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

MedChain and 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.

**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.

**Provider node and patient 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.

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

**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.

**Decision making based Proof of Authority 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

**Advanced Encryption Techniques and Super peer**

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.

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

**Objective 1:**

**Linear Elliptical Curve Digital Signature (Lecds) With Blockchain Approach For Enhance The Security On Cloud Server**

To introduce a proposed security framework, namely Linear Elliptical Curve Digital Signature (LECDS) with hyperledger Blockchain, to prevent sensitive, non-sensitive information. First, to apply the Linear regression method to classify the user information categorize the data into one of the two classes. The LECDS method cluster the sensitive and non-sensitive user data in different encrypted ways. The non-sensitive data encryption using normal RSA used and sensitive data encryption using the LECC method. Modified Spider Optimization search Algorithm (MSOA) to verify the integrity of outsourced data and search user query information in a cloud server. The hyperledger fabric blockchain method verifies the user policy to create a private network to secure the cloud network. In this analysis of the proposed method, results evaluated using performance metrics such as security, throughput, classification accuracy, and error rate are compared to the existing method.

**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.

**Modified Spider Optimization search Algorithm**

The 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 spider optimization algorithms to achieve better query selection. Spider optimization performed a wide range of user searches and sent food odor information to surrounding spider 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.

**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

**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.

**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.

**Objective 2**

**Medchain Security Management Based Rehashing Shift Code Rail Encryption For Enhancing The Data Security**

To propose a Rehashing shift code Rail encryption (RSCRE) using circular shift round random padding key for decentralized medical cloud environment. To propose a Rail block-based permissioned voting protocol for voting aggregation peer requests. The privacy verifies from potential voting aggregators to authenticate the key at the peer end to enhance the security. Each part of this tree contains the hash of the neighborhood content. To optimize the node and key search method, introduce an adaptive memetic search optimization. To implement the access policy method, verify the user data access limitation in the blockchain node. The most frequently requested node/file information is achieved in the primary indexing of the hash table. The overall system provides an authenticating mechanism to prevent and authorize users by building a trustworthy network.

**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

**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.

**Rehashing Shift Code Rail Encryption (RSC)**

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 ciphertext 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.

**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

**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.

**Summary**

Cloud computing is a well-known technology as it has existed for many years. But people are still struggling to overcome some challenges of cloud computing like data security, data management, interoperability, etc. Blockchain technology is an emerging technology well known for its security and authenticity, which are the main characteristics that are making the world turn to its side. By integrating Blockchain with cloud computing, there will be many advantages in usability, trust, security, scalability, data management, and many other advantages. In this article, we brieﬂy introduced cloud computing, Blockchain technology. This chapter discussed the beneﬁts of integrating the Blockchain network with a scalable cloud environment to enhance conﬁdence, server service, data security, and user data management.