MAES-RAC: BLOCKCHAIN BASED MODIFIED ADVANCED ENCRYPTION STANDARD AND RULE-BASED ACCESS CONTROL FRAMEWORK FOR ENHANCING DATA SECURITY IN CLOUD

Sanketi Raut [1], Vishal Shinde [2], Akshay Agrawal [3], Dr. Rahul Thour[4]

[1,2,3] Ph.D. Scholars, Department of Computer Science & Engineering, Desh Bhagat University, Punjab

[4]Assistant Professor, Department of Computer Science & Engineering, Desh Bhagat University, Punjab

Abstract:

In the field of healthcare, secure transmission and access control of medical data is significant. Various systems are introduced for secure storage and access of medical data but the existing healthcare systems often rely on public cloud storage for the collection and storage of patient data. While these approaches offer convenience, they also introduce significant challenges, such as less security, higher computational load, low scalability, higher encryption and decryption time, and so on. Therefore, this research proposes a Modified Advanced Encryption Standard and Rule-based Access Control (MAES-RAC) framework to overcome the existing drawbacks and provide secure storage and access to medical data. The security level of the MAES-RAC framework is enhanced due to the incorporation of Modified Advanced Encryption Standard (MAES) algorithm, which speed up the encryption process with lower computations and offers higher security. Moreover, the Modified Rule-based Access Control (MRAC) mechanism ensure security through the integration of Bell-LaPadula (BLP) mechanism that prevent data access to unauthorized user by rejecting the unauthorized access. Additionally, the employment of blockchain technology to store medical data enhances the scalability and interoperability of MAES-RAC framework. The MAES-RAC framework's experimental results show that it achieved an encryption time of 1.44ms, decryption time of 1.23ms, memory usage of 394.6KB, genuine user rate of 0.931, and responsiveness of 4.255ms using a healthcare management system dataset, respectively.

Keywords: Medical data,cloud computing,Blockchain,Data security,Access Control mechanism.

I. INTRODUCTION

Healthcare and medical-related data are significant in patients' daily lives because they are utilized to recognize patterns, understand the medical issues of patients, and diagnose and treat diseases [1]. This enhances the patient's fulfilment through personalizing the care system and efficiently dealing with the chronic situations of patients. There is a progressive rise in both the amount and variety of medical data due to the quick growth of recent technologies and the expanding digitalization of the medical field [2]. When the necessity of dealing with the patient's medical data arises, only authorized individuals can able to access the stored medical data of the patients within the network [3] [4]. Conventionally, the stored medical data of the patients tend to be modified and stolen by unauthorized persons, thus data security is one of the key challenges in healthcare organizations [5] [6]. Accordingly, medical data are desired to be stored automatically to eradicate the complications in data storage and exchange between the healthcare providers [1]. Electronic Health Records (EHRs) are one of the most broadly utilized resources in the healthcare sector, they offer an extensive interpretation of the medical status of the patients and consist of all medical-related data and medical history of the patients [7]. Generally, EHRs are created and collaborated with doctors and nurses via the system of cloud computing, which results in a more suitable method for dealing with such medical data [8].

Recently, the storage of patients' medical-related data in the cloud has produced new issues in authentication, data access control, authorization, and controlling compliance [9]. These medical-related data include a broad range of data attributes, such as genomic data, real-time patient monitoring data, imaging data, and medical histories. These data need to be secured from cyber-attacks, unauthorized and breaches [10] and the absence of data security in the healthcare organization causes a major loss to the organization [4]. Nowadays, various types of hackers have emerged to alter the patient's data and insert dangerous malware into the hospital's computer system, which makes the data inaccessible [11] [12]. So there is an urge to develop a system to secure the entire healthcare organization. Conventional healthcare systems depend on deep learning and machine learning algorithms, which frequently face various complications in secure cloud storage, continuous data sharing among healthcare providers, and effective data transmission. The effectiveness of traditional ML approaches is limited due to the diversity of medical data and they frequently encounter the inherent complexities [13]. Likewise, DL approaches, such as recurrent neural networks and convolutional neural networks surpass at identifying the patterns in medical images and medical sensor data. Nevertheless, the deep learning approaches also exhibited computational issues mainly in the sector of secure data storage [14].

Currently, several technologies are utilized to store the patient's medical data and the choice of selecting the appropriate solution for storing data is based on numerous factors, such as complexity level, availability of resources, type of data, scalability, and privacy level [15]. The conventional access control mechanisms, such as Role-Based Access Control (RBAC) [16] and Attribute-Based Access Control (ABAC) [17] offer a foundation for handling access to the medical data within the medical organization. Even though the ABAC offers essential flexibility in intricate environments, they depend on a huge amount of attributes, which leads to an enlarged administration overhead, policy intricacy, and latency in making decisions associated with access [18] [19] [10]. Nevertheless, developing technologies, such as blockchain-based systems provide an effective solution to conquer the difficulties and transform the medical sector [14]. Blockchain based data access and storage aids the patients via reducing the cost and letting remote monitoring [20]. Without believing a third party, blockchain can attain various fascinating features and the more vital one is tamper-proof, which is attained through the mechanism of consensus and distinct data structure [21]. Furthermore, the information stored on blockchain are extremely trustable, nevertheless, they have certain drawbacks in the implementation of healthcare blockchain, latency, and scalability [6].

The notable drawbacks of the existing methods are conquered by proposing the MAES-RAC framework to securely store and access the healthcare data or medical files of the patients. The medical files of the patients are securely stored using the MAES algorithm and the key is generated from the key generation center. The Break Glass Key Access (BGKA) mechanism is utilized to generate a key break auxiliary message, which is used to extract the break glass key (BGK) to decrypt the medical files. The Emergency Access Control (EAC) mechanism is utilized for the authentication checks of the Emergency Contact Person (ECP).The other main contribution of this research is described as follows:

➢ Modified Advanced Encryption Standard and Rule-based Access Control (MAES-RAC) framework: In the MAES algorithm, a modification is introduced in the mix columns step and it is executed by reordering the fixed matrix's column through the rank value. This modification reduces the computation time and speeds up the encryption process. Moreover, the issues of computational overhead are overcome by the MAES algorithm and offer improved security. MRAC is one of the access control, which is formed through the combination of both role and attribute-based access control to check the privacy policy, also the BLP model is integrated with the MRAC mechanism, which validates the privacy policy based on the BLP properties and grant access to the data requester. This MRAC mechanism reduces the risk of intentionally or accidentally revealing healthcare data. Additionally, the incorporation of blockchain in the MAES-RAC framework for storage boosts the overall security level in storing medical files.

This research article is arranged as follows: The literature review and the challenges are covered in section II, section III covers the system model, section IV covers the overall methodology of the MAES-RAC framework, and the results and discussion part is described in section V. This research is concluded with a conclusion and future work in section VI.

II. LITERATURE SURVEY

Ali, A. et al. [14] suggested a permission-based blockchain approach to secure the system of healthcare. The suggested approach improved security and data privacy due to the utilization of standard encryption approaches and biometric authentication approaches. Additionally, the suggested approach solved the scalability drawbacks of the conventional blockchain approach. However, the suggested approach failed to deal with the huge amount of healthcare data effectively. Sangeetha, S.B. et al. [10] suggested a strong framework, which was named as Secure Healthcare Access Control System (SHACS) to improve the effectiveness and security in the environment of healthcare. The incorporation of SHACS with various healthcare administrations can enhance the user satisfaction level and alleviate the reputational and legal risks. However, it required higher computational resources to execute the suggested SHACS.

Oh, J. et al. [2] suggested a secure medical data-sharing approach to attain a balance among privacy and medical data confidentiality. The usage of Key Aggregate Encryption (KAE) in the suggested approach improved the medical data’s security by diminishing the danger of illegal disclosures and information breaches. However, it exhibited a higher computational load on every unit due to the employment of a homomorphic encryption algorithm.Kala, M.K. and Priya, M. [22] developed a Blockchain-based Decentralized Safe Sharing (BDSS) by the Shuffled Random Starvation Link Encryption (SRSLE) approach to secure the Personal Health Records (PHR). The complex cases of PHR were arranged and analyzed through the Quasi-sensitive attribute Identification approach. The suggested BDSS approach can be efficiently executed in a real-world medical environment, nevertheless, it exhibited certain drawbacks, such as scalability, higher costs of execution, and interoperability.

Ryu, J. and Kim, T. [12] developed an authentication protocol to secure the medical data within the systems of healthcare. The suggested scheme encrypted the medical-related data or records on the blockchain and they securely interchanged between the hospitals. Additionally, the suggested approach was constructed by the elliptic curve cryptography (ECC) based private-public key scheme, which made the encryption process easier to transmit the encrypted data. However, it failed to store the encrypted medical data on the blockchain. Almalawi, A. et al. [23] introduce da Lionized remora optimization-based serpent (LRO-S) encryption approach to secure healthcare data from hackers and unauthorized users. Before storing the data in the cloud, the sensitive medical data were encrypted by the LRO-S approach, also the asymmetric hash signature approach was utilized to improve the mechanism of security. The suggested LRO-S approach exhibits lower decryption and encryption time and an increased rate of confidentiality; however, the cost consumption of the LRO-S approach was higher.

Reegu, F.A. et al. [20] suggested an interoperable blockchain-based EHR (BCIF-EHR) to secure health data. The suggested BCIF-EHR framework employed wallets and cloud agents to store EHR and also blockchain was used to store automatic verifiable data and maintain public key signs. However, the drawbacks of the BCIF-EHR framework are that it can’t be applied to the actual groups contributing to the EHR scheme and it cannot be implemented effectively. Da Costa, L. et al. [8] suggested the Sec-Health approach, which is a blockchain-based procedure to secure the medical records of patients. The decentralized networks and attribute-based cryptography were employed in the Sec-Health approach to secure the storage and achieve access control, integrity, and confidentiality. However, the Sec-Health approach has high memory overhead and also it took more time to execute.

II.1 CHALLENGES

- The suggested approach in [14] eliminates the traditional issues of scalability and enhances the transaction performance, however, it failed to deal with the huge amount of healthcare data due to the computational issues.
- The suggested SHACS approach [10] strengthens the security level of the healthcare systems, however, latency and computational overhead issues arise due to the larger number of users and the increasing amount of medical data.
- The suggested LRO-S approach [23] minimizes the duration of decryption and encryption and the confidentiality rate also improved. Nevertheless, the cost consumption and execution time increase in the LRO-S approach.
- The Sec-Health approach [8], secures the data storage and accessing highly, but it exhibits issues of memory overhead and takes more time to execute the whole process.

III. SYSTEM MODEL

Figure 1 shows the system model for the MAES-RAC framework. When an emergency occurs, the patient's medical data should be accessed only by the authorized person over the network and the patient's medical data should be kept as private and secure. Still, data security is the key challenge in the medical institution. To overcome the security challenges, firstly the patients encrypt their medical data using the secure cryptographic algorithm, simultaneous auxiliary messages are generated from the BGKA mechanism and both encrypted file and auxiliary messages are securely stored in the storage. If an emergency case occurs, an emergency contact person give request to access the data and after the various authentication verification, the encrypted medical file is decrypted and given to the ECPs. Thus, the security challenges in accessing and storing the medical data are overcome.

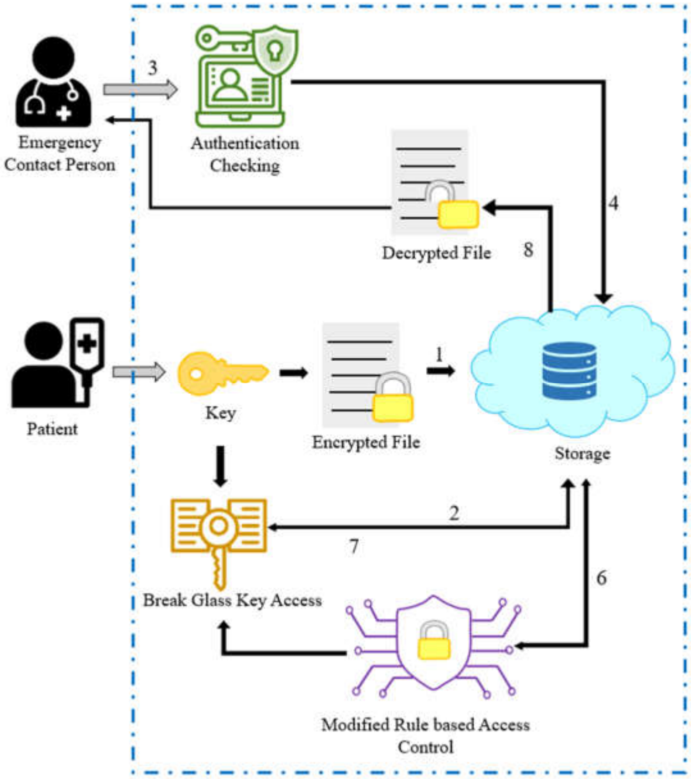

Figure 1.System Model

IV. MODIFIED ADVANCED ENCRYPTION STANDARD AND RULE-BASED ACCESS CONTROL FRAMEWORK FOR SECURE STORING AND ACCESSING OF MEDICAL DATA

The ultimate aim of this research is to securely store and access medical-related data by maintaining access control. Thus, this research proposed a MAES-RAC framework to provide secure storage and access. The MAES-RAC framework consists of various segments, such as the initialization phase, registration phase, login and assignment of ECPs phase, data storing phase, and data accessing phase. Firstly, in the registration phase, both the patients and ECPs register their details, such as identity, passwords, and biometrics in the medical institute database. After the successful registration, the patients login with the registered credentials and assign the ECPs to access their medical files, when an emergency occurs. If the invalid patient tries to login with the fake credentials, the medical institute database automatically rejects the login request. After assigning the ECPs, initially, the keys are generated in the data-storing phase through the key generation center. Simultaneously, the BGKA framework generates the break-glass key auxiliary message. Then, the MAES algorithm is utilized to encrypt the patient's medical file, and both break-glass key auxiliary messages and encrypted medical files are stored in the blockchain securely. After successful data storing, if an emergency arises, the ECPs try to access the patient's medical file by giving a request to the Emergency Access Control (ECA) mechanism. If the access is granted, further the request is given to the blockchain to access the data. Then the blockchain gives a request to the MRAC mechanism to check the privacy policy, if it is valid the MRAC mechanism gives a response to the blockchain as permission granted. Further, the blockchain gives a request to the BGKA framework with the generated auxiliary message to extract the break-glass key to decrypt the medical file. The BGKA framework verifies the auxiliary messages and gives a BGK to the blockchain. After receiving the key, the same MAES algorithm is used to decrypt the patient's medical file and given to the ECPs to review the patient's medical data. The block diagram of the MAES-RAC approach is displayed in Figure 2.

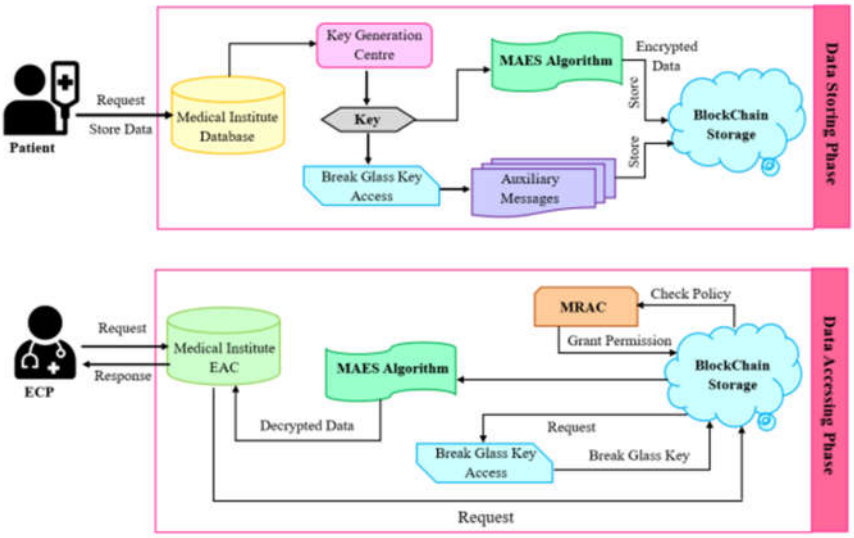

Figure 2. Overall Block Diagram for MAES-RAC Framework

IV.1 INITIALIZATION PHASE

In this system, the patient plays the role of data owner. The patient set V is mathematically denoted as,

$$V = \{v_1, v_2, \ldots v_j, \ldots v_m\} \quad (1)$$

$$v_j = \{v\_id_j, v\_pw_j, v\_bio_j\} \quad (2)$$

where, v_m indicates the total number of patients, v_j represents the j^{th} patient in the set of patients V. The v_j consists of the patient's identity, password, and biometric and they are denoted as v_id_j, v_pw_j, and v_bio_j respectively. The ECP is the doctor or the nurse, who can access the medical file of the patients when the patients are in an emergency medical situation. The ECP set F is mathematically denoted as,

$$F = \{f_1, f_2, \ldots f_j, \ldots f_n\} \quad (3)$$

$$f_j = \{f\_id_j, f\_pw_j, f\_bio_j\} \quad (4)$$

where, f_n indicates the total number of ECPs, f_j represents the j^{th} ECP in the set of ECPs F. The f_j comprises of ECPs identity, password, and biometric and they are represented as f_id_j, f_pw_j, and f_bio_j respectively. The medical data of the j^{th} patient, which needs to be stored on the cloud server, is mathematically represented as,

$$D_j = \{d_1^j, \ldots d_N^j\} \quad (5)$$

Where D_j contains a different number of medical files of the j^{th} patient, N denotes the total number of medical files.

IV.2 REGISTRATION PHASE

The Registration Phase (RP) is used to register all the details of both patients and the ECPs in the medical institute database. The RP is responsible for creating the attributes that aid for the right authorization. Initially, the patients register their details into the medical institute database by giving requests to the database with their credentials, such as identity, password, and biometrics. After the successful registration, the database sent valid acknowledgment to the patients. Likewise, the ECPs send requests to the medical institute database with their credentials, such as identity, password, and biometrics to make the registration. After registering the details, the database sent a valid acknowledgment to the ECPs as a reply. Figure 3 depicts the system of the registration phase.

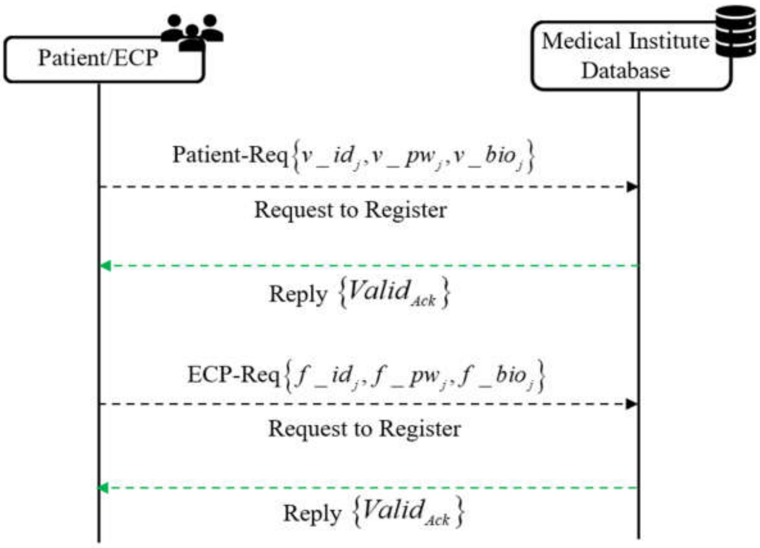
Patient/ECP
Medical Institute Database
Patient-Req$\{v_id_j, v_pw_j, v_bio_j\}$
Request to Register
Reply $\{Valid_{Ack}\}$
ECP-Req$\{f_id_j, f_pw_j, f_bio_j\}$
Request to Register
Reply $\{Valid_{Ack}\}$

Figure 3. Process of Registration Phase

IV.3 LOGIN AND ASSIGNMENT OF ECP PHASE

In this phase, the patients give login requests to the database with their credentials, such as passwords, identity, and biometrics. After receiving the login request, the database checks that the credentials are already stored in the database. If it is already stored in the database, it grants access to the further process by sending a valid acknowledgment as a reply to the patient or otherwise rejecting the login request. After the successful login, the patient assigns their ECPs by sending a request with their identity and the ECP's identity, passwords, and biometrics to the database. Then the database stores the ECP details for that particular patient and sends a confirmed acknowledgement as the reply to the patient. In case of any emergencies, the assigned ECP can only access the patient's medical data. Figure 4 depicts the workflow of Login and Assignment of ECP Phase.

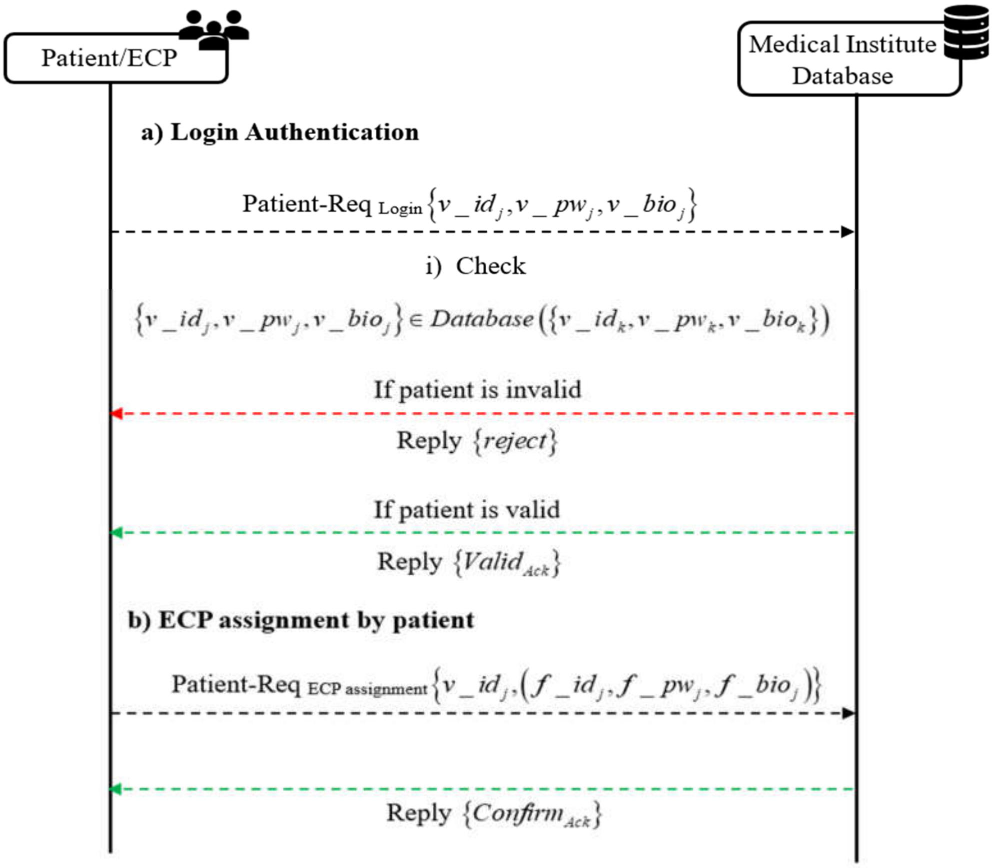
Patient/ECP
Medical Institute Database
a) Login Authentication
Patient-Req Login $\{v\_id_j, v\_pw_j, v\_bio_j\}$
i) Check
$\{v\_id_j, v\_pw_j, v\_bio_j\} \in Database(\{v\_id_k, v\_pw_k, v\_bio_k\})$
If patient is invalid
Reply $\{reject\}$
If patient is valid
Reply $\{Valid_{Ack}\}$
b) ECP assignment by patient
Patient-Req ECP assignment $\{v\_id_j, (f\_id_j, f\_pw_j, f\_bio_j)\}$
Reply $\{Confirm_{Ack}\}$

Figure 4. Login and Assignment of ECP Phase

IV.4 DATA STORING PHASE

After login and assignment of ECPs, the user gives a request to the database to store all the details. For secure storing, initially, the keys are produced from the key generation center. The patients give requests for generating to the key generation center with their identity and password. Then, the key generation center provides the key K as a reply to the patient. Simultaneously, the BGKA framework [24] generates the break-glass key auxiliary message through the attribute-based break glass key generation mechanism, which is clearly explained in the following section

IV.4.1 ATTRIBUTE-BASED BREAK GLASS KEY GENERATION MECHANISM

Let G be the prime orders bilinear group and the generator of G is represented as q . The patient's identity v_id_j, and password v_pw_j are taken as input to generate break-glass key auxiliary messages. The patients randomly choose the variables ($\eta_1,\eta_2,\mu_1,\mu_2$), which belong to the whole number set Z_o^* and λ,λ_1 belong to the generator set G . Also, the break glass key bgk_j is the same as the key K, which is generated from the key generation center. Then, $K = bgk_i = \mu$ and additionally compute,

$$\lambda_2 = K\left(q^{\mu_1+\mu_2}\right)^{\eta_1} \cdot \left(\lambda_1\right)^{-1} \tag{6}$$

$$C_{v\_id_j} = \left(q^{\mu_1+\mu_2}\right)^{\eta_2} \cdot q_1^{H\left(v\_id_j\right)} \tag{7}$$

where $C_{v\_id_j}$ indicates the patient’s cipher identity, $H\left(v\_id_j\right)$ represents the hash of the patient's identity. The break-glass key auxiliary messages are utilize to aid the ECPs retrieve the break-glass key to decrypt the patient’s encrypted medical files and they are computed as,

$$bgk_{j,1} = \left(\mu_1,\lambda_1,q^{\eta_1},q^{\eta_2},C_{v\_id_j}\right) \tag{8}$$

$$bgk_{j,2} = \left(\mu_z,\lambda_2,q^{\eta_1},q^{\eta_2},C_{v\_id_j}\right) \tag{9}$$

Finally, the generated auxiliary messages $bgk_{j,1}$ $bgk_{j,2}$, patient's medical data, and privacy policy P are encrypted using the Modified Advanced Encryption Standard (MAES) algorithm. P is a policy describing who can access d_1^j and the privacy policy contains an access privacy level, that will allow or deny the ECPs to access the medical data d_1^j. The process of encryption through MAES is clearly explained in the following section

IV.4.2 MODIFIED ADVANCED ENCRYPTION STANDARD ALGORITHM FOR ENCRYPTION

The MAES algorithm is one of the symmetric key and block cipher encryption algorithms and it overcomes the computational overhead and excessive computation issues and improves performance of throughput. In the traditional AES [25] algorithm, the mixed column step is the higher calculation operation, which slows the overall encryption process. Therefore, the modified mix columns step is introduced in the MAES algorithm to speed up the process of encryption and decryption with less computations and improved security. The number of decryption and encryption rounds to be executed is determined by the key size. The algorithm with a larger key size increases the security level of the algorithm. The one round of the MAES algorithm comprises four steps and there are 10 rounds are executed for complete encryption. The four steps used in the MAES algorithm are substitution bytes, shift rows, modified mix columns, and round keys. Figure 5 depicts the architecture of the MAES algorithm

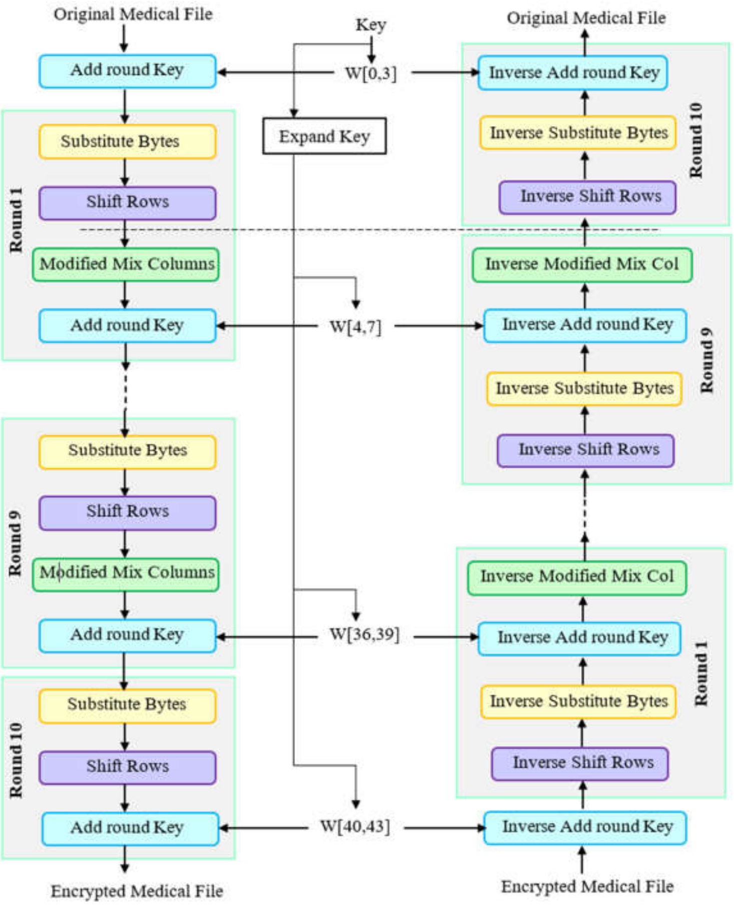

Figure 5. Structure of Modified Advanced Encryption Algorithm

IV.5 DATA ACCESSING PHASE

Once an emergency arises, the ECP gives a request to the Emergency Access Control (EAC) to access the patient's medical data with their identity, password, biometric, patient identity, and privacy policy, that is $\{f\_id_j, f\_pw_j, f\_bio_j, v\_id_j, P\}$. Then the authentication check is done to validate whether the ECP is valid or not by checking whether the requested credentials belong to the data already stored in the database. If the authentication is not valid, reject the request with the reject reply, but if it is valid the access request is continued and further the request is passed into the Blockchain. Then the blockchain gives a request to the MRAC mechanism to check the privacy policy.

IV.5.1 MODIFIED RULE-BASED ACCESS CONTROL MECHANISM

The MRAC mechanism is one of the effective algorithms to regulate who can access patient data. In this mechanism, the rule is defined by an attribute and the role. The attributes consist of the time of the request, the location of the requester (ECP), the role of the requester, and the IP address of the requester. Additionally, in the MRAC mechanism, the Bell-LaPadula (BLP) model is also incorporated to check the privacy policy. Consider, that the request contains Req Data $\{v\_id_j, ECP_{Detail}, Rule-attribute\}$, where the rule attribute consists of location, time, IP address, and the role of the requester that is a doctor or nurse. The ECP details consist of the identity, password, and biometrics of the requesters. The authorization check is the initial check of the authorization process and it is done with the details of ECPs or requesters and it is the process of checking whereas the requester has the suitable rights to access the patient's medical data, while policies are the attributes and the guidelines are utilized to determine access to the patient's medical data. The MRAC mechanism is used for the second check, which is based on the rule that is the attribute and role of the ECPs. The BLP model integrates the multilevel security through the policy of discretionary access control and also the BLP model applies both the policy of discretionary access control and multi-level security to ensure the flexibility in access control. The access permission is granted by the BLP model, if and only if the policy should have the higher level of clearance. In BLP model, a system comprises of set of users, which is represented as R, set of data is denoted as T and the set of security level is denoted as α. The relation of domination among the set α is defined by $\leq_a$.

The group of triples (L_R, L_T, L_g) is denoted by L, where L_R and L_g indicates the mapping function of users to their highest clearance level and the present clearance level. The mapping function of data to its security level is represented as L_T. The group of access control is represented by $E = \{rd, wr, ap\}$, which includes writing, appending and reading respectively. The group of present access policy is denoted by $J = R \times T \times E$ and the group of discretionary access control is represented as $N \subseteq R \times T \times E$. The BLP model is defined as quadruple model (g, a, l, p), where $g \subseteq J$ comprises the user's present access control, $a \subseteq N$ comprises the policy of present discretionary access control, security level of triple function includes $l = (l_R, l_T, l_g) \in L$ and the hierarchy of data is denoted as p. The BLP model checks the privacy policy, if they satisfy the properties of simple security policy (ss-policy), star policy and discretionary security policy (ds-policy), it grant permission to access the data.

➢ The property of ss-policy $(r, t, e) \in (R \times T \times E)$ is satisfied if the privacy policy holds one of the following rules;

- $e = ap$
- $e = rd\,(or)\; e = wr \text{ and } l_T(T) \leq_a l_g(R)$

➢ The property of star policy (*-policy) $\forall (r, t, e) \in (R \times T \times E)$ is satisfied if the privacy policy holds one of the following rules:

- $e = ap \text{ and } l_g(r) \leq_a l_T(T)$
- $e = wr \text{ and } l_g(r) = l_T(T)$
- $e = rd \text{ and } l_T(T) \leq_a l_g(R)$

➢ The property of ds-policy is satisfied, if the privacy policy holds one of the following rules:

$$(r, t, e) \in g$$
$$(r, t, e) \in a$$

The doctor has full access to privacy that is he can read, write, and edit the medical files. However, the nurse has a partial access policy that is he can only read the medical files.
Table 1 describes the working of MRAC.

If all the rules are validated, permission is granted to access the patient's medical files or otherwise access is denied. After granting permission to access, the blockchain gives a request with the identity of the patient and the BGK auxiliary messages to the BGKA mechanism for getting the key to decrypt the medical data. The key is extracted using the attribute-based break glass key extraction mechanism, which is clearly explained in the following section.

Table 1. Working of MRAC mechanism

```
Modified Rule-based Access Control Mechanism
Modified_Rule_based_Access (Rule)
{
   Check (Request. Location ∈ Medical Institute.Location ∩
   Request.time ∈ Range (Role.time)
   ∩ Request. IP_address ∈ Medical Institute.IP_address ∩ Check Access
   Privacy (Request. Role))
}
Check Access Privacy (Request. Role)
{
If (Request. Role==Nurse)
    If (Request. Access policy ≤ Role.Accesspolicy) ^ (Valid_Doctor-Ack)
Validate (Bell-LaPadula_Model);
    Else
       Return Reject "No"
Else
    Validate (Bell-LaPadula_Model);
Return Grantpermission "Yes"
}
```

IV.5.2 ATTRIBUTE-BASED BREAK GLASS KEY EXTRACTION MECHANISM

If the patient faces an emergency medical condition, the attribute-based break glass key mechanism uses the patient's identity and breaks glass key auxiliary messages to extract the key for decrypting the medical files. Initially, choose the random number, s which belongs to Z_o^* and compute α, then choose the random integer b_1, b_2 which belongs to Z_o^* and compute Q_1, Q_2. These calculations are represented in the following equations.

$$\alpha = q^s \cdot q_1^{H(v\_id_i)} \tag{14}$$

$$Q_1 = \left(q^{\eta_2}\right)^{b_1} \tag{15}$$

$$Q_2 = \left(q^{\eta_2}\right)^{b_2} \tag{16}$$

Then compute the value of X_1, X_2 and B_1, B_2, where $B_1 = q^{b_1}$, and $B_2 = q^{b_2}$. These values are computed using the following equations.

$$X_1 = \lambda_1\left(C_{v\_idi_j} \cdot \alpha^{-1}\right)^{b_1} \cdot \left(q^{\eta_1} \cdot Q_1 \cdot Q_2\right)^{-\mu_1} \tag{17}$$

$$X_2 = \lambda_2\left(C_{v\_idi_j} \cdot \alpha^{-1}\right)^{b_2} \cdot \left(q^{\eta_2} \cdot Q_1 \cdot Q_2\right)^{-\mu_2} \tag{18}$$

Finally, the BGK is generated using the following equation

$$K = (X_1 \cdot X_2) \times (B_1 \cdot B_2)^s \quad (19)$$

After generating the BGK, the BGKA mechanism sends the key as a reply to the blockchain to decrypt the patient's medical file. Then the decryption is done through the MAES algorithm to decrypt the medical file. The decryption process is the same as the encryption process, which is clearly explained in section 3.4.2 but the decryption process is an inverse of the encryption process. The decryption using the MAES algorithm is mathematically represented as

$$d_l^i = MAES\_Dec(K, c^j) \quad (20)$$

After decrypting, the patient's medical data is forwarded to the ECPs, who need to access the patient's medical data to review the condition of the patient. The utilization of various authentication mechanisms and effective encryption processes makes the patient's medical data secure and it can't able to access by an unauthorized person. Figure 6 depicts the workflow of data data-accessing phase.

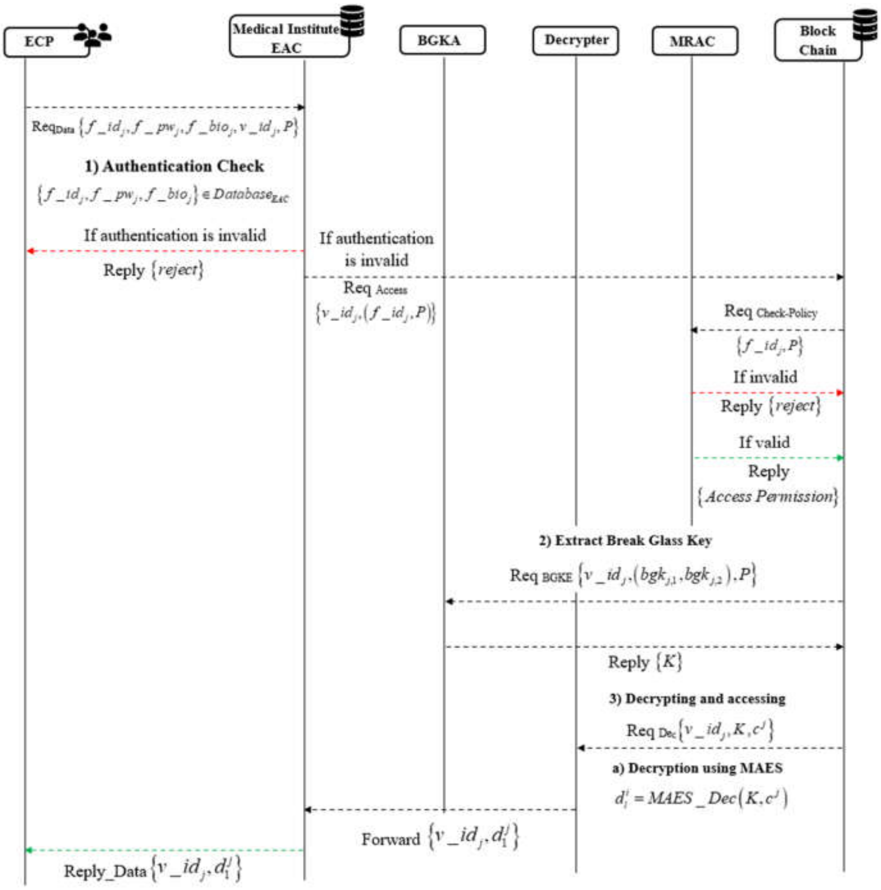
ECP
Medical Institute EAC
BGKA
Decrypter
MRAC
Block Chain
Req$_{Data}$ $\{f\_id_j, f\_pw_j, f\_bio_j, v\_id_j, P\}$
1) Authentication Check
$\{f\_id_j, f\_pw_j, f\_bio_j\} \in Database_{EAC}$
If authentication is invalid
Reply $\{reject\}$
If authentication is invalid
Req $_{Access}$ $\{v\_id_j, (f\_id_j, P)\}$
Req $_{Check\text{-}Policy}$ $\{f\_id_j, P\}$
If invalid
Reply $\{reject\}$
If valid
Reply $\{Access\ Permission\}$
2) Extract Break Glass Key
Req $_{BGKE}$ $\{v\_id_j, (bgk_{j,1}, bgk_{j,2}), P\}$
Reply $\{K\}$
3) Decrypting and accessing
Req $_{Dec}$ $\{v\_id_j, K, c^j\}$
a) Decryption using MAES
$d_l^i = MAES\_Dec(K, c^j)$
Forward $\{v\_id_j, d_1^j\}$
Reply_Data $\{v\_id_j, d_1^j\}$

Figure 6. Data Storing Phase

V. RESULTS AND DISCUSSION

This section describes the efficiency of the MAES-RAC framework, by comparing it with the existing approaches.

V.1 EXPERIMENTAL SETUP

The MAES-RAC framework is executed on the latest version of PyCharm with Windows 11 OS and RAM of 16GB, ROM of more than 100GB, and a CPU with a speed of 1.7 GHz.

V.2 DATASET DESCRIPTION

The Healthcare dataset [26] and the Healthcare Management System dataset [27] are utilized in this research. The Healthcare dataset comprises 10,000 records and all records represent an artificial patient medical record. It consists of numerous parameters, such as basic information about the patient, admission details of the patient, and the patient's medical conditions. The Healthcare Management System dataset includes various tables, such as patients table, doctors table, appointments table, medical procedure table, billing table, and demo table. Each table stores data about the patients, and healthcare providers, including their contact details and name.

V. 3 EVALUATION METRICS

The evaluation metrics, such as decryption time, genuine user rate, encryption time, memory usage, and responsiveness matrices are utilized to estimate the efficiency of the proposed MAES-RAC framework

Encryption Time: The encryption time measure is utilized to estimate the total period taken through the proposed MAES-RAC framework to convert the original data to the encoded data, which is mathematically represented as,

$$Enc_T = \frac{Enc_{Data}}{T} \tag{21}$$

where Enc_T represents the encryption time, Enc_{Data} indicates the encrypted data, and T denotes the time.

Decryption Time: The decryption measure is utilized to estimate the total period taken by the proposed MAES-RAC framework to convert the encoded data into the original data, which is mathematically represented as,

$$Dec_T = \frac{Dec_{Data}}{T} \tag{22}$$

where Dec_{Data} indicates the encrypted data, Dec_T represents the encryption time, and T denotes the time.

Genuine User Rate: It is the proportion of the total amount of valid users to the total number of users and it is mathematically represented as,

$$gur = \frac{t_{Valid}}{t_{users}} \tag{23}$$

where, t_{users} represents the total number of users, and t_{Valid} is the total number of valid users.

Memory Usage: It is the measure used to estimate the total volume of memory utilized by the system for implementing both the process of decryption and the encryption respectively.

Responsiveness: A responsiveness measure is used to estimate the speed of the framework to process the request.

V.4 PERFORMANCE ANALYSIS

The performance of the MAES-RAC framework using both the Healthcare and Healthcare Management System datasets in terms of genuine user rates with varying key sizes, such as 128, 192, and 256.The genuine user rate is evaluated for varying numbers of users as 50, 100, 150, 200, and 250 with different key sizes. For the Healthcare dataset, the MAES-RAC framework achieved a rate of 0.9352 for the key size 128, 0.9358 for the key size 192, and 0.948 for the key size 256of the 250 users. For the Healthcare Management System dataset, the MAES-RAC framework achieved the rate of 0.913 for the key size 128, 0.921 for the key size 192, and 0.931

for the key size 256 of the 250 users. It shows that the genuine user rate upsurges with the increasing volume of users as well as key size respectively.

V.5 COMPARATIVE DISCUSSION

This section describes the comparison discussion over the proposed MAES-RAC framework and the existing SHACS, ECC, LRO-S, and KAE approaches. The compared existing approaches revealed the significant advantages in storing and accessing medical files, but still due to the presence of certain limitations in the existing approaches they can't perform well in securing the patient's medical files. The suggested SHACS approach can't be executed over the huge distributed system of healthcare due to its low computing resources. Due to the utilization of the homomorphic encryption algorithm in the suggested KAE approach, the computational load occurred on every unit. In the suggested ECC approach, medical data leakage happens, due to the usage of a manual system to encrypt and store the medical files. The security level is decreased in the suggested LRO-S, due to the absence of integration of blockchain technology in the LRO-S approach.

The proposed MAES-RAC framework overcomes the limitations of the compared existing approaches by integrating the MAES algorithm to encrypt the medical files securely and the computational load of the existing approach is conquered by the MAES algorithm. Additionally, the mixing of blockchain in the MAES-RAC framework enhances the overall security of the MAES-RAC approach in storing the patient's medical data. Moreover, the MAES-RAC approach can execute on the huge distributed system of healthcare, due to the existence of the MRAC mechanism and high computing resources in the MAES-RAC approach. These advantages make the MAES-RAC framework more secure in terms of storing and accessing the patient's medical files.

The outcomes achieved by the MAES-RAC framework and existing approaches using both datasets are shown in Table 2

Table 2. Comparative Discussion of MAES-RAC Framework

Methods/Metrics		SHACS	ECC	LRO-S	KAE	MAES-RAC
Health care Dataset	Encryption Time (ms)	3.742	3.582	2.777	1.930	1.229
	Decryption Time (ms)	2.755	2.412	2.315	1.825	1.454
	Genuine User Rate	0.759	0.833	0.852	0.904	0.948
	Memory (KB)	496.7	496.3	491.6	489.8	487.8
	Responsiveness (ms)	3.244	3.971	4.129	4.278	4.394
Health care Management System Database	Encryption Time (ms)	3.830	3.729	3.389	2.836	1.446
	Decryption Time (ms)	2.520	2.255	2.190	1.915	1.235
	Genuine User Rate	0.695	0.750	0.766	0.906	0.931
	Memory (KB)	407.6	405.7	402.4	396.8	394.6
	Responsiveness (ms)	3.026	3.425	3.786	4.058	4.255

VI. CONCLUSION

In this research, the MAES-RAC framework is proposed to provide secure storage and access to medical data, which enhances patient privacy, protects against unauthorized access, and improves the overall integrity of healthcare data. The utilization of the MAES algorithm minimizes the computation and speeds up the process of both encryption and decryption. Moreover, the utilization of the MRAC mechanism with the BLP model and EAC mechanism checks the policy and authentication and restricts unauthorized access to the patient's medical file. Additionally, the employment of blockchain technology to store medical data enhances the scalability and interoperability of the MAES-RAC framework. Overall, the MAES-RAC framework effectively secures sensitive healthcare data and ensures that only authorized persons or ECPs can access the patient's medical file. The MAES-RAC framework is evaluated using the measures, such as decryption time, genuine user rate, encryption time, responsiveness, and memory usage and they achieved the values of1.23ms, 0.931, 1.44ms, 4.255ms, and 394.6KB using healthcare management system dataset and obtained the values as 1.45ms, 1.22ms, 0.948, 4.39ms and 487.8KBfor healthcare dataset, respectively. The future direction of research would include optimization driven framework for secure key generation mechanism in order to store and access the data at faster and secure rate.

REFERENCES

[1] R.G. Sonkamble, A.M. Bongale, S. Phansalkar, A. Sharma, and S. Rajput, “Secure data transmission of electronic health records using blockchain technology,” Electronics, vol. 12, no.4, pp.1015, 2023.

[2] J.Oh, S.Son, D.Kwon, M. Kim, Y. Park, and Y.Park, “Design of secure and privacy-preserving data sharing scheme based on key aggregation and private set intersection in medical information system,” Mathematics, vol. 12, no.11, pp.1717, 2024.

[3] S.M. Pournaghi, M. Bayat, and Y. Farjami, “MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption,” Journal of Ambient Intelligence and Humanized Computing, vol.11, no.11, pp.4613-4641, 2020.

[4] R. Kumar, and R. Tripathi, “Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell–LaPadula model,” Journal of Ambient Intelligence and Humanized Computing, vol.12, pp.2321-2338. 2021.

[5] N. Raghav, and A.Bhola, “Blockchain based privacy preservation in healthcare: a recent trends and challenges”, Psychol. Educ. J, vol. 58, pp.5315-5324, 2021.

[6] B. Shen, J. Guo, and Y. Yang, “MedChain: Efficient healthcare data sharing via blockchain,” Applied sciences, vol.9, no.6, p.1207, 2019.

[7] C.S. Kruse, A. Stein, H. Thomas, and H. Kaur, “The use of electronic health records to support population health: a systematic review of the literature”, Journal of medical systems, vol.42, no.11, p.214, 2018.

[8] L. Da Costa, B. Pinheiro, W. Cordeiro, R. Araújo, and A. Abelém, “Sec-Health: A blockchain-based protocol for securing health records,” IEEE Access, vol.11, pp.16605-16620, 2023.

[9] B.Y. Kasula, "Framework development for artificial intelligence integration in healthcare: optimizing patient care and operational efficiency", Transactions on Latest Trends in IoT, vol.6, no.6, pp.77-83. 2023.

[10] S.B. Sangeetha, C. Selvarathi, S.K. Mathivanan, J. Cho, and S.V. Easwaramoorthy, "Secure Healthcare Access Control System (SHACS) for Anomaly Detection and Enhanced Security in Cloud-Based Healthcare Application," IEEE Access, vol. 12, pp. 164543-164559, 2024.

[11] J. Ryu, D. Kang, H. Lee, H. Kim, and D. Won, "A secure and lightweight three-factor-based authentication scheme for smart healthcare systems", Sensors, vol.20, no.24, p.7136, 2020.

[12] J. Ryu, and T. Kim, "Enhancing Hospital Data Security: A Blockchain-Based Protocol for Secure Information Sharing and Recovery," Electronics, vol.14, no.3, p.580, 2025.

[13] Q. An, S. Rahman, J. Zhou, and J.J. Kang, "A comprehensive review on machine learning in healthcare industry: classification, restrictions, opportunities and challenges", Sensors, vol.23, no.9, pp.4178, 2023

[14] A. Ali, H. Ali, A. Saeed, A. Ahmed Khan, T.T. Tin, M. Assam, Y.Y. Ghadi, and H.G. Mohamed, "Blockchain-powered healthcare systems: enhancing scalability and security with hybrid deep learning," Sensors, vol. 23, no.18, pp.7740, 2023.

[15] O. Siedlecka-Lamch, "Secure Medical Data Storage with Blockchain Technology", Procedia Computer Science, vol.225, pp.961-968, 2023.

[16] L. Zhou, V. Varadharajan, and M. Hitchens, "Trust enhanced cryptographic role-based access control for secure cloud data storage", IEEE Transactions on Information Forensics and Security, vol.10, no.11, pp.2381-2395, 2015.

[17] S. Bhatt, T.K. Pham, M. Gupta, J. Benson, J. Park, and R. Sandhu, "Attribute-based access control for AWS internet of things and secure industries of the future", IEEE Access, vol.9, pp.107200-107223, 2021.

[18] C. Anitha, C.R. Komala, C.V. Vivekanand, S.D. Lalitha, and S. Boopathi, Artificial "Intelligence driven security model for Internet of Medical Things (IoMT)", In 2023 3rd International Conference on Innovative Practices in Technology and Management (ICIPTM). 1-7. IEEE, 2023.

[19] D.S. Gupta, N. Mazumdar, A. Nag, and J.P. Singh, "Secure data authentication and access control protocol for industrial healthcare system", Journal of Ambient Intelligence and Humanized Computing, vol.14, no.5, pp.4853-4864, 2023.

[20] F.A. Reegu, H. Abas, Y. Gulzar, Q.Xin, A.A. Alwan, A. Jabbari, R.G. Sonkamble, and R.A. Dziyauddin, "Blockchain-based framework for interoperable electronic health records for an improved healthcare system," Sustainability, vol.15, no.8, p.6337. 2023.

[21] W.J. Gordon, and C. Catalini, "Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability", Computational and structural biotechnology journal, vol.16, pp.224-230, 2018.

[22] M.K. Kala, and M. Priya, “Smart IoT-Blockchain Security to secure Sensitive Personal Medical Data using Shuffled Random Starvation Link Encryption,” IEEE Access, vol. 12, pp. 168182-168196, 2024.

[23] A. Almalawi, A.I. Khan, F. Alsolami, Y.B. Abushark, and A.S.Alfakeeh, “Managing security of healthcare data for a modern healthcare system,” Sensors, vol.23, no.7, p.3612, 2023.

[24] M.T. De Oliveira, A. Michalas, A.E. Groot, H.A. Marquering, and S.D. Olabarriaga, “Red Alert: break-glass protocol to access encrypted medical records in the cloud”, In 2019 IEEE International Conference on E-health Networking, Application & Services (HealthCom),1-7, 2019.

[25] A.M. Abdullah, “Advanced encryption standard (AES) algorithm to encrypt and decrypt data”, Cryptography and Network Security, vol.16, no.1, pp.11, 2017.

[26] Healthcare dataset, https://www.kaggle.com/datasets/prasad22/healthcare-dataset, Accessed on March 2025.

[27] Healthcare Management System Dataset, https://www.kaggle.com/datasets/anouskaabhisikta/healthcare-management-system?select=Patient.csv, accessed on March 2025.