting of the parameter qualities to be improved. Such values are arbitrarily and consistently dispersed between the pre indicated low beginning parameter limit. The higher primary value limit similarly as it conveyed by utilizing equation.

**4.3.5 Symmetric key generation**

Authentication is a mechanism provided by the user to check the integrity of the data stored in the cloud. The proposed method creates a private key Sk, controlling or creating a key on the cloud at the user's request. The keys in the cloud obtain by encrypting the sensitive and non-sensitive data. For each user request to verify in key auditing to allow the user. Well-known organizations for data authentication add MACs to their data.

**Algorithm steps**

Input: NULL

Output: Service Key Set SKS.

Begin

Step 1: Initialize Service set Ss.

Step 2: Identify the set of all services available.

SS =

Step 3: For each service Si from SS

Initialize service I'd SID.

Compute maximum bytes of streams to remain attached.

Ms =

If data ==S

Generate Encryption key Ek and encrypt using elliptic curve cryptography.

Else if data ==NS

Generate Encryption key Ek and encrypt using RSA.

Cs=compute the current size of the stream using the prime factor.

SID = .

Perform Encryption Cipher ∑ Encrypt (SID, EK).

Store Cipher, SID, EK to the key set.

SKS = {Cipher, SID, EK}.

End

LECC algorithm with Hyperledger and Modified Spider optimization search Algorithm (MSOA) to verify the user query information effectively encrypts the user's medical information.

Initialize Service set

Generate Encryption key using elliptic curve cryptography

For each service Si from SS

If data ==S

Calculated maximum bytes of streams to remain attached

If data ==S

Generate Encryption key Ek and encrypt using RSA.

Perform Encryption Cipher

No

No

Yes

Yes

**Figure 4.4: Flow diagram for Symmetric key generation**

Figure 4.4 Flow diagram for symmetric key generation. In addition, a 160-bit size LECC-based key offers the same level of security as obtained using 1024 bit RSA-based key generation.

**4.3.6 Hyperledger Fabric Blockchain**

The Hyperledger fabric's anatomy obtains a Blockchain network with authority set by the tissues trying to form the consortium. Each component unit in the Blockchain network is responsible for configuring the network in which the peer participates. All these peers' needs consist of certification authorities and other information similar to the appropriate cryptographic material.

* Membership Services Provider: Enrolls the clients
* Peers: Peer nodes can be endorsers (endorse the proposal for the transaction)and committer nodes (write block of transactions to the ledger)
* Chain code: Peer nodes having chain code becomes the endorser for that chain code. ESCC (Endorser system chain code) executes the chain code using read-write set information.

Hence Distributed Ledger Technology (DLT) to maintain all the user records. In this hyperledger fabric, blockchain following building block and flow is present in the figure. Generations within the membership organization receive customer transaction call requests from within the organization. The client can be any particular sensitive file for a particular application/service portal. All peers maintain their accounts per channel, and they subscribe.

**4.4. Summary**

Ensuring digital data security during storage and transmission is a great challenge faced by the digital society. New encryption schemes are needed to withstand new forms of attacks. RSA and LECC cryptography is an emerging field in cryptography and can produce strong encryption algorithms. The detailed study of the conventional symmetric encryption schemes and RSA-based cryptographic algorithms led to the development a novel RSA-based Symmetric Cipher. This proposed hyperledger Blockchain provides a higher security performance and classifies the sensitive and non-sensitive data from the cloud. The sensitive data will encrypt using an LECC method, and the RSA algorithm used to encrypt non-sensitive data. This Hyperledger encryption method provides efficient, stronger security. The SSO method searches the user query and fastest transaction query processing in the blockchain network. This overall proposed method LECDS method provides better performance compared to another existing method.

**MEDCHAIN SECURITY MANAGEMENT BASED REHASHING SHIFT CODE RAIL ENCRYPTION FOR ENHANCING THE DATA SECURITY**

**5.1. Introduction**

Blockchain innovation is a decentralized computerized record innovation that monitors as of late-developing information records and exchanges. The three principle models for blockchain distinguishing proof and access are public or lower-level endorsement, private or endorsement and association. The most significant and novel part of the blockchain idea is that the put-away data is completely ensured in the squares of the blockchain exchange. Its decentralized agreement model has three primary qualities: consistency, usefulness and adaptation to internal failure.

Blockchain innovation has been utilized well in different fields. While carrying out blockchain innovation on the Internet of Things (IoT) to trade and share network information, logs, confirmation and security administrations, related issues are being scrutinized, especially network security. Web of Things Business Unit Physics System. Many authorized organizations are attempting to guarantee their IoT organizations' legitimate activity, uprightness, and security right now. These organizations team up utilizing blockchain innovation and distributed computing. This innovation gives straightforwardness, unwavering quality and sufficient administration over IoT data frameworks.

Blockchain innovation rethinks the information model, and the public authority is carrying out blockchain in numerous IoT applications. Such applications are amazingly appealing with uncommon variation and the capacity to separate, secure, and share IoT information and administrations. Blockchain innovation is at the focal point of many advances in the present Internet of Things industry. One explanation is that numerous IoT administrations are defenseless against assault and challenge. The utilization of blockchain innovation can tackle numerous digital material science issues on the Internet. As the IoT business moves to the organization sensor model, certain advantages should be considered to assemble a feasible brilliant city and a significant number of its related parts.

Cloud user data is risky and can be lost, leaked or attacked, but there is no way to eliminate this ineligible situation. Cloud users don't even know with whom they process or share their data. Transparency is also a very serious problem. Cloud users have no information about data users or data flow within the cloud. Blockchain is a new technology that cloud users can use to increase trust, provide data security, and at the same time, outsource and retrieve services from the cloud. Compared to centralized database security, blockchain can offer a high degree of security. The blockchain uses a cryptographic hash function to continuously monitor the list of records linked to and protected by the previous block. Blockchain is a distributed ledger that allows to record transactions. Block chains are typically managed through peer-to-peer networks and are intended to disable any tampering. Blockchain can provide the same security as central database data storage. On the administrative side, can prevent data storage corruption and attacks. In addition, because the blockchain is open, it can provide data transparency when applied to fields that require public data. These benefits make it useful in various fields, including the financial sector and the Internet of Things (IoT) environment and its applications. Because of its performance and availability, cloud computing is used in many IoT environments. In addition, cloud security and privacy issues are discussed from key aspects of security.

Blockchain technology is investigated by analyzing general technology and research trends, discussing the safe use of Bit coin and solutions in future research areas. The investigation results can be used as important basic data for blockchain investigations and help understand the security issues known so far. Understanding blockchain security development trends can accelerate the development of blockchain technology in the future.

For block chains can use hash functions to verify the integrity of the block and transactions. Blockchain saves the hash value of the previous batch of information at the beginning of each block, allowing users to compare the calculated hash value with the saved hash value. Next, check the consistency of the previous batch of information. In the same way, can the hash function be used to create public-private key pairing? A hash pointer is a data structure that, in addition to the conventional mouse, contains some data and cryptographic hash associated with the information. Use custom pointers to retrieve information, and use hash pointers to verify that the information in the blockchain is a list of hash pointers linked by hash values. To ensure the integrity of the batch information, check whether the data in the batch has changed to the hash value.

**5.2. Problem identification factors**

Blockchain innovation adjusts exceptionally to the data age; it is becoming increasingly more alluring to the future. It can utilize blockchain innovation for the Internet of Things (IoT). Because of the headway of IoT innovation in different fields, conveyed frameworks have gained huge headway. The blockchain idea requires circulated information the board framework for putting away and sharing information and exchanges over the organization.

Blockchain innovation is intended to adjust to an assortment of non-monetary applications. Nonetheless, because of the intricacy of blockchain innovation, it is regularly troublesome and exorbitant for most engineers or gatherings to make, keep up with, and screen a blockchain network that upholds their applications.

Information is gathered from Edge terminals or Internet of Things (IoT) gadgets with processing innovation. In any case, the unwavering quality and security of information in the edge PC climate is a vital thought. It can cause difficult issues, particularly if the information gathered is deceitful or false or, on the other hand, if the information is abused or spread without consent.

Blockchain is a decentralized association, and security is a vital factor in its prosperity. Nonetheless, regardless of its prevalence and reception, it comes up short on a normalized model for concentrating on security dangers identified with block chain.

The Internet of Things has confronted numerous long periods of difficulties, including wellbeing, correlation, energy utilization, and variety of gear, because of the restricted energy and registering (handling, stockpiling, and so forth) assets of associated gadgets.

These applications have been created utilizing IoT innovation for constant following. Because of low preparing force and capacity limit, existing security and encryption innovation are not utilized, defenseless against knowledge assaults.

Blockchain technology is committed to changing the way to live, behave and act. Recently, education, business and researchers have been actively studying all aspects of blockchain as a new technology, unlike other blockchain research focusing on its use, challenges, properties or security, evolution, architecture, development architecture and chain technology.

Once successfully used in crypto currency, can explore business, industry and service systems, alternative functions offered by Ethereum smart contracts, and cryptographic security support for public and private keys.

In work certification and stock agreements, participants' incentives and consensus standards vary from person to person. An important part of this work is integrating the graphical model into the functions of blockchain and its components. It also enhances its advantages in data analysis by identifying relationships between data and extracting their true values.

Ethereum is a distributed blockchain that is known as the second-largest common chain after Bitcoin. As Ethereum is decentralized, the status of the specification is determined by a consensus mechanism by participants in the Ethereum network, and there is no centralized coordinator. Network participants must evaluate every transaction from the Beginning block. It requires many networks, computes, and storage resources, and this is impractical for devices with limited computing resources and many devices with intermittent network connections.

Identity verification is the first entry point for various information systems. Nevertheless, traditional centralized unilateral recognition is still weak, and there is a risk of unilateral failure or interference due to external attacks or internal fraud. On the fringe and in the Internet of Things (IoT) environment, blockchain can use margin devices to improve services for the Internet of Things and provide decentralized, high-security service solutions.

It has to deal with many new issues, including drug attacks, poor performance and data resources. Recent research is keen to explore this issue, which often leads to incredible performance, inefficiency and privacy leaks.

Cloud-based electronic medical record sharing solutions offer many features. Cloud centralization is inevitably a threat to data security and privacy protection due to its unique distribution, anonymity, counterfeit counterfeiting capabilities, and verification.

The quantifiable issue of block chain conventions has gotten far and wide consideration, and shortening is perhaps the most encouraging solution for block chain improvement. The essential thought behind the short code is to isolate the block chain network into a few gatherings, and each group manages separate issues.

The Internet is a model of new advancements dependent on wise frameworks that depend vigorously on manufactured stages, edge processing and the Internet of Things (IoT). IoT, Edge figuring and block chain mix are ideal ways of conveying new robotization administrations and plans of action with different positive components like self-check, self-enactment, consistency and information unwavering quality. It would be a significant factor. Progress Block chain keen agreements and holders are secure and confidential. Block chain permits a gathering of members to arrive at an agreement in a sad environment as an indispensable extra disseminated record. Stability is a block chain that permits information to be put away for all time however is at this point not lawfully legitimate, and the block chain contains illicit substance and can't be changed. Likewise, block chain change is required for the "right to be neglected" information guideline.

Block chain is a decentralized public and digital ledger technology used in peer-to-peer networks and has received widespread attention in various fields such as finance, healthcare and distribution chain. This problem is severely affecting the widespread adoption of block chain technology.

Block chain and other Distributed Ledger Technologies (DLTs) have been altogether evolved over the most recent couple of years. They are prescribed for some applications because of their capacity to give straightforwardness, repetition, and responsibility.

Block chain innovation gives a better approach to make a solid, dependable, and appropriate framework for tackling security and individual protection issues of Internet of Things (IoT) applications. Because of the great figuring force of the block chain mining measure, lightweight IoT gadgets need to ascertain assets to share their PC assignments from Edge servers.

Modern chain framework gear is regularly utilized for control order dissemination, information assortment, and collaboration in modern applications. These days, security dangers to modern chains are expanding, and modern administrative frameworks need certainty components.

Block chain architecture is a new solution for creating a distributed network and restructuring the traditional industrial IoT architecture. First, explore key issues in the traditional industrial IoT architecture and summarize existing solutions. Next, it will introduce security and privacy models to help design block chain-based architecture.

Identity-Based Encryption (IBE) is a public-key encryption system requiring certificate management in Public Key Infrastructure (PKI) and traditional public-key systems. Due to the deficiency of PKI, the issue of withdrawal in the IBE system is a major issue, and several reversible IBE schemes have been proposed to address this problem.

Patients can upload their Personal Health Information (PHI) files to the cloud, and Health Service Providers (HSP) can obtain the correct information to determine their health status in the cloud. This system can reduce not only medical costs but also provide a timely diagnosis to save lives. However, some privacy issues arise when sharing confidential information.

Malicious attackers can try various attacks through such channels. Therefore, it is essential to establish a secure authentication process between patient and client. Furthermore, the storage capacity of wearable devices is low and can solve this problem by providing storage services in the context of the cloud Computing Telemedicine Information systems.

Searchable Encryption Data allows users to select and retrieve documents encrypted in the cloud data based on their searches. Most searchable encryption programs focus only on accurate keyword searches, and if the data user writes incorrectly, these programs will not give the desired result.

**5.3. Materials and Method**

Med chain uses block chain technology to create a user-centric electronic medical record while maintaining a single true data version. Med chain allows users to give healthcare professionals access to their health data. Med chain then records the interaction with these data in Med chain distributed ledger in an auditable, transparent and secure manner. The use of block chain technology and how the med chain uses it to solve certain problems and improve user health care records. It is to improve the care of data by putting patients at the center of digital transformation in health care.

User

Input file

Adaptive memetic search Algorithm (AMSA)

Rehashing Shift Code Rail Encryption (RSCRE)

Decryption Key generation

Key Authentication

Key generation

Policy method

Med block chain

Decryption file

**Figure 5.1: Proposed block diagram**

Figure 5.1 describes the block chain network for analyzing the user's information sent and receiving using the med chain block chain policy database. User input files are encrypted using the Adaptive memetic search based on the med chain block chain to send and receive the information. RSCRE authenticates the secure information and downloads the files using the Rehashing Shift Code.

**5.4** **Adaptive memetic Search Algorithm**

The Adaptive Memetic Search Algorithm (AMSA) is an evolutionary computation-based technology. AMSA is considered to be an improved encryption algorithm is integrated with the local search mechanism. Adaptive AMSA performs well in their small size, but they perform as in dimension. Adaptive memetic algorithms have been developed to adaptively set environmental influencing factors for each person's learning ability. This leads to some degree of autonomous behavior, and the individual will gain some experience after some time. Simulation results demonstrate that this adaptation method can improve the quality of the results while reducing computational time, in the encrypted text file improving the searching keys. The Standard local search analyzes the optimal to generate the next position for using a key size based on the key search. Problem-solving can be implemented using precision methods, approximate algorithms or local search heuristics. Memetic finding good solutions or find solutions that cannot be reached only by local search methods.

**Algorithm steps for Adaptive Memetic Search Algorithm (AMSA)**

Standard Local Search (I)

Begin

Produce a string solution (S) to Problem Instance (I);

Evaluate each values;

Repeat until (Locally optimal) Do

AMSA🡪Using S and I generate the next position NI, S;

If (NI, S, Is better than S) Then

S: = NI, S;

End

While (Key < Key size)

Apply generate Key parameters (KP)

Apply local search;

End while

Stop

Where, AMSA- Adaptive Memetic Search Algorithm, N-number of text, S-string solution, I-problem instance, KP-Key parameters, Memetic algorithm evaluate the each values based on the condition, and it is compressing the searching time and complexity of files.

Evaluate each values

Adaptive Memetic Search Algorithm

If (N1>S) then S=N1

Repeat until true

While (Key<key size) then S=N1

Generate Key parameters

Apply local Search

End while

Yes

No

No

Yes

**Figure 5.2 Flow chart for Adaptive Memetic Search Algorithm (AMSA)**

Figure 5.2 describes the flow chart for Adaptive Memetic Search Algorithm (AMSA) for evaluating the values and check the key parameters and searching the values or attributes based on the AMSA process.

**5.5 Key Generation Rate (KGR)**

Cryptography is an important part of maintaining the security of the data and information in different organizations and needs to encrypt the data. Encryption also helps ensure the confidentiality and integrity of data being transmitted over the communication network. The importance of the key used for encryption is a key part of the strength of the algorithm. Most cryptographic algorithms are more secure in generating keys. The most important part of data encryption is that it does not repeat the key generated to ensure better results and be unbreakable. KGR represents the number of secret bits produced per second/measurement. It largely depends on the environmental conditions and determines the amount of randomness it can use for extraction. The real-time key generation process requires a high KGR because the encryption scheme requires a key of a certain length and the Advanced Encryption Standard (AES) requires a minimum length of 128-bit key series.

**Algorithm Steps**

Step 1: Select random two prime numbers x, y

Step 2: Calculate l=x\*y ------ (5.1)

Step 3: Calculate part

= (x-1)\*(y-1) ------- (5.2)

Step 4: Calculate encryption key

----- (5.3)

Step 5: Calculate decryption key

Step 6: Generate the random keys

Let assume p, s are two prime numbers, d refers to the decryption key, refers to the encryption key, mod refers to modular, and total totient. The above algorithm steps random key generation for the private key and secret key for encryption and decryption.

**5.6 Rehashing Shift Code Rail Encryption (RSCRE)**

A simple and efficient hash function, which can use for secure information authentication. This structure is mainly used for message verification on systems that implement stream cipher encryption, and it is also suitable for other applications. The proposed Rehashing Shift Code Rail Encryption (RSCRE)algorithm converts the given plain text into the fence cipher text by generating the arrangement of the plain text. The outer loop of the algorithm selects a tracking number starting from 1, and the inner loop puts letters into the password and calculates the letter's position in the message. The next character will be using Rehashing Shift Code Rail Encryption (RSCRE)selected by the outer loop until all the texts on that padding are finished. Suggest a Rail block-based allowed voting procedure for aggregation peer requests. Potential voting aggregators verify privacy, and the opposite key is verified to enhance security. Each part of this tree contains a hash of content in the encryption.

**Algorithm for Rehashing Shift Code Rail Encryption (RSCRE)** Begin

Cipher char ← 1

Step 1-Sender sends plain text data.

P\_len ← length of plaintext

For x ← 1 to Rehashing shift (RS) rail no

Flag ← 1

Step 2: Read the

Ordinary characters ← i

And ordinary characters ≤ p\_len

cipher text [cipher char] ← Plaintext [plain\_char]

Password character ← Password character +1

SR🡪 Changed the character values to right side

[Text\_ char] 1010🡪Using SR🡪0101

Step 3: Sender encodes the message using a secret key ()

tep 4-Delete all spaces in the text.

Step 5: Change the text to ASCII and then add odd numbers.

Step 6: Then again assign the ASCII values for the alphabet

Step 7: Convert the message into cipher text ()

= mod l

Exit

The algorithm above provides secure communication between the two over the network. The sender sends the data, changes the text value to an ASCII value, adds an odd number, and uses the Rehashing Shift Code Rail Encryption (RSCRE) algorithm to generate a secret key for secure communication. Let assume refers to plain text, the secret key, refers to cipher text, SR-Shift Right, l refers to modular of a security key, define odd numbers, and refers to the length of the message.

Length of plaintext

Read the characters

Cipher text [cipher char] ← Plaintext [plain char]

Sender encodes the message using a secret key ()

Change the text to ASCII

Again assign the ASCII values for the alphabet

Yes

No

Convert the message into cipher text

**Figure 5.3 Flow for Rehashing Shift Code Rail Encryption (RSCRE)**

Figure 5.3 shows the flowchart for Rehashing Shift Code Rail Encryption (RSCRE) Algorithm procedure. This method initially read the characters (Cipher and plain text converted), send the messages encoded using secret key and change the text in ASCII value, and finally converted messages into Cipher text.

**5.7 Data Decryption**

Decrypting data is the opposite of data encryption. Decoding is a method of transforming encrypted data into its original format. The private key decrypts the message provided to the authorized person, and the decryption process and format become file-readable format. Its main task is to convert the cipher text into plain text. The encrypted message can be decrypted using the private key and the private key. On the other hand, the recipient receives the plaintext and the translation when using the private key to decrypt.

**Algorithm Steps:**

Step 1: Encryption Message

Step 2: Enter the Private Key.

Step 3: Change the corresponding binary value to the ASCII value

Cipher char ← 1

char\_len ← length of cipher text

Step 4: Change the ASCII value to characters to be used to decrypt the message.

-------- (5.4)

For i ← 1 to rail value

Flag number 1

plain\_char ← i

Plain\_char is ≤ chiper\_len

Plaintext [plain\_char]

Cipher char ← cyber char +1

If i = 1 or i = rail no

plain\_char ← plain\_char + (Rail\_txt.1) × 2

End if

Step 5: Cipher text to plain text

--------- (5.5)

Step 6: original data.

The algorithm steps provide a receiver for decrypting data using the private key of a readable formatting process.

**5.8 Med Block chain Network Policy method**

Data is contained in a distributed block chain containing health records, files storage, and data throughput limitations; the information contained in the proposed health block chain will be an index, a list containing health records and data for all users. Med Chain is defined as a permitted block chain, and only trusted parties have the right to operate the block chain on a private network. These parties will manage Med Chain and form alliances to ensure compliance with relevant regulations and interoperability standards. Permission is further extended to patients, and alliance members review them before creating an account. This process can reflect the patient's portal. All will store medical data in a database called Data Lake by Block chain. Data Lake is highly scalable and can store all data types, from images to documents to key-value storage. The latter system provides the same hashing and authentication strength of a completely random matrix, but the random cost, key size and implementation complexity are significantly reduced. Independently and interestingly, when combined with (secure) stream ciphers, the attributes required by the hash function can safely authenticate.

Medical Data

Peer

Peer

Peer

Peer

Peer

SC

SC

Peer

SC

SC

SC

SC

SC

Peer

Ledger

SC-Smart contract

APPLICATION

Encrypt and digital signature

Update

Medical Data Policy validate

Medical Block chain

Result

**Figure 5.4 Medical Block chain policy methods**

Figure 5.4 described as, The Medical block chain network has trusted verification nodes, each containing a copy of the network ledger to maintain the consistency of the distributed ledger. The ledger contains a block chain and a data pool and stores a consistent, ordered record of transactions used to maintain various medical data. Block chain is a transaction record that records all the changes that lead to a data lake, which is an off-chain database.

The user assigns a set of permissions and specifies who can query the data and write to the block chain. The mobile dashboard application allows users to see who has access to their block chain. Users can also view audit logs of users accessing the block chain, such as access time and access data. The same dashboard allows users to access and cancel access to any one person with a personal identifier.

**5.9 Summary**

Block chain technology is also a relatively new technology in the computing and healthcare fields. This technology has great potential in the healthcare subsector, which solves key problems with its function and characteristics. Technology can revolutionize the entire ecosystem. Sending data safely is an important challenge, and however, the possibility of shifting the code sent to the received block. Rehashing Shift Code Rail Encryption (RSCRE) is a cryptographic system belonging to the symmetric key cryptographic algorithms class, and encryption and decryption use the key. The number of hashing text is small. The cipher text assignment will be closer to the characters in adjacent plaintext, but if the number of rails is a message, the cipher text will be the same as the specified message. In the proposed method, Rehashing Shift Code Rail Encryption (RSCRE) is analyzed. The key generation is 88%, security is 93%, accuracy is 92.5%, encryption time complexity is 25sec and decryption time complexity is 23sec.

**Result and Discussion**

**6.1 Environment Setup**

The performance analyses given below shows the accuracy tested with retrieval performance, false retrieval and semantic closeness measure the proposed system produce good resultant with previous query agent base search intents. Users can count on access and permissions for thousands of files, proving the impact of rating agencies on privacy issues. The proposed Rehashing Shift Code Rail Encryption (RSCRE) method is compared to the existing Linear Elliptical Curve Digital Signature (LECDS), AuthPrivacyChain, and Merkle Hashing Tree (MHT) method.

**Table 6.1: Simulation parameters**

|  |  |
| --- | --- |
| **Parameters** | **Values** |
| Simulation Tool | Microsoft Visual studio |
| Language | C#.net |
| File size | 50-150 MB |
| Method | Rehashing Shift Code Rail Encryption (RSCRE) |
| Technology | Med chain(Block chain) |

Table 6.1 shows that the simulation parameters used in proposed algorithm and the performance results are analyzed with the existing methods.

**6.2 Performance Analysis**

Performance is measured based on some evaluation metrics like query retrieval accuracy, sensitivity, specificity-measure, time complexity and false retrieval accuracy. The testing metrics tested true positive, false positive, true negative, false negative to defined the network. The parameters are recorded underneath.

**6.2.1 Query retrieval accuracy**

Distributed query retrieval accuracy is one of the most popular metrics in distributed information evaluation. It is the proportion of the number of true positive and true negatives obtained through the knowledge learning algorithms in the total number of queries submitted.

-------------------- (6.1)

**6.2.2 Sensitivity query analysis**

Another common metric for evaluation of relational queries is the sensitivity matches to the location of retrieved queries. Sensitivity represents the true positive rate and it is calculated by the division of true positive information from location by true positive and false negative queries retrieval.

………………………….. (6.2)

**6.2.3 Specificity query analysis**

Specificity of the information retrieval is based on the location of distributed system whether the query is retrieved from that available nearest location. It is defined as the number of true negative location availability divided by all other negative locations.

…………………………..(6.3)

**6.2.4 F-measure**

F-measure is the harmonic mean of precision and recall where Precision is the proportion of the true positives against all the positive results (i.e. both true positives and false positives) and Recall is the proportion of true positives against true positive sand false negatives.

………….. (6.4)

……………………… (6.5)

F− measure (False classification) = 2∗Precision∗Recall / (Precision + Recall)…. (6.6)

**6.2.5 Time complexity**

Time complexity is identified as the overall time taken to load the query to process the information retrieval and distributed approach using the semantic relational process by in certain amount of time. The time complexity is calculated as in form of mile seconds. The actual representation of this time complexity is measured by using the system configuration under 4GB of ram with i3 Intel processor haven mat lab 2017 intent framework.

**6.3 E-Healthcare system in cloud computing using blockchain and medchain technology to protect user data**

The performance of the proposed membrane calculation is evaluated by comparing the results obtained with those using existing systems. Performance factors such as sensitivity, specificity, and accuracy were calculated and compared in the experiment. Even when the number of stored medical records and the number of submitted queries are increased, the stability of the system throughput proves that the system can process large data sets with high frequency and low latency as in EMR systems. Therefore, in addition to interoperability and effective access to EMR, it will take advantage of relational databases in terms of performance. Block chain advantages in terms of high security and privacy it obtain best performance and safety to the maximum level.

|  |  |  |  |
| --- | --- | --- | --- |
| No of data | LECDS in % | MSOA in % | DPoAC in % |
| 10 | 70 | 84 | 90 |
| 20 | 66 | 70 | 82 |
| 30 | 50 | 62 | 80 |
| 40 | 42 | 50 | 63 |

**Table 6.2 Analysis of Sensitivity**

Table 6.2 describes the sensitivity comparison noticed that DPOAC achieved the highest accuracy in both categories. To highlight the accuracy comparison, the accuracy values obtained by all methods. Comparisons show that membrane calculations achieve higher accuracy than other existing methods.

**Figure 6.1: Analysis of Sensitivity**

Figure 6.1 shows the sensitivity comparison noticed that DPOAC achieved the highest accuracy in both categories. To highlight the accuracy comparison, the accuracy values obtained by all methods. Comparisons show that membrane calculations achieve higher accuracy than other existing methods.

|  |  |  |  |
| --- | --- | --- | --- |
| No of data | LECDS in % | MSOA in % | DPoAC in % |
| 10 | 60 | 80 | 84 |
| 20 | 54 | 60 | 80 |
| 30 | 50 | 56 | 70 |
| 40 | 42 | 50 | 60 |

**Table 6.3 Analysis of Specificity**

Table 6.3 describes Even with more medical records stored and queries sent, the peculiarities of system throughput prove that the system can process large datasets with low latency and high frequency like EMR systems.

**Figure 6.2: Analysis of Specificity**

Figure 6.2 shows even with more medical records stored and queries sent, the peculiarities of system throughput prove that the system can process large datasets with low latency and high frequency like EMR systems.

|  |  |  |  |
| --- | --- | --- | --- |
| No of data | LECDS in % | MSOA in % | DPoAC in % |
| 10 | 80 | 84 | 88 |
| 20 | 76 | 80 | 82 |
| 30 | 60 | 72 | 78 |
| 40 | 50 | 62 | 66 |

**Table 6.4 Analysis of Accuracy**

Table 6.4 describes Medical institutions upload patient consumption data and store it in Medchain technology to ensure the accuracy of the uploaded data in collaboration with multi-nodes. The insurance company can know the total cost through the permission of the patient

**Figure 6.3: Analysis of Accuracy**

Figure 6.3 describes Medical institutions upload patient consumption data and store it in Medchain technology to ensure the accuracy of the uploaded data in collaboration with multi-nodes. The insurance company can know the total cost through the permission of the patient

|  |  |  |  |
| --- | --- | --- | --- |
| No of data | LECDS in % | MSOA in % | DPoAC in % |
| 10 | 28 | 20 | 18 |
| 20 | 34 | 30 | 22 |
| 30 | 48 | 33 | 30 |
| 40 | 50 | 40 | 34 |

**Table 6.5 Analysis of Time complexity**

Table 6.5 describes the time complexity is calculated experimentally and compared to other encryption methods. The encryption and decryption times obtained by the proposed algorithm it reduce the time complexity. Other existing methods obtain a little more time during the encryption-decryption process than the proposed algorithm, and it obtains a better time complexity in the encryption-decryption process.

**Figure 6.4 Analysis of Time complexity**

Figure 6.4 shows the time complexity is calculated experimentally and compared to other encryption methods. The encryption and decryption times obtained by the proposed algorithm it reduce the time complexity. Other existing methods obtain a little more time during the encryption-decryption process than the proposed algorithm, and it obtains a better time complexity in the encryption-decryption process.

**6.4 Linear Elliptical Curve Digital Signature (LECDS) With Block chain Approach for Enhance the Security on Cloud Server**

In this section aims to improve the fact that it has a significant impact on security and mental accuracy, the time complexity of user roles, and secure access to cloud environments. A tool in the Microsoft .net Framework for SQL Server databases generates test cases with appropriate user access to access private and public users throughout the configuration design process. Users can trust access and permissions to thousands of files, demonstrating the high impact of the evaluation department on privacy issues. The proposed Linear Elliptical Curve Digital Signature (LECDS) method is compared to the existing AuthPrivacyChain, MHT (Merkle Hashing Tree) method.

**Figure 6.5 Analysis of classification Error performance**

Figure 6.5 defines the analysis of classification error performance using linear regression based on LECDS algorithm. These results prove the low error rate for sensitive data analysis compared to other machine learning blockchain methods. This optimized spider search solution provides higher fitness support compared to other methods.

**Figure 6.6 comparison of security analysis**

Security analysis is the process of calculating how many attacks can be accurately detected and prevented in a manual attack. In this analysis of security result proposed method LECDS provides a 91.4% security compare to existing methods MHT has 86.1%, AuthPrivacyChain has 84.4%, security in the medical Blockchain network. Figure 6.6 represents the comparison of the proposed and existing method graphs.

**Figure 6.7 Analysis of execution time**

Figure 6.7 present the proposed LECDS method comparison of execution time analysis. The proposed Modified Spider Optimization search Algorithm (MSOA) based on LECDS utilize for a more secure process. The proposed provides execution time result is 320 MS is a low execution time for 6000 bytes compared with the existing method. The hyperledger Blockchain creates a private channel for each user and provides security for each data transaction. So the proposed method LECDS provides better performance.

**Figure 6.8 Comparison of throughput Analysis**

The proposed LECDS method of throughput analysis comparison is shown in figure 6.8. The spider optimization Search reduces the user search time and improves the throughput when several transactions are processed compared to the existing method. The proposed LECDS method of transaction performance provides a 700tps (transaction per second) for 500 transactions. Similarly, the existing method results are SDS method result is 690tps, MHT method result is 410tps, AuthPrivacyChain which provides a 650tps lower rate.

**Figure 6.9 Misclassification performance analysis**

Figure 6.9 defines the proposed linear regression-based LECDS algorithm to provide low misclassification results compared with the existing method. The proposed LECDS results provide 0.21% for 150 blocks, similarly existing method results are MHT result of 0.68%, AuthPrivacyChain result is 0.49%, and SDS misclassification result is 0.27%. The proposed algorithm provide low misclassification result compared with existing method.

**Figure 6.10 Average Latency analysis**

The analysis of average latency performance has been measured and presented in Figure 6.10 where the proposed LECDS algorithm has produced lower latency performance than other methods. In this result, the proposed LECDS method 0.6 for 2sec for the transaction. Similarly, AuthPrivacyChain provides 0.98sec, the MHT method has 1.22sec, and the SDS method has 0.7sec. In this average latency analysis result of the proposed method, LECDS provides a lower latency rate than other existing methods.

**6.5 Med chain Security Management Based Rehashing Shift Code Rail Encryption for Enhancing the Data Security**

This section aims to enhance security, which significantly impacts the user role time complexity and secure access to the cloud environment. Test cases with relevant user rights throughout the configuration design process are accessible to private and public users.

**Figure 6.11: Analysis of the Key generation**

Figure 6.11 describes the encryption performance for secure data communication, in the proposed method of Rehashing Shift Code Rail Encryption (RSCRE) is 30% Generating performance for existing methods of AuthPrivacyChain is 48%, Linear Elliptical Curve Digital Signature (LECDS)is 43%, Decision making based Proof of Authority (PoA) Consensus (DPoAC)is 38%, Merkle Hashing Tree (MHT) is 45%.

**Figure 6.12: Analysis of the security**

Figure 6.12 describes the security score is improving in the med blockchain encryption standard, in the proposed method of Rehashing Shift Code Rail Encryption (RSCRE) is 93% better performance for existing methods of AuthPrivacyChain is 69%, Linear Elliptical Curve Digital Signature (LECDS) is 80%, Decision making based Proof of Authority (PoA) Consensus (DPoAC) is 88%, Merkle Hashing Tree (MHT) is 75%.

**Figure 6.13: Analysis of False rate**

Figure 6.13 describes the False rate score is reducing in the med blockchain encryption standard, in the proposed method of Rehashing Shift Code Rail Encryption (RSCRE) is 14.2% better performance for existing methods of AuthPrivacyChain is 9.2%, Linear Elliptical Curve Digital Signature (LECDS) is 10.8%, Decision making based Proof of Authority (PoA) Consensus (DPoAC) is 11.9%, Merkle Hashing Tree (MHT) is 10.1%.

**Figure 6.14: Adaptive Memetic Search Algorithm based on time**

Figure 6.14 describes the Adaptive Memetic Search Algorithmis reducing searching time, in the proposed searchin algoritrhm of Adaptive Memetic Search Algorithmis 0.16 sec better performance for existing methods of AuthPrivacyChain is 0.38sec, Linear Elliptical Curve Digital Signature (LECDS) is 0.28sec, Decision making based Proof of Authority (PoA) Consensus (DPoAC) is 0.24sec, Merkle Hashing Tree (MHT) is 0.34sec.

**Figure 6.15: Execution of Encryption time complexity**

Figure 6.15 defines the execution of encryption time performance based on cryptography secure data communication. The proposed Rehashing Shift Code Rail Encryption (RSCRE) algorithm encryption time performance is 25 sec. Also, AuthPrivacyChain is 35se, Linear Elliptical Curve Digital Signature (LECDS) is 30sec, Decision making based Proof of Authority (PoA) Consensus (DPoAC) is 28sec, and Merkle Hashing Tree (MHT) is 33sec.

**Figure 6.16: Analysis of Decryption time complexity**

Figure 6.16 defines the execution of decryption time performance based on cryptography secure data communication. The proposed Rehashing Shift Code Rail Encryption (RSCRE) algorithm decryption time performance is 23 sec. Also, AuthPrivacyChain is 33se, Linear Elliptical Curve Digital Signature (LECDS) is 28sec, Decision-making based Proof of Authority (PoA) Consensus (DPoAC) is 26sec, Merkle Hashing Tree (MHT) is 30sec.