Advanced Cryptography & Block Chain Based Cloud Environment for Secured E-Health Record

Sonya A (sonya.yasmin55@gmail.com)
B. S. Abdur Rahman Crescent Institute of Science and Technology

Kavitha G
B. S. Abdur Rahman Crescent Institute of Science and Technology

Research

Keywords: Electronic Health Records (EHRs), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Attribute Based Encryption (ABE), Blockchain, Cloud Environment.

DOI: https://doi.org/10.21203/rs.3.rs-633622/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Advanced Cryptography & Block chain Based Cloud Environment for Secured E-Health Record

Sonya A, Kavitha G

Department of Information Technology, B. S. Abdur Rahman Crescent Institute of Science and Technology, India

Corresponding Author Email: sonya.yasmin55@gmail.com

Abstract - There has been noteworthy issues that must be tackled by the healthcare sector along with handling the security concerns that are intensely linked with offering of healthcare services, inculcating novel electronic healthcare systems, and secure data communication with different healthcare and government institutions. These security related concerns project several privacy preserving methodologies pertaining to the privacy and security of EHRs (electronic health records) in the cloud. The EHRs comprises of information related to demographics, medical histories, digital images, medications, lab reports, billing details and other sensitive patient information. All this sensitive patient information is kept highly secured and resides in third party servers with definite access controlling mechanism. The conventional system employs various cryptography algorithm for authorization, encryption, decryption, key generation and validation algorithms. There is proposal of a new cryptography algorithm for combating the limitations of AES, RSA and ABS. For securing the healthcare data residing in the cloud, the research presents effective utilization of new hybrid cryptography algorithm and Blockchain technology with smart contract. Unlike the prevailing three cryptographic algorithms, the proposed algorithm offers enhanced time, accuracy, efficiency and key generation and
performance. Overall, there is a drastic transformation in securing the healthcare records using the proposed approach.

**Keywords:** Electronic Health Records (EHRs), Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Attribute Based Encryption (ABE), Blockchain, Cloud Environment.

1. **INTRODUCTION**

Cloud computing has completely reformed and uplifted the face of technology, with its massive usage in health care sector. Not only has it aided in sound storage of medical information but also its communication between various associates. For effective management of such voluminous information, the cloud network must be highly developed so as to make both the storage and accessing of information feasible online. The medical industry has witnessed a huge transformation from management of paper-based records to electronic records. With such a significant changeover, there is effective rise in both competence and adaptability along with transmission of medical information amidst various associates. The conversion of paper-based records into digitalized electronic records is in terms of EMR (Electronic Medical Records), EHR (Electronic Health Records), PHR (Personal Health Records), and EHD (Electronic Health Data). EHR and EMR includes patient’s medical information that is being handles by medical expertise.

According to [1] the healthcare sector is emphasizing and challenging towards offering sophisticated and at per services since there is intense need of quality treatment and wellbeing of health by every other individual. Health issues have become a prime concern for every person
and so is the issues related to it. Resultant, there must be state-of-the-art technique and services that offers both benefit and comfort.

[2-3] Information security refers to providing the information access just to the authentic clients whereas organization security refers to access and movement of information amidst two authorized clients via organization. To certain extent, Distributed computing makes use of Internet and since the information resides in the cloud, there is possibility of breach in information and organization security. This user-friendly model tests on a portable Android application and distributed computing provided by AWS (Amazon Web Services). It’s visible from the evaluation output that the above technique fits for various e-wellbeing situations. The benefit of this model is that it offers high adaptability, low operational cost and EHRs accessibility to the health administrators. Though there prevails the concerning issue regarding both information and organization security for e-wellbeing frameworks. Sharing of EHRs in a systematic and orderly manner with the potential partners by maintaining high-security levels tends to be quiet challenging task. Today, the Healthcare industry is intensely transforming towards being information-centric. [4] points out that enforcing security measures helps in protecting or safeguarding the sensitive information and framework assets. Security of framework assets emphasizes actually on the Cloud computing equipment and programming whereas information security caters to secure information exchange within the Cloud computing. Among the various merits of Distributed computing, some are: asset sharing, adaptability, cost and energy investment funds and quick arrangement. [5] specifies that based on the clinical information the specialists carry out the patient’s treatment rather than on the information which must actually be provided directly by the patient. Herein, the Blockchain becomes helpful by allowing making acute agreements, thereby making it adaptable in various domains. The same
has been inculcated in the e-wellbeing sector. One of the hurdles in the prevailing e-wellbeing is that, when a patient’s inspection is performed in any of the emergency clinics, the data remains unshared between them. The recommended framework enforces the entire medical staff as well as patients to handle the storage of information in a trustworthy manner, abide by all. It’s also essential that the medical administrators couldn’t misuse or alter the clinical information of their patients for any illegitimate purchase or activity. [6] discusses that the private blockchain deals with handling the PHI (personal health information) and the consortium blockchain supervises or monitors the protected files of the PHI. For ensuring information security, access control, protection and secure hunt, the PHI (personal health information), watchwords along with the patients' personality undergoes public key encoding with watchword search. It’s important that the watchword size must neither be large enough for controlling the productivity of the exchange nor less enough in accordance with the framework accessibility. [7] Discusses that acceptance of conventional cryptographic natives aiming towards information trustworthiness is difficult since it does not ensure any security pertaining to any conflict amidst the cloud worker and clinical organization. There can be no alterations in the EHRs once the comparing exchange gets recorded in the blockchain. This allows any member to verify their respectability by going through the comparing exchange. It’s clear from the security analysis and performance evaluation that the recommended framework ensures a robust security and yields high efficiency. The present research enhances security measure and computation execution via encoding. The research consolidates blockchains with encryption algorithm for upgrading the competence of correspondence offices and organisation’s information flow. The research work has been divided into following sections: Section 2 covers up the related work, Section 3 presents the proposed
structure. The output generated along with brief discussions is highlighted in section 4 with the conclusion and future work put forth in section 5.

2. RELATED WORKS

The popularity of cloud computing is growing ceaselessly and so its usage amidst various sectors and businesses. By putting away their data on cloud, the users avail the merit of low storage costs, space availability and Scalability. Moreover, there is no hassle of maintaining the storage infrastructure, upgrading the software or any routine servicing. Though the cloud computing technology still confronts the hurdle of security and privacy concerns. Shortage of storage space and centralized data remains the thought-provoking concern of many organizations, hence building a cloud space that ensures secure and trustworthy data sharing based upon cryptographic framework remains the need of the hour as indicated by [8].

Hajny at el., [9] put forth that by performing the encryption of critical information, standard security level can be fulfilled. The encryption process helps in anticipating and guarding against unauthorized personnel that are in attempt of breaching the security to fetch the desired information. Using the above-mentioned technique in the frameworks, the two trustworthy correspondence hubs can share a typical secret key (that must be pre-conveyed) to carry out the information symmetric encryption (AES, XTEA, IDEA ..). Encryption that is irregular such as RSA leads to scrambling of information by open keys and unscramble the distribution in frameworks. So, essentially the cryptographic systems must fulfill such magnified prerequisites, simultaneously showing its competence on compelled gadgets too.

[10] Suggests the use of ABS technique for replacing the original signature in the blockchain as it offers the benefit of fine-grained access control. Since the cloud space can be
prone to leaking user data or insecure user privacy, a privacy-preserving and user-controlled data sharing architecture has been recommended along with fine-grained access control that relies upon the blockchain model and attribute-based cryptosystem.

Shi, Set al. [11] proposes a blockchain-put together App design with respect to PC referred to a HDG (Healthcare Data Gateway). The proposed reason driven admittance control model is divided into crude information (medical services administration) and measurable information (clinical exploration) based upon access purposes. Any sort of exchange is carried out using different sharing techniques that fulfill multiple objectives. Resultant, it’s possible for the patients to oversee and go through their shared medical care information smoothly. Some frameworks employ smart contract that involves predefined access strategies based on requestors’ purposes and based-job/based-reason benefits. Attending such spontaneous or dynamic occasions can be inflexible and can apparently lead to security threats.

A crossover answer has been proposed by Manoj et al., [12] for sharing EHRs in a crossover cloud climate, taking in accord the security and protection parameters. For achieving fine grained admittance control for EHRs, the two ABE (Attribute Based Encryption) strategies have been consolidated for encoding the EHR record of each patient. Be it remarkable merits and administrations, security of accessing the clinical information or the overall security remains an arduous aspect for the administration providers. The Advanced Encryption Standards (AES) technique has though proven to be robust enough in safeguarding the critical information with revealing competence in insurance. Albeit, committing security assurance and preparation time has been its demerit.

[13] Tremendous development of computational mists has pulled in and empowered concentrated calculation on asset compelled customer gadgets. There has been development of
hi-ended mobiles for data transaction and for applications that are computational dominated by making use of request administration model of remote server farms. Apparently, there must be upgrading of the traditional AES (Advanced encryption standard) technique so as to prevent any unexpected security threats in the cloud environment. The research provides overview of system along with upgraded security and proprietor's information privacy. Albeit, authenticating users and classified information to remote personnel needs to cater to emerging concerns associated with security and safeguarding of information.

[14] Proposes a technique that enables the users to verify data integrity of their information residing in the cloud thus resolving this concerning issue. With this mechanism the user can fetch the desired data without worrying about the source or origin of the data as well as monitor if any sort of encroachment has taken place against the data integrity. Data Provenance is one such concept that looks after this issue. Usually, the user is not granted any physical access to their data stored in Clouds is physically not accessible to the users. Rather the user’s data is transferred to remote storage locations, unknown to the user.

[15] Discusses that lately the E-health system has marvellously reformed technically as well as in delivering the medical service. All the medical information pertaining to a patient is well stored by this system which is being further effectively utilized by the medical practitioners. The present research elaborates certain identity associated cryptographic techniques such as new IBE schemes, new identity-based proxy re-encryption schemes.

According to Bhabendu et al., [16] the Blockchain technique has been widely adopted as it offers the advantage of peer-to-peer transaction, immutable properties and is decentralized. The present work covers up the implementation of this technique in various domains along with the problems confronted in doing so.
For sharing and storing the data in cloud space, Jasper et al.[17] has proposed two techniques namely, ECC (Elliptic Curve Cryptography) for encryption of medical data and the CAS (Certificate less Aggregate Signature) scheme for generating digital signature. If the critical health information of a patient suffers from confidentiality and integrity issues, it can severely hamper the patient’s health. To prevent this, Cloud-based eHealth systems are built that helps in handling the EHRs effectively and securely thus benefitting both the patients and medical firm.

[18] Has presented a blockchain-assisted eHealth framework that safeguards outsourced EHRs that comply with the identified condition. In addition, there is description of certain concerning challenges and further research on blockchain-assisted secure EHRs in cloud-based eHealth systems. EHRs tends to be highly sensitive in nature and of paramount importance to the adversaries. It’s but obvious that the outsourced EHRs can experience security risks that may be intrinsic or extrinsic.

By highlighting the demerits of conventional medical management system, Haiping et al., [19] emphasises on the construction of effective cloud-assisted e-health system. Towards this, there is proposal of BCES (blockchain-based e-Health system) that gives the assurance of examining any alteration or fiddling with the EHRs. Both the security and privacy issues in data storage are of grave significance. Not only its challenging to commit the EHRs integrity while data outsourcing but it’s also arduous to commit the EHRs privacy and traceability at the time of data sharing.

[20] Has put forth that the technique of blockchain has without doubt proven its worth in the medical sector by offering decentralization, security, confidentiality and privacy. It mainly focuses towards imbibing the blockchain technology for EHR and offering secure storage of
electronic records through a set of granular access rules for the users. Moreover, there is a
discussion of the scalability issue experienced by the blockchain through the means of off-chain
record storage. Above all, the prime concerns for the Electronic Health Record (EHR) systems
are of data integrity, security, and management.

The survey performed by Kuo et al., [21] elaborated implementation of blockchain in the
area of biomedical and healthcare. It was deduced that the technique of blockchains greatly aided
in decentralization, durability of medical records, data pedigree, ceaseless data accessibility and
access of secure information by the biomedical or healthcare personnel. Any sort of damage or
alteration to the HRE may result in erroneous treatment or diagnosis. As such there are bleak
security measures followed by the Healthcare systems for maintaining the EHRs.

Hussein et al., [22] recommends a cryptography-based key generation algorithm which
aids in authenticating the genuine user. By employing a genetic algorithm and discrete wavelet
transform, problem of scalability and optimality is generated. [23] Presents a framework
pertaining to automatic network configuration and organization that relies upon distributed and
temper-proof properties of blockchain. Data collection process works towards gathering network
data, then pre-processing it and finally producing the processed data. Albeit, the diversified
collection of mobile network operators cause the major data hindrance amidst the operators thus
limiting the usage of overall capability. [24] Believes that the health care data forms the
backbone of the healthcare system and the more the healthcare data is shared, the more robust,
functional and effective the healthcare system would become. Blockchain exhibits fruitful
performance in the financial sector by delivering trustworthy, auditable computing by the means
of a decentralized peer network with the support of a public ledger. The research recommends an
app referred to as HGD (Healthcare Data Gateway) architecture that employs blockchain
technique for allowing the patient to securely handle and share their own data easily in a protected manner thus giving an innovative platform for the enhancement of healthcare systems in a safeguarded manner. Though the healthcare data systems are struggling hard enough to offer high security and protection towards collection, storing, and analysis of personal healthcare data being in at par with the privacy terms.

Yin et al. [25] has proposed a cloud-based patient centric system that comprises of three layers which are 1.) Data collection layer, 2.) Data management layer and 3.) Data service layer. A prototype referred to as ‘MedRec’ has been recommended by Ekblaw et al. [26] that makes the Blockchain as the core component for identifying and working upon the security measures concerning the so called EHT (electronic health records). Using the fail proof technique of blockchain, achieving essential factors such as integrity, authenticity, auditability and data sharing was the prime purpose. The cryptographic function stands as the foundation of this technique which enables data encryption.

[27] have recommended a secure EHR (electronic health record) system for encouraging fine-grained access control and for ensuring that the medical data remains confidential, authenticated and integrated. The proposed system relies upon attribute-based cryptosystem and blockchain technology. Encryption of medical data is performed by the means of IBE (identity-based encryption), and IBS (identity-based signatures) help in implementing digital signatures. To collectively employ the functionality of both IBE and IBS in one cryptosystem, a new cryptographic primitive namely, IB-ES (identity-based encryption and signature) has been inculcated. Resultant, the system’s management is geared up without the hassle of involving different cryptographic systems that caters to different security needs. EHR data residing on the cloud is very much prone to varying security risks. [28] Asserts that there is need of self-
improving and highly adaptable programming techniques that gets further enhanced with
significant tools and are capable of performing high-end tasks as well as overcome any sort of
programming setback or usage of screen asset in real time for desired rebalancing. Amidst
various set of applications, certain recommended techniques are, DES (Data Encryption
Standard) and the AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman).
Since the client’s information may confront security breach or misuse of information, it’s
trending now that the cloud specialist provide worker side security for controlling and managing
the client’s information. Hence there is pre-requisite of customer side encryption system that can
safeguard and secure the client’s information irrespective of who is controlling the overall cloud
storage. Usually, the information residing within the cloud is present in scrambled form and is
decoded once it reaches the client’s end. Such an encryption process aids in safeguarding the
cloud information against hacking and malicious attacks.

3. PROPOSED WORK

The present research aims to secure the E-healthcare records using the recommended Blockchain
technique. The following algorithms of key generation, authorization, encryption, decryption,
and validation are employed along with the cryptography algorithms namely, AES, RSA and
ABS. There is proposal of a novel hybrid cryptography algorithm with blockchain to protect
healthcare data hosted within the cloud. Every transaction is stored on records or blocks that are
linked via cryptography in order to build a Blockchain. The proposed system works by accepting
the user fed data as input. The user fetch their unique ID from the Message Service Provider and
enrol it too. The user’s input then undergoes encryption and is converted to a cryptographical
form. AES (Advance Encryption Standard), RSA (Rivest-Shamir-Adleman) and ABE (Attribute
Based Encryption) are recommended hybrid algorithms for encryption that ensures improvised security. The above algorithms are capable of carrying various encryption processes by maintaining limited data input size, accuracy, comprehensibility as well as efficient memory usage. Thereafter, the encrypted data is transferred to the blockchain block which then undergoes two processes namely, Smart contract and Blockchain. The data is stored in blocks and chained via Blockchains. After the block gets completely filled with data, it is chained to the previous block thus chaining the entire data together. In the smart contract process, an agreement is done amidst people which allows exchange of either shares, money or property transparently without any conflicts and involvement of a third person. The peers caters to privacy notion within the block. The **endorsing peers** works towards preparation of transaction proposal and simulating transactions. The **Committing peers are responsible for handling the** full ledger of records in their ledger. Whereas the **Ordering peers which being a** special type of nodes, accepts endorsed transaction. Subsequently, the overall transaction data is securely updated on cloud space.
Figure 1: Overall Proposed Architecture

Fig1 presents the medical data residing within a public cloud with healthcare providers. The EHRs comprises of patient’s personal information along with their medical records. Every patient has a unique patient ID. The electronic health records can be fetched by referring the patient’s address base. It’s recommended that just the patients addresses resides on the blockchain through hybrid algorithm and the huge medical records are stored by the decentralized cloud storage.

For generating a digital signature, private key is employed by the Signature generation algorithm whereas a public key is employed by the signature authentication uses that is unlike private key but do resembles it. Every signatory holds a pair of private and public key. From the visibility point of view, public keys are openly known but the private keys are strictly confidential. The private key blocks the user record and if the user wants to carry out any operations, the user must generate new block identifier and a new signature. Though the identifiers of the remaining blocks remain unaffected. It’s essential that the user’s partial private key is also stored during the sign operation process. The proof generation helps in verifying the total count of blocks in shared data, compute random values and thereafter the details are sent to the Blockchain by the verifier. Every block’s possession is then computed followed by computing the signature for each block and sending an auditing proof to the verifier. The public verifier holds every user’s public keys. ProofGen aids in checking the integrity of shared data. Both the ProofGen and public key helps in data decryption, which is then eventually transmitted, to the data owner. Unlike the three prevailing cryptographic algorithms, the proposed system yields significant performance in terms of Authentication, Confidentiality and Validation performance.
**Authentication**: This process involves generation of important user credentials (user and password) to build a single credential. The message service provider provides the identifier.

**Validation**: by maintaining a controlled climate, the validation has been performed and the data on which the validation need to be performed is provided by the cardiology experts from an emergency clinic. Most importantly, there was no recognizable patient’s information in the collected data such as his/her names, last names, telephone numbers, messages etc…, and was uniquely examined.

**Confidentiality**: based on the patient’s willingness to offer information access permissions, their data was gathered from the doctors.

**Implementation**: The entire e-health system is implemented using the object-oriented programming language ‘Java’, Java Net bean software is employed to build smart contracts for the Blockchain technique with cloud and Mysql is used as the backend tool. The implemented hybrid algorithm ensures secure patient focused information so as to significantly benefit in cooperation and synchronized working in an eHealth system, at the same time maintaining security while collecting and exchanging patient’s information using the eHealthbased devices. The recommended system blends cryptographical aspects in order to deliver protected and efficient framework for good storage, exchange and access of EHR (electronic health records) within the cloud space. Unlike the three prevailing cryptographic algorithms, the proposed system yields significant Authentication, encryption and decryption time, efficient memory space usage, Execution Time and Key Generation. The mentioned parameters are cited in (section 4) Result and Discussion with table and its corresponded graphs through the following formulations.

*Memory Space*
TS = CS – AS i.e, Total memory space (TS) = Consumed memory space (CS) – Amount of free space (AS).

**Execution time**

Execution Speed (SP) = Instruction* cycle per instruction* Time.

**Key Generation Time**

KG (Key Generation time) = Number of keys * Number of organization involved in the process.

**Encryption Time/ Decryption Time**

Encryption Time/Decryption Time = Number of attributes * number of groups.

**Buffer time**

Buffer time = additional time added to a service length that you use to clean up after the arrangement, or get ready for the following arrangement.

**Accuracy**

Accuracy or the preciseness refers to the ratio of the number of predictions that are accurate to the total number of input samples.

**Accuracy**

No. of Correct Estimating/ Total no. of Estimating.

**Recall**

It is the number of accurate positive outcomes, broken down by the number of all related samples (all samples that should have been identified as positive)

Recall = True outcomes/ True outcome + False Neural

**Security**

Security = policy + procedure + management + Technology.
**Mean Absolute Error**

The average difference between the original values and the expected values is the mean absolute error. This provides us with a measure of how far the projections are from the actual production. They don't, however, give us any indication of the error's course, i.e. whether we are predicting the data or predicting the data over. It is represented, mathematically, as:

$$\text{Mean Absolute Error} = \frac{1}{n} \sum_{i=1}^{n} |Y_a - Y_b|$$

### 3.1 Problem Definition

It's observed that employing the means of commercial systems by the patient’s for storing their health-related data invites various security threats. The ABE (Attribute Based Encryption) technique and other traditional access control systems suffers major shortcomings when dealing with access policy and data security maintenance. Ideally, there must be a central server for the storage of overall data that is locked by the access control system. Moreover, as and when the data is sent to the requestor, there should be no control of the owner over the data. The prevailing system doesn’t fulfill the concept of data outsourcing, wherein the data access is prohibited for the third party that stores the data. Nor does there are trustworthy access control policies for implementation. Encryption and computation of the healthcare record tends to be extremely time engulfing, similar to the challenging task of integer factorization of patients database. One such challenge was the RSA (Rivest-Shamir-Adleman) Factoring Challenge pertaining to computational numbers of medical data, involving infeasible factoring of large integers (database) that would result in slowing the execution of output. Unlike others, the technique of AES (Advanced Encryption Standard) works uniquely in encrypting and decrypting the Healthcare sensitive data, though its implementation is not across all the worldwide hardware and software. Maintaining the confidentiality and patient privacy policy amidst access to
significantly huge amount of data tends to be arduous. Though there may prevail voluminous data that is extremely important for the use of all the medical experts, it must be highly secure and protected.

3.2 Blockchain Technology
Blockchain technology application has been encouraged in certain major sectors including the health care industry. The benefit of Blockchain is that it provides secure and relevant information without any need of central person or an administrator. Blockchain make use of a distributed, shared organization for the continuous generation of requested records termed as ‘squares’ so that a computerized record is formed. The organization of its own permits the exchange, of the cryptographically marked square. It’s noteworthy that the Blockchain technique offers applauding performance in terms of authorization and straightforwardness of healthcare information and thus securing the EHR (Electronic Health Records) for uninterrupted case handling.

3.2.1 Expanded Capacity
This being, the prime most element of the Blockchain. The astounding technique of blockchain works efficiently in expanding the capacity to handle the overall health organization. Towards achieving this, there is involvement of innumerable computers that works in an integrated manner in offering exceptional power and support.

3.2.2 Better Security
From the security point of view, the Blockchain provides unmatched security to an extent that there remain utterly bleak chances of the e-health framework getting shutdown. Unlike the other critical frameworks that have possible chances to get hacked, the assurance of blockchain
network is vouched by numerous computers called hubs which work towards sustaining any sort of exchange within this network.

### 3.2.3 Permanence

The blockchain emphasizes towards assessment of Permanent record maintenance. Information that is voluminous and intense is highly prone to hacking and other security threats, hence there must be trustworthy outsource medium that can guarantee information security. Bitcoin is such a Blockchain that maintains the records in any situation.

### 3.2.4 Quicker Settlement

Frameworks that are customary financial ones are adequate enough and involve immense settlement time, consuming many days. This reason is realistic enough for such financial organizations to seek renovation of their frameworks.

### 3.2.5 Decentralized System

The concept of Decentralization implies that all the information and resources are stored in an organization that can be accessed through various means of the web portal. Also a resource is almost equivalent to a report or an agreement and the proprietor has full rights on his record through the means of a key that is associated to his own record and this enables the proprietor to willingly and freely move the resources for whosoever he desires.

### 3.3 Smart Contracts

A smart contract refers to a self-working computer program that is subsequently executed upon fulfilling the explicit criteria. There is a keen contract in the Ethereum blockchain, which resembles an uncommon record, comprising of information, and code that holds many programmable abilities. This Clients are able to interact with keen agreements by the means of Ethereum record and using the application binary interfaces. Capacities that are listed in smart
contract can be initiated through another exchange that the record sends. In the proposed healthcare system, there can be consistent use of the smart contracts thus preventing and removing any incompetency in it. If the patient is willing to make use of smart contracts for buying insurance, then the entire agreement and policy is kept secured in the patient’s profile itself. Subsequently, this information is stored on the blockchain, which ensures of a much-secured ledger and being robust against any sort of vulnerability of threat. The Smart Contract concept provides a framework for varying types of non-financial blockchain-based applications. The prime attributes of Blockchain such as the security, decentralization, invariable review trail, information provenance makes it worth so. Implementation of blockchain in inventory applications is importantly because of the reason that the blockchain information remains static or invariable. Making use of appropriated record innovation based on blockchain yields in the merits of delivering items to conveyance, ensuring quality control, providing an integral and trustable cycle. Overall, a Smart Contract is a self-executed or self-workable program dedicated towards security of the two clients and intakes the amount of desired data.

3.4 Use scenarios

3.4.1 A client understands his/her Healthcare record from a Provider:
A client needs to understand his/her record from a Provider information base. He/she makes an inquiry solicitation to get to the record. This inquiry, along with a return esteem that is either the mentioned information or an entrance denied message, will be a log that is hashed and added to the Record relationship contract.

3.4.2 A HealthcareProvider peruses records from another Provider:
A Provider B needs to peruse a client's record from Provider an information base. B makes an inquiry solicitation to Provider. This question, along with a return esteem that is either the
mentioned information or an entrance denied message, will be a log that is hashed and added to the Record relationship contract.

3.4.3 A Healthcare Provider alters records:

A provider needs to peruse or alter a client's record from its own information base. The provider makes an inquiry to the record.

3.5 HYBRID ALGORITHM:

In this paper, it is been described about the potential use of new hybrid cryptography algorithm to protect healthcare data hosted within the cloud. The encryption improvisation we proposed that hybrid algorithm which provides,

- First-key-policy ABE
- Chinese Remainder Theorem (CRT)
- AES 256

3.5.1 First-key-policy ABE:

The KP-ABE (first key-policy attribute-based encryption) plan comprises of non-monotonic access structures with fixed cipher text size. In order to achieve this, there is depiction of a particular class of character-based transmission encryption resulting in monotonic KPABE frameworks in the specific set model. In this framework, the cipher text size is directly generated using the assigned volume of cipher text and the solitary kind of special cases so as to withhold restricted kind of edge access methods. Here, yet another productive personality-based repudiation system is depicted which on integrating with certain launch of monotonic development, exponentially rises the significant KP-ABE acknowledgment by keeping static cipher text size. There is proposal of a advance version of a key-policy attribute-based encryption technique that enables imbibing of patient’s or organizational access control policies
in a manner which is accessible by everyone but its decryption is possible only by the authenticated users belonging to the patient’s family, friends, or fellow patients or the legitimate skilled users like the doctors or nurses.

Algorithm 1: First-key-policy ABE

Input: Message

Output: Fixed Size

Step1: The setup algorithm sets a security parameter and an index value attribute. It produces those public parameters and the hidden key (SK). The Authority of Trusted Attributes (AA) publishes and retains a hidden key Parameter of security $\lambda \in \mathbb{N}$ and binding parameter $n \in \mathbb{N}$.

Step2: As input, the key generation takes the public parameters, the master secret key and an access structure allocated to the user by the AA. It outputs an SK decryption key associated with the structure of the access.

Step3: The algorithm for encryption takes the public parameters, a set of attributes and a message as input. It outputs text from the cipher. It requires $r \leftarrow KZ * p$ and calculates $skID = (n_1, n_2, n_3) = g^\alpha \cdot f_1(ID) \cdot r, gr, f_2(ID) \cdot r \in G_n$.

Step4: The decryption algorithm takes the public parameters, the cipher text $ct$ that has been encrypted under the attribute collection, and the decryption, SK for the access structure, as its input. The message is output: it parses $skID = (n_1, n_2, n_3)$ and $C = (Ct0, Ct1, Ct2)$ and then runs $D(n_1, n_2, n_3), ID, (Ct1, Ct2), S) \rightarrow e(g, g) \alpha$.

Advantages of First-key-policy ABE

1. Secure and fine-grained data sharing and access control.
2. At par performance and reliability is delivered.
3. Users are able to decrypt private keys access structures that control cipher texts.
4. Overall robust security is ensured with restrictive attribute employed in private key.

3.5.2 Chinese Remainder Theorem (CRT):

The Chinese remainder theorem (CRT) helps in providing a special answer for synchronous straight congruences with coprime moduli. In its basic form, the Chinese remainder theorem determines a number ‘n’ which if divided using certain given divisors, gives the remnants. The application of the CRT is in the area of cryptography and secret sharing is one such significant topic. This theorem tends to be a secret sharing scheme with no alterations involved. Let $m_1, m_2, \ldots, m_r$ be $r$ pairwise relatively prime positive integers. Implementation of the CRT theorem is widely witnessed in various sectors like computing, and coding. Essentially, it must be ensured that the key generation is strong enough and if not, the RSA will be prone to vulnerability and security threats. Hence, it’s crucial that two large random prime numbers are chosen for computing the modulus $n$.

Algorithm 2: Chinese Remainder Theorem (CRT)

**Input:** Message

**Output:** Fixed Size

---

**Step 1:** Finding the $M$ is assigning values to variables $a$. Suppose $m_1, m_2, m_r$ are relatively prime positive integer int pairs, and let $f_1, f_2, \ldots$ be integer fr.

**Step 2:** Find $m_1, m_2, m_3$ using function $M = num_1 \times num_2 \times num_3$.

**Step 3:** Load the Secret Key Value, to create a scheme to evaluate the secret $S$ for any $k$ shares.

**Step 4:** $M$ inverse locate, $m_1' m_2' m_3'$.

$M_1 = m_1 \text{ MOD } num_1,$

$M_2 = m_2 \text{ MOD } num_2,$

$M_3 = m_3 \text{ MOD } num_3.$
Step 5: Using function \( X = M_1 \times M_2 \times M_3 \), take the module.

Step 6: Calculate \( Y = [(m_1' \times m_1 \times f_1) + (m_2' \times m_2 \times f_2) + (m_3' \times m_3 \times f_3) \mod X] \).

**Advantage of Chinese Remainder Theorem**

1. Improve the computation speed.

2. Provide different libraries for performing computation on large numbers.

### 3.5.3 AES 256

The Encryption technique has completely transformed and elevated the concern pertaining to the security of critical information and thus it is massively adopted. In this process plain content or data is taken as input which is converted into figure text that comprises a set of random characters. This information can only be decoded by those having the special secret key. AES makes use of symmetric key encryption wherein just a single secret key is employed for data encoding and translation. AES 256 resembles a symmetric key code for both encryption and decoding whereas the sender and receiver of the information is provided with the duplicate key. Unlike AES 256, the awry key frameworks employs an alternate key for performing the encryption and decryption. Alternate keys works ideal for external record moves whereas symmetric keys are ideal for internal encryption.

**Algorithm 3: AES 256**

**Input:** Message

**Output:** Fixed Size

**Step1:** Initialize with the block data the state array (plaintext).

**Step2:** Inside the block there are substitute key, shift rows, mix columns.

**Step3:** substitute key
i) Each byte is replaced by row-indexed double byte (left 4 each byte is replaced by row-indexed double byte (left 4-bits) & bits) & column (right 4 column (right 4-bits) of 16x16 table bits).

**Step4: Rows Shift**

i) 1st row unchanged row unchanged, 2nd row 1 byte circular shift to left row 1 byte circular shift to left, 3rd row 2 byte circular shift to left 3rd row 2 byte circular shift to left, 4th row 3 byte circular shift to left 4th row 3 byte circular shift to left.

**Step5: Columns Mix**

i) Prime polynomial prime polynomial multiplication of the matrix \( m(x) = x^8 + x^4 + x^3 + x + 1 \).

**Step6: Add the initial round key to the round key (AddRoundKey).** The designed main length is 256-bit, which is 14 rounds, representing the number of rounds to be carried out.

**Step7: Do decryption, in reverse, the same procedure is performed.**

**Advantage of AES-256:**

1. AES algorithm effectively combats hacking.

2. AES tends to be extensively imbibed open source technology across the world.

3. Data hacking becomes impossible.

**3.6 HYBRID BASED ENCRYPTION ALGORITHM PROCESSING:**

In this Hybrid algorithm, the combination of all three algorithm processes that solves the same problem. Our hybrid algorithm solves the security problem and protect sensitive dataDataset which achieves Accuracy, Comprehensibility, Data input size, Memory utilization as proposed below processes. In our proposed algorithm various steps to achieve the encryption for security.
The first step is key generation, is the way toward producing keys in cryptography. A key is utilized to encrypt (private key) and decrypt (public key) whatever information is being encrypt/decrypt shown in Figure 3 separately. Here the database encrypted using private key to make it as cipher text ten it will decrypt with public key.

The user generates signature using the private and public key. That is, the private key helps in encrypting the data as well as the user’s signature. Then there is verification of the encrypted signature and by using the public key the signature is decrypted as illustrated in Figure 4.
Figure 4: Process of Sign Generation

After completion of Sign generation, need to generate the proof to the user. In this proof generation provider sends the proof to the verifier for verification of the proof shown in Figure 5.

Figure 5: Process of Proof Generation
By utilizing the private key, user’s message is split into message block. For carrying out any sort of operations such as insert, update or delete, the user is required to compute new block identifier. User’s partial private key must be stored during the process of sign operation. After signature verification. The message blocks are shared and there is verification of number of blocks in shared data by the proof generation, which is being depicted in Figure 5, 6. Eventually, the encrypted data is transmitted to the data owner.

Algorithm 4: Hybrid Algorithm

Input: Message

Output: Fixed Size

Step1: mixture of attributes that are collected in a format for encrypting medical information.

Step2: Key Generation:

i) User picks his private key for encrypting the user medical record ski.

ii) User picks his public key for decrypting the user record pk i.

Step3: Sign Generation:

i) The user selects his private ski key.

ii) The user selects his pki public key.

iii) Block of Messages mj = (mj, 1, mj, k).

iv) Block calculation mjisσj = (σj, 1…Σj,d).

Step4: Modify insert

i) User records are blocked using a private key.

(ii) If any insertion operations are to be performed by the user, the new block identifier m'j is computed.
Iii) New signature computed by this user. The identifiers of these blocks are not updated for the remainder of the blocks.

iv) The user's partial private key should also be stored at the time of operation of the sign.

(v) The number of blocks increased to n+1 in the shared data.

**Step 5: Update to Modify**

i) The user uses his private key to enter the message block.

(ii) If any insertion operations are to be performed by the user, the new block identifier m'j is computed.

iii) New signature computed by this user. The identifiers of these blocks are not updated for the remainder of the blocks.

iv) The user's partial private key should also be stored at the time of operation of the sign.

v) The no. of blocks in shared.

(vi) The number of blocks in the shared data remains n.

**Step 6: TheProofGen**

i) Check the number of blocks in the shared data.

ii) Create $y_j \in \mathbb{Z}_p$, for $j \in J$, random values.

(iii) Verifiers apply the information to the Block Chain.

iv) Calculate each block's ownership.

V) Measure each block's signature.

Vi) Aggregate the signatures produced.

Vii) Returns evidence of audit to the verifier.

**Step 7: Decryption to validate proof**

i) The public verifier initially has public keys for each user.
ii) Verify, using ProofGen, the credibility of shared data.

iii) ProofGen and pki compare.

iv) Forward the result to the owner of the data.

### 3.7 Blockchain-Based eHealth System

Blockchain-Based eHealth System (BCES) is further renovated based on customary cloud assisted electronic wellbeing frameworks. The blockchain is employed for uploading operational data into the cloud space from the source of information generation. There are seven elements involved in this framework namely: 1) patients; 2) clinics; 3) key worker; 4) research establishments; 5) cloud specialist co-op (CSP); 6) Blockchain which being depicted in Fig 7. Following describes their individual properties:

1. **Patients:** they are the actual proprietors of EHRs (electronic health records) who provides first hand medical info and can also handle it remotely.

2. **Hospitals:** these are chosen by the patients for assessing the EHRs and uploading it to the cloud.

3. **Key Server:** they are responsible for generating keys and conveying them to various relevant entities.

4. **Research Institutions:** Research organizations are central repository for information wherein the clients sends inquiry requests to the cloud worker and also provide their own incoming as and when needed.

5. **Cloud Service Provider:** CSP act as an intermediary that enables putting away and sharing the EHRs.

6. **Blockchain:** The BCT (blockchain chain Technology) forms the backbone of the entire framework and work towards recording every level of EHRs in the squares in a safe and secure manner. Information residing in the blockchain is preserved as evidence. After checking and
verifying for authorization, the element's duty can be examined using the evidence or information residing in the blockchain.

![Blockchain-Based eHealth System Diagram]

**Figure 7: Blockchain-Based eHealth System**

The Blockchain based e-health system resembles the EPR (Electronic Patient Record) which is designated for recoding the patient’s health data and is effectively adopted by majority of health care providers. This particular framework stores files in data sets and provides an interface for enrolling, browsing and revealing data from these e-health files. Moreover, these information bases can be openly accessed by various entities fulfilling the desired authorization. Apparently, the above-mentioned Blockchain based e-health framework is equivalent to the EHR (electronic health record) frameworks, which is being adopted by diverse health workers. Though the entire framework is seemingly yet to be implemented. The patient’s health records are stored in different health providers’ information bases. Maintenance of a patient’s record using the secure blockchain technique is depicted in Fig 7. The hospital helps in uploading the patient information in form of an EHR using the Blockchain.
3.8 Storage Process of Hybrid based Encrypted database

Our proposed framework encrypts the stored data until transmitting it to unlike the centralized models, the data owner with customer involvement in key generation credentials; whereas there is no role for Customers' presence exists. Without ensuring the correctness and trustworthiness of the data within the cloud, privacy is incomplete. In making transactions open and confidential for data owners, blockchain technology plays a crucial role to generate a digital signature. It does not have this attribute due to limitations by the traditional cloud storage providers relating to the foundations of decentralization. Our approach applies a hybrid blockchain-based algorithm which encrypts data until outsourcing everything to a cloud of third parties utilizing improved FKP-ABE, CRT and AES 256. The patient’s medical database will be taken as an input and the data will be preprocessed. After that the database will be passed into proposed hybrid algorithm, here the database will be encrypted with the private key and it is forwarded to the blockchain. The Blockchain network efficiency is usually calculated as the average time it takes to validate and store a transaction in each peer node so that it cannot be reversed or revoked and finally the database stored in Cloud Database securely.
The main aim of this hybrid algorithm is achieved high security to data for upload and download from cloud. Hybrid algorithm solves the security, confidentiality and authentication issues of cloud.

4. RESULT AND DISCUSSION

Out of various technologies, there are many which are incapable of protecting and safeguarding against vulnerabilities since they are not equipped with robust and foolproof security system. Keeping in mind the present scenario, there are certain significant systems that have been highlighted which though performs well but are still unable to come up to the expectations of fulfilling the security, integrity and confidentiality of e-health data. There is recommendation of a technique that performs well by merging cryptographical aspects thus ensuring a protected framework that helps in accessibility, storing and transferring of EHRs (electronic health
records) in the cloud space. The performance analysis of cryptography algorithms is presented in Table 1.

Table 1: Comparative Analysis of different algorithm

| Techniques                                             | Accuracy | Recall | Mean Absolute Error |
|--------------------------------------------------------|----------|--------|---------------------|
| Hybrid based Encryption algorithm (HBEA)               | 0.98     | 0.67   | 0.53                |
| Attribute based Encryption algorithm (ABEA)            | 0.82     | 0.95   | 0.93                |
| RSA (Rivest–Shamir–Adleman) algorithm                  | 0.89     | 0.84   | 0.81                |
| Advance Encryption Standard Algorithm (AESA)           | 0.92     | 0.72   | 0.62                |

The analysis of different algorithm shows the performances of cryptographic Algorithms, in which the existing algorithms have low inaccuracy and high in error level. Our proposed hybrid algorithm achieves high in accuracy and low in error and recall depicted below figure 9.

![Figure 9: Performance Analysis for different Algorithm](image)

E-health information compromises of diverse information that is both confidential and critical and can range from liberal to monetary information including federal retirement aide number.
The CSPs (cloud service providers) as well as various administrations proposes for a collection of efficient safety measures so as to uplift the confidence and trust of patients and organizations.

Table 2. Memory Space Consumption

| S. no | Algorithm                  | Memory Used (bytes) |
|-------|----------------------------|---------------------|
| 1     | AES                        | 10.7                |
| 2     | ABE                        | 18.6                |
| 3     | RSA                        | 14.7                |
| 4     | Proposed Hybrid Algorithm(PHA) | 8.8                |

Table 2 and Fig. 10 depict the usage of memory space in an encryption cycle by the recommended work. The measure of extra room required for execution of the computation with an information measure of information is referred to as the encryption extra room. According to this, the proposed systems engulf low storage space unlike the other prevailing techniques.

Figure 10: Performance of Memory Space Consumption

Lesser the memory or space utilization, least will be the capacity cost involved in the cloud. For every potential model, cloud computing comes as a boon. These parameters make memory expense of encryption negligible in contrast to the entire encryption of information.

Table 3: Execution Speed Analysis
Execution speed in the proposed framework hinges around the encryption and decryption of total number of records. Instead of scrambling the entire lot of attributes, only a certain set of properties can undergo encoding and decoding.

![Figure 11: Performance Analysis of Execution Speed](image)

By performing this act, the execution time reduces, unlike in the case when the entire set of attributes need to be encrypted and decrypted. This execution speed has been shown in Table 3.
Table 4. Analysis of Key generation time

| Keys Number | ABE (ms) | AES (ms) | RSA (ms) | Hybrid Algorithm (ms) |
|-------------|---------|---------|---------|----------------------|
| 1           | 3.9     | 1.2     | 0.99    | 0.05                 |
| 2           | 4.98    | 1.79    | 1.25    | 0.35                 |
| 3           | 5.99    | 2.83    | 2.27    | 1.29                 |
| 4           | 6.87    | 5.87    | 3.2     | 2.2                  |

The key age depicts usage of total number of keys which is compared with the prevailing framework and it’s concluded that the proposed framework comparatively less memories. Table 4 depicts the key generation time for the proposed framework and this measure is determined only once.

Figure 12: Performance of Key Generation Time
Time consumed by the proposed Hybrid framework is quite low unlike the remaining techniques for various quantities of key generation. The quantity of key generation is dependent on the quantity of associations associated with a process.

**Table 5. Comparative Analysis**

| S. no | Algorithm                              | Size | Encrypt Time (sec) | Decrypt time (sec) | Buffer Time |
|-------|----------------------------------------|------|--------------------|--------------------|-------------|
| 1     | Hybrid Encryption Algorithm            | 153  | 3.7                | 3.1                | 145         |
| 2     | Attribute based Encryption algorithm   | 153  | 7.4                | 5.1                | 152         |
| 3     | Rivest–Shamir–Adleman algorithm        | 153  | 6.6                | 7.2                | 162         |
| 4     | Advance Encryption Standard Algorithm  | 153  | 5.7                | 8.5                | 177         |

Table-5 helps in assessing that the time consumed by AES, ABE and RSA for performing encoding and decoding exceeds the time that is consumed by the Hybrid algorithm. Apparently, there is variation in buffer size and doesn’t increase in terms of file size in all the algorithms. Figure 13 helps in analyzing the buffer size utilization by AES, ABE and RSA algorithm which being more compared to the buffer size usage by Hybrid algorithm which is very less for all the document sizes.
Figure 13: Comparative Analysis of Algorithms

The experimental output helps in deducing the clear-cut fact that the Hybrid algorithm in performing encryption and decryption time along with the buffer usage utilizes the least time when the comparison is made with the other algorithms. It’s clearly elucidated that rest of the algorithm engulfs high encryption time and buffer usage. Moreover, decryption process of hybrid algorithm is enhanced than all.

Figure 14: Security Comparison
The hybrid encryption achieves the security and secrecy. The Figure 14 shows the security execution correlation. The proposed hybrid algorithm provides higher security level than existing algorithms.

Table 6: Blockchain Survey

| S. No | Parameters   | Percentage |
|-------|--------------|------------|
| 1     | Security     | 30.88      |
| 2     | Accuracy     | 20.6       |
| 3     | Memory Used  | 10.7       |
| 4     | Execute      | 3.45       |
| 5     | Others       | 0.98       |

Table 6 shows percentage of parameters that used in blockchain; it achieves high security on healthcare environment. Blockchain technology used to secure networks and devices from attacks. In addition, blockchain protection implies that the network data going through it is no longer governed by the authority.

Figure 15: Performance percentage of Blockchain
Blockchain technologies provide advantages, such as high security and accuracy, time for execution, more faith in systems, and much more shown in fig 15. The system proposed is a combination of three algorithms of cryptography, i.e. a combination of FKP-ABE, CRT, AES-256, Hybrid cryptography algorithm creation and idea. The design of the algorithm here is used to provide better security for the data and performance.

5. CONCLUSION

Executing and maintaining e-Health system stands utterly crucial in any region for the upliftment of trustworthy and efficient health care services. For encouraging and inspiring the health care workers or providers, building and providing at par security and privacy which can guard against any vulnerability and security breach is of paramount importance. Thus, for implementing and improvising the security parameters in the e-Health domain, certain highly significant models have been recommended which ensures of successfully achieving the desired benchmark. Apart from this, the proposed work highlights prime area of research with classified angles design, encryption techniques, and access control elements. In addition there is exploration of certain attentive concerns along with future research aims for building noteworthy methodologies ensuring uncompromised security in smart health arrangements. In all, fulfillment and implementation of such an overall security framework can intensely safeguard the highly important health care sector.

ABBREVIATIONS

EHR – Electronic Health Records
AES - Advanced Encryption Standard
RSA - Rivest-Shamir-Adleman
AFBE - Attribute Based Encryption
BC - Block chain
EMR - Electronic Medical Records
PHR - Personal Health Records and
EHD - Electronic Health Data
AWS - Amazon Web Services
PHI - Personal Health Information
HDG - Healthcare Data Gateway
ECC - Elliptic Curve Cryptography
CAS - Certificate less Aggregate Signature
IBE – Identity Based Encryption
BCES – Block Chain-based E-Health System
IBS – Identity Based Signatures
CSP - Cloud service providers
DES - Data Encryption Standard
TS - Total memory space
CS - Consumed memory space
AS - Amount of free space
KG - Key Generation time
CRT - Chinese Remainder Theorem
KP-ABE - First Key Policy Attribute Based Encryption
SK - Hidden Key
AA - The Authority of Trusted Attributes
HBEA - Hybrid based Encryption Algorithm
BCES – Blockchain-Based eHealth System
BCT - Blockchain chain Technology
EPR - Electronic Patient Record

**Funding**
Not applicable.

**Availability of data and materials**
All data generated or analysed in this study are included in this published article.
Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

REFERENCES:

[1] Aceto G, Persico V and Pescapé A (2020), "Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0", Journal of Industrial Information Integration, 18, p.100129, Elsevier.

[2] Suciu, George, Victor Suciu, Alexandru Marian, Razvan Craciunescu, Alexandru Vulpe, Ioana Marcu, Simona Halunga, and Octavian Fratcu (2015), "Big data, internet of things and cloud convergence—an architecture for secure e-health applications", Journal of medical systems, Vol. 39, No. 11, pp. 1-8, Springer.

[3] Nguyen D.C, Pathirana P.N, Ding M and Seneviratne A (2019), "Blockchain for secure ehrs sharing of mobile cloud based e-health systems", IEEE access, 7, pp.66792-66806.

[4] Al-Issa Y, Ottom M. A&TamrawiA (2019), "eHealth cloud security challenges: a survey", Journal of healthcare engineering, 2019.

[5] Casado-Vara, R. and Corchado, J (2019), "Distributed e-health wide-world accounting ledger via blockchain", Journal of Intelligent & Fuzzy Systems, 36(3), pp.2381-2386.
[6] Zhang A and Lin X (2018), “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain”, Journal of medical systems, 42(8), pp.1-18, Springer.

[7] Cao S, Zhang G, Liu P, Zhang X and Neri F(2019),”Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain”, Information Sciences, 485, pp.427-440, Elsevier.

[8] Eltayieb N, Elhabob R., Hassan A and Li F(2020),” A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud”, Journal of Systems Architecture, 102, p.101653, Elsevier.

[9] Malina L, Hajny J, Fujdiak R and Hosek J (2016),“on perspective of security and privacy-preserving solutions in the internet of things”, Computer Networks, 102, pp.83-95, Elsevier.

[10] Zhang Y, He D and Choo K.K.R (2018), “BaDS: Blockchain-based architecture for data sharing with ABS and CP-ABE in IoT”, Wireless Communications and Mobile Computing, 2018.

[11] Shi S, He D, Li L, Kumar N, Khan M.K and Choo K.K.R (2020), “Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey”, Computers & Security, p.101966, Elsevier.

[12] A.Sonya, G.Kavitha, “Securing the Healthcare Data with Blockchain Technology” International Journal of Advanced Science and Technology, Vol. 29, No.4, (2020), pp.9474 –9481.

[13] A.Sonya, G.Kavitha “Encrypting Healthcare Data in Cloud Using Cryptographic Algorithms” Test Engineering and Management, Volume 83, Page No. 26722 – 26731, August 2020.

[14] Manoj R, Alsadoon A, Prasad PC, Costadopoulos N, Ali S(2017),” Hybrid secure and scalable electronic health record sharing in hybrid cloud”, In2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud) 2017 Apr 6 (pp. 185-190). IEEE.
[15] Awan I.A, Shiraz M, Hashmi M.U, Shaheen Q, Akhtar R. and Ditta A (2020), "Secure Framework Enhancing AES Algorithm in Cloud Computing", Security and Communication Networks, 2020.

[16] Imran M, Hlavacs H, Haq IU, Jan B, Khan FA, Ahmad A (2017), "Provenance based data integrity checking and verification in cloud environments", PloS one. 2017 May 17;12(5):e0177576.

[17] Wang X.A, Ma J, Xhafa F, Zhang M and Luo X, (2017), "Cost-effective secure E-health cloud system using identity based cryptographic techniques", Future Generation Computer Systems, 67, pp.242-254, Elsevier.

[18] Bhabendu Kumar Mohanta, Debasish Jena, Soumyashree S. Panda, Srichandan Sobhanayak (2019), "Blockchain technology: A survey on applications and security privacy Challenges”, Internet of Things (2019).

[19] Benil T and Jasper J (2020), "Cloud based security on outsourcing using blockchain in E-health systems”, Computer Networks, 178, p.107344, Elsevier.

[20] Cao S, Zhang X and Xu R (2020), "Toward secure storage in cloud-based eHealth systems: a blockchain-assisted approach”, IEEE Network, 34(2), pp.64-70.

[21] Huang H, Sun X, Xiao F, Zhu P and Wang W, (2021), "Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments”, Journal of Parallel and Distributed Computing, 148, pp.46-57, Elsevier.

[22] Shahnaz A, Qamar U and Khalid A (2019), "Using blockchain for electronic health records”, IEEE Access, 7, pp.147782-147795.
[23] Kuo T.T, Kim H.E and Ohno-Machado L (2017),”Blockchain distributed ledger technologies for biomedical and health care applications”, Journal of the American Medical Informatics Association, 24(6), pp.1211-1220.

[24] Hussein A.F, ArunKumar N, Ramirez-Gonzalez G, Abdulhay E, Tavares J.M.R and de Albuquerque, V.H.C (2018),”A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform”, Cognitive Systems Research, 52, pp.1-11, Elsevier.

[25] Xia Q, Sifah E.B, Smahi A, Amofa S and Zhang X (2017),”BBDS: Blockchain-based data sharing for electronic medical records in cloud environments”, Information, 8(2), p.44.

[26] Yue X, Wang H, Jin D, Li M and Jiang W (2016),”Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control”, Journal of medical systems, 40(10), pp.1-8, Springer.

[27] Zhang Y, Qiu M, Tsai C.W, Hassan M.M and Alamri A (2015),”Health-CPS: Healthcare cyber-physical system assisted by cloud and big data”, IEEE Systems Journal, 11(1), pp.88-95.

[28] Wang H and Song Y (2018),”Secure cloud-based EHR system using attribute-based cryptosystem and blockchain”, Journal of medical systems, 42(8), pp.1-9, Springer.