Journal of Theoretical and Applied Information Technology
15th February 2023. Vol.101. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT ELECTRONIC HEALTH RECORD (EHR) BASED INTEGRITY AND MCP-ABE MODEL FOR DISTRIBUTED BLOCK CHAIN FRAMEWORKS

KEESARA SRAVANTHI[1,3], P CHANDRA SEKHAR[2]

[1]Research Scholar, Department of Computer Science and Engineering, GITAM, Visakhapatnam, AP, India.
[2]Associate Professor, Department of Computer Science and Engineering, GITAM, Visakhapatnam, AP, India.
[3]Assistant Professor, Department of Information Technology, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, India.

ABSTRACT

Most of the conventional cloud based security frameworks are applicable to provide data security on homogeneous electronic health records(EHRs) due to data size and computational time. In the unstructured EHRs, traditional models use limited data size with partial data security in cloud computing environment. In this work, a hybrid security framework is proposed in order to provide strong security to the block chain heterogeneous databases. In this work, homogeneous 2D EHRs and heterogeneous 3D EHRs are used to compare the proposed approach to the traditional approaches. Experimental results present the proposed heterogeneous data security framework has better efficiency than the conventional models in terms of computational overhead and average runtime(ms) computations.
Keywords: *EHR Data, Cloud 2D Data, Medical 3D Data, Attribute Based Encryption.*

1. INTRODUCTION

Cloud computing is a technology where one server or a set of servers make the computing at one place for other servers that are located somewhere else that are connected using the Internet . Cloud is a space where one can use any technology remotely, without any installation at its machine, and it may never pay for this in case it do not use this technology. The term "cloud" in cloud computing is taken from the symbol of cloud used in Internet, but used interchangeably with "data center". Now a day the user using conventional computing technique are shifting to the use of cloud computing, because of the fast track advancements in the area of computer science and information technologies in the last few decades. The advancement include the wide spread availability of the Internet, the widespread usage of broadband. This advances leads to scalable software infrastructure with high performance for the data centers and the medical applications using cloud due to the concept of utility computing. Cloud computing is a multi-level framework, using a large pool of system/resources that are connected in a group using fast communication links, to provide dynamically scalable infrastructure for storing the data and executing the application. In this, the pool is constituted in such a way that only those technologies that are well tested and robust are implemented on the pool members[1]. These services are used for hosting a number of applications at various data centers consisting of appropriate hardware and system software[2]. In the security guidance report CSA define three different types of cloud based upon the services they provide, that are IaaS, PaaS and SaaS. IaaS provides computer infrastructure that include processor for processing any application, storage space for raw data and networking to customers such as Amazon EC2[3]. This includes support for all the processes that are required for development, testing and deployment of applications that work over the Internet. SaaS, is a cloud model where everything required for the working of the application that include the software and its associated data are stored in the remote system with the feature of cloud and accessed using Internet by users via browsers [4-7]. . Data integration[8] is nothing more than an assurance that the data stored on the cloud server are maintained in its original form and that unauthorized persons have not deliberately or inadvertently deleted or modified it. Now-a-days, smart functionality is very much essential in order to implement continuous, clinical data and the analysis of collected data. Hence, there is necessity of a key application in order to enforce data integrity constraints. Before implementing different analysis approaches in order to perform the task of knowledge extraction, the anomaly identification process must be implemented. Because of the vast quantities of gathered data, may create serious issues

related to large-scale, heterogeneity and complexity of data[9]. Therefore, it is very much required to develop an effective anomaly identification services. In the domain of big data applications, there are numbers of different challenges in the field of computational and storage capabilities. The above mentioned challenges can be resolved through the implementation of cloud technology[10]. To limit unauthorized access, the method of encryption and access control is very essential[11]. Data ownership states data control. When data is in local systems, the data owner is ultimately responsible for any data operation, including insertion, data deletion and modification. The process of encryption and access control are very vital to restrict the unauthorized access. Attribute based encryption technique is considered as an advanced cryptographic primitive[12-13]. It has an objective to encrypt the access control mechanism in order to outsource data. There have been vast amount of research works performed in order to propose an efficient attribute-based encryption technique.

Problem Statement:

Most of the conventional integrity based block chain frameworks are independent of data size and number of blocks for the homogenous data types. Since, electronic health records are heterogeneous in nature and it is difficult to find the integrity and security for multi-users. As the size of the distributed users are increasing in number then it is difficult to control the users using traditional security frameworks.

2. RELATED WORK

[14] mentioned elasticity and accessibility as two chief characteristics that provided prevalent acceptance of cloud computing and sanctuary threats as a vital hindrance in the espousal and growth of a safe protocol for data stowage, allocation, and reclamation. The paper discussed and pointed out the advantages and shortcomings of some of the approaches and compared them like AES, HE, ABE, proxy encryption, HIBE, and IBBE for secure data saving in cloud computing. From the comparison table, it was found that fully HE and Hierarchical Attribute-Based Encryption (HABE) were inferred as the best data security schemes [15]. Li et.al, mentioned that the chief concerns allied with information stowage management are CIA triad. Data encryption, homomorphic encryption, and secret sharing algorithms were listed as the methods widely employed for safeguarding information outsourcing. The paper mentioned why multi-clouds or inter-clouds are preferred over single clouds because a single cloud agonizes from several safety issues like vendor lock-in, data availability, etc. The paper used a Shamir secret sharing scheme to provide security in multi-clouds[16]. Liang et al. revealed in what way homomorphic encryption was deliberated to be suitable for keeping the documents onto the cloud and stated numerous concerns associated with it. It described that homomorphic encryption not only provided privacy of data in communication but also had additional competencies of calculating over encoded information, searching an encrypted data, etc. A multi-cloud style of 'N' dispersed servers to repartition the information and to approximately achieve fully homomorphic encryption was proposed for processing encrypted data. The security of the system was enhanced by increasing the confidentiality of data and performance by splitting the stored data using Data Partitioning Algorithm (DPA) amongst numerous cloud suppliers to (1) diminish the fear of the information breaches and (2) increase the parallel dispensation executing homomorphic encryption. The forthcoming effort would focus on the execution of the proposed architecture and perform safety and performance tests in view to show its feasibility[17].Liu et.al ,explored the issues, elucidations, and restrictions of cloud security. The author correlated information confidentiality and customer authentication. Thepaper mentioned that the reliability of cloud computing actions was influenced by the implementation of safety policies and therefore, security flaws and shortages must be tackled. The main aspects of security at the customer side, the connection and the server-side which all operate in a shared environment; thus their safety & secrecy concerns must be handled. Issues like server availability, multitenant services, data storage, access control, identity protection were described. A number of solutions to address them were proposed like homomorphic encryption, reliable credential management, distributed access control, etc[18]. Mandal et al. described cloud computing to evolve animatedly and diverse cloud facets were mentioned to emerge. The paper aimed to comprehend the sanctuary concerns related to cloud storing and highlighted the prominence of information integrity systems. The identification and analysis of the impact of a set of parameters of data integrity schemes were done. These parameters were mentioned to analyze the overall efficiency of the different schemes. The security attacks and mitigation techniques were discussed. Relative scrutiny of the utmost prevailing data integrity structures grounded in the recognized features was made. The future trends of exploration in the

perspective of data integrity patterns were mentioned [19].

Patil et al. described cloud computing to reshape the IT and anticipated as an auspicious facility for the subsequent generation internet. Still, security and privacy were deliberated as the key tasks inhibiting the cloud computing widespread recognition. The precision of data storing and calculation were revealed to be conceded owed to the deficiency of control of data security for clients. The author anticipated "SecCloud" as an effective and competent protocol for safety in the cloud. The impending dimension continued to be deliberate, and emphasize on privacy preserving concerns [20].Vengadapurvaja et al. (2014) emphasized the usage of big data in healthcare organizations. The paper presented a manner for safety and privacy conserving sharing of medicinal big data among organizations in a data multi-cloud environment. The architecture utilized attribute-based encryption scheme for authorization of users and secret sharing because of segmented information amid several clouds. Multicloud proxies were used to dispense and recover encoded medicinal data to and from multiple clouds in parallel. Role-based access policies and ABE for choosing traits of a medical record were used. An execution and assessment by numerous experiments were discussed and showed the useful viability and decent performance. The forthcoming effort was mentioned to check inter-organizational facets of key management and Role Based Access Control (RBAC) strategy administration, and numerous improvements for the multi-cloud proxy [21].Wang et.al, mentioned security and key management as key concerns in cloud storage despite their attractive features. A scheme called 'CloudStash' was proposed, implemented, and evaluated as a mechanism applying the secret-sharing method directly on the files for storing multiple segments of a file in multi-clouds. The mentioned technique along with multithreading was said to enhance confidentiality, availability, performance, and fault tolerance. The method was described to achieve faster speed for small files and medium files during upload and download operations. The design and algorithm analysis was done for upload and download operations utilizing multi-threading to provide a high performance. A comparison between the baseline algorithm using AES, SHA512 and RSA 1024 with CloudStash setup was done. The signature of the share was done using RSA and hashing using SHA512 on each share. The experiments were conducted in python with amazon AWS S3 API and used numerous files and eight storage centers of AWS S3 [22]. Zhanget et.al, presented a capable record level of leadership quality based encryption plot was presented in circulated figuring. The layered access structures were consolidated into a singular access structure, and thereafter, the different leveled reports were mixed with the organized access structure. The cipher text fragments related to characteristics could be shared by the archives. In this way, both cipher text accumulating and time cost of encryption was saved. Furthermore, the presented arrangement was wind up being secure under the standard supposition. Preliminary amusement shows the proposed arrangement was particularly viable with respect to encryption and translating. With the amount of the reports extending, the advantages of our arrangement become progressively self-evident[23].Xiang et.al, proposed a new key management system using identity-based authentication facility to change the data update and key multi-user access environment management operations. We also improved the encryption scheme based on the attributes to provide several control mechanisms based on the authority. Mechanisms for access control are divided into four major classes: optional, compulsory, role-based, and attribute-based. Under discretionary access control, the holder determined the subjects that were allowed to access the asset, where the access control was controlled only by the administrator, as in compulsory access control. Access was influenced by the roles of the user in roles-based access control while the user's attributes managed the access in attribute-based access control[24]. Yang et.al, introduced a common framework for public key management and multi-access control policies to ensure flexible and fine-grained information outsourcing authentication in a dual-owner environment through the use of Public Key Infrastructure (PKI) and access control. Key management complexity was minimized and the keys were distributed using a PKI-based key management protocol. A multiple model of enforcement of access control policy has been proposed to regulate multiple policies in parallel by flexibly separating administrative duties. To remove the key search process, the cryptographic protocol used for re-encryption regenerates the shared symmetric key[25]. A ring signature scheme which is based on the ElGamal signature scheme concept is developed [26]. Encoding and forwarding activities over encrypted messages are supported by this proxy re-encryption technology. This strategy, however, incurs additional expense in terms of encoding and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

forwarding procedure. Most of the traditional IDS techniques are based on encryption techniques and hash functions [27] to overcome the limitations of localization attacks. As the size of the cloud storage capacity increases, these models require high computational time. In dynamic cloud environments, chaotic linear functions are not strong to detect and prevent the attack. In this paper, a novel integrity verification model is designed and implemented to detect and prevent the malicious attacks in dynamic cloud environments[28]. In many types of attacks and threats, cloud computing is vulnerable. Since there are many safety problems in cloud computing, the risks and vulnerabilities are being researched. Cloud computing depends on multiple customers exchanging resources. Many cloud services, for example, hold a backup of the encryption key and conceal this information from their clients, they can theoretically decrypt and view all the data stored on their servers, such as Apple, which has a program called "iMessage," which manages text messages in cloud. We ensure that all messages are encrypted end-to-end but do not inform their clients that they are legally allowed to hold a copy of the key[29]. CSPs encryption process allows the clients to trust the CSPs entirely as they control the keys. To ensure the security of the cloud's sensitive and confidential data, some research suggests that the clients encrypt the data until it is stored in the cloud. Cryptonite is a secure repository of storage available on Cloud that addresses these problems by a strongbox mannequin for shared key administration. The author describes Cryptonite as a service for computing device customer that discuss efficiency and optimum utilization of resources, and furnish an empirical evaluation of upgrades[30].

Research Objectives

1. To implement an efficient integrity approach for the block chain framework on EHR records.
2. To implement a fast user access control based security approach on HER databases.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. PROPOSED MODEL

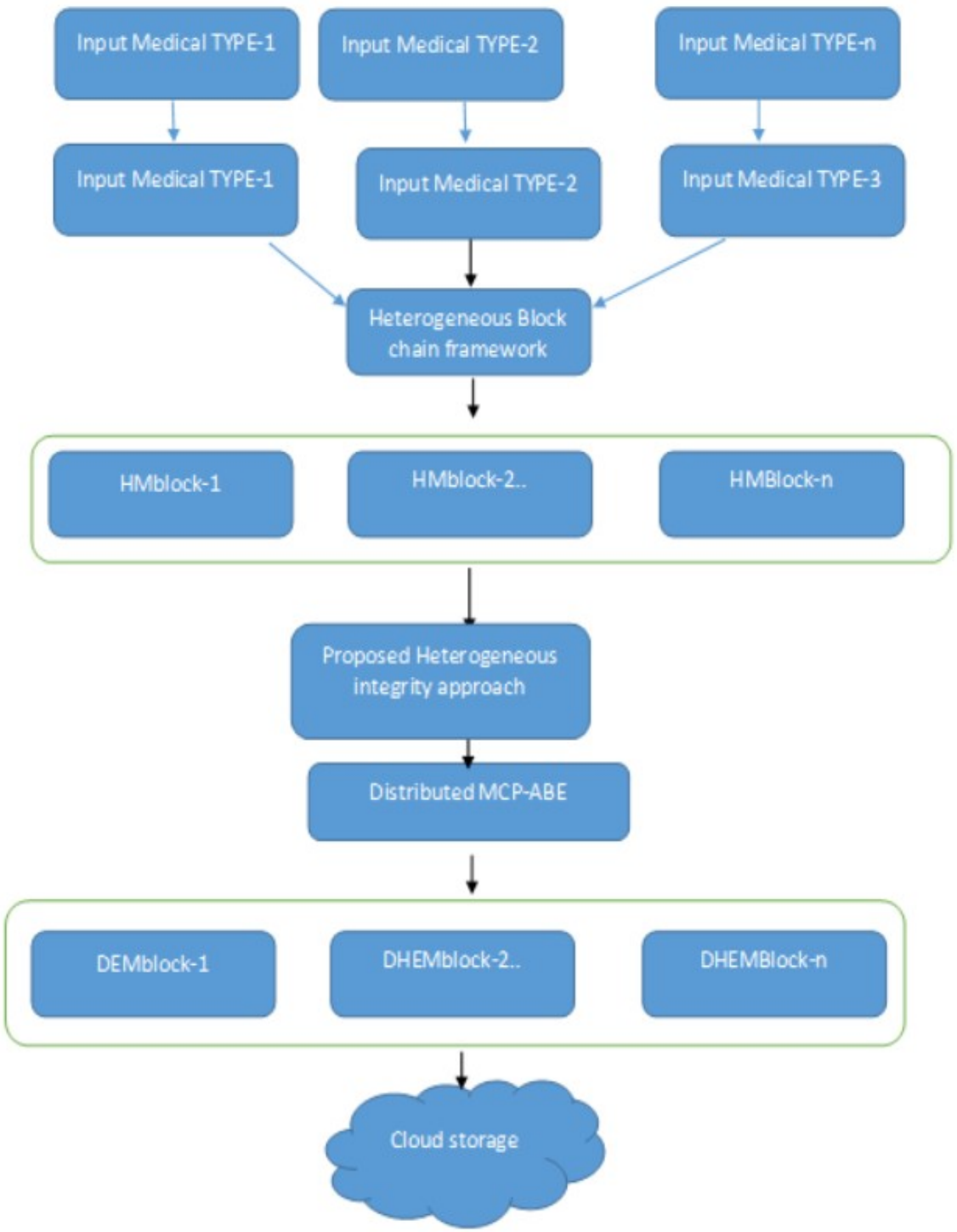


Figure 1: Proposed Approach For Block Chain Data Security

MULTI-USER DISTRIBUTED HETEROGENEOUS INTEGRITY APPROACH

```
Input: M, secret key (Sk) Hash size (HS) Initialization parameters
Step1: Read input data D, as M = D
Step2: Initialize parameters HS, NR (no of rounds)
Step3: Select the secret key to each cloud multi-user
Step4: Divide the data M into blocks of HS/8
Step5: While (|M|>HS/8)
            Do padding (add padding bit at the end 10000000…)
            Start Block processing (goto step 6)
Step6: Block process
    Partition each block into sub block of size of 4 bytes each.
    Convert block in PS[].
    For m= 0 to |PS|
    Do
        For each round r in NR-1
            Do
                Perform process subblock (PS[m]) // goto step 7
                Reverse(PS[m])
            Right shift(PS[m]
            Done
    Done
Step7: Process-Subblock
    For each byte in PS[m]
        Do
            Calculate r1, r2, r3
            Calculate H[i] = r1 ⊕r2 r3
        Done
  Generate Final Hash value H = H[1] + H[2] +H[3] ….. H[NR]
Output: Final Hash value H
```

Figure 1, Describes The Proposed Heterogeneous EHR Framework For Real-Time databases

In this framework, 2D and 3D medical images are used to improve the efficiency of the computational overhead and runtime on large data. Proposed framework is developed in three stages. In the first stage, EHR medical data collection, different medical images are loaded for the integrity and encryption process. In the second stage, an advanced statistical integrity approach is developed on the 2D and 3D medical images. In the third stage, a multi-user access control based heterogeneous data security framework is developed for different image databases.

EHR data collection: In the proposed model, a hybrid data integrity and multi-user encryption framework is designed and implemented on the cloud medical datasets. Most of the conventional integrity models are independent of medical data type with 2D and 3D images. 3D medical images such as brain and spinal cord DICOM images are difficult to compute its integrity due to variation in data and type. Also, traditional attribute based approaches such as KP-ABE,C-ABE etc. are difficult to encode the heterogeneous data types due to variation in data.

EHR data integrity computation phase - Proposed EHR Integrity model

In the proposed integrity model,

Proposed Data transformation process

Input: Input Data M = PT

PT=[r1, r2..rn]=P[]

Convert to byte array

To each partition data in multi-search file p[]

do

Mean μ = new Mean(p);

Variance σ^2 = new Variance(p);

Skewness sk = new Skewness(p);

Kurtosis k = new Kurtosis(p);

ss=$\sum p^2$

Evalute(η)

Transformation box=$\{\sigma, sk, k, Evalute(\eta)\}$

done

Evaluate(p)

Select any two randomized cyclic group elements as m1, m2

In order to improve the security parameters in the key generation process, the non-linear chaotic equation is given as

$$F_n = mx + F_{n-2}$$
$$F_0 = 1$$
$$F_1 = k(1+m^2)$$

EHR data integrity computation phase: In this phase, a set of statistical measures are used to improve the chaotic nature of the integrity approach for heterogeneous medical images. In this approach, a variable sized integrity value is generated for 2D and 3D image data.In the proposed integrity approach, a set of non-linear functions are used to enhance the integrity verification for the input data with different key sizes.

Where m is a security value from the cyclic group $Z(n^2,*)$

Return $F_n[p]$.

Output:

Transformation box=$\{\sigma, sk, k, Evalute(\eta)\}$

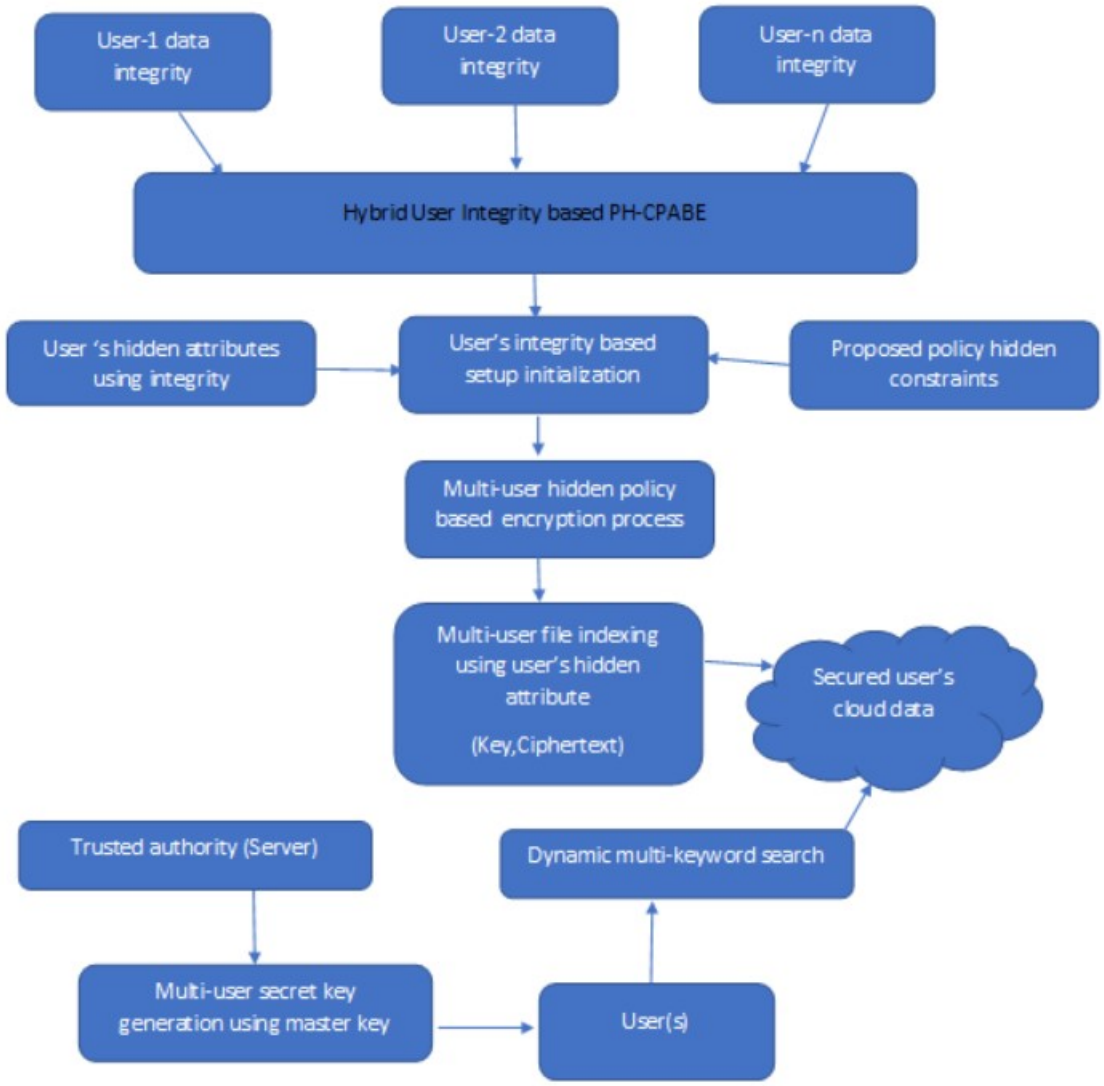
Multi-Document indexing :

In this work, a novel similarity indexing measure is used to find search the files in the cloud databases.

$$Score(k_i, d_j) = \frac{|k|_{ij}}{prob(k_{ij}/d_j)} \times \log_2 \frac{|D|}{1+|prob\{w_i \in d_j\}|}$$

Heterogeneous cloud based EHR data encryption and decryption (HCEHRE)

In this work, a hybrid non-linear data integrity computation model is proposed to verify the integrity of each user in the multi-user for strong cloud data security. In this work, a multi-user non-linear-integrity-based encoding framework is developed to improve the cloud data security for the EHR data. In the proposed multi-user encryption model, four key phases are implemented to secure the data in the block chain technology. The four phases include, multi-user access key initialization process, Multi-Access User EHR Data encryption phase, Multi-access secret key generation phase, Multi-Access user data decryption phase.



Step 1: In this step, each patient byte array data and integrity value are taken as input for the encryption process. Here, in the data initialization process, user's integrity value is considered as the key access constraint for the encryption process. User's integrity value is taken as token value for the user's key generation process. In this step, user's token and heterogeneous EHR byte array data are used to generate the public key and multi-access control key for the encryption process.

T represent the token key of the EHR cloud user.
P is the pairing of three groups with prime order r.
t_α is the randomized field element of pairing element Z_r.
t_tk is the randomized field element fo pairing element G_2 using T.
n1,n2 are the two randomized prime order field elements.

Step 2: EHR data encryption process: In this phase, Compute token based public key for the HEHR encryption process as

Journal of Theoretical and Applied Information Technology
15th February 2023. Vol.101. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$Token\_PK(T,P) = \{E(G_1 + t\_t_k), E(G_2 * t\_t_k), E(G_1 + t\_t_k)^{E(n1*n2)}, P(E(n1*n2), E(G_2 * t\_t_k)^{Z_T}, E(n1*n2))\}$$

Step 3: Compute token based multi-user access control key as

$$Token\_CK(T,P) = \{E(n1*n2), E(G_2 * t\_t_k)$$

Step 4: Encode the HEHR data using the token based public key and token key.

$$s = E(G_1)^{E(t\_t_k)}$$

Bind each user's token key in the pairing library access tree structure in the JPBC.

$$Fillpolicy(Tk[], s, Token\_PK(T,P))$$

$$ct1 = mP(E(n1*n2), E(G_2 * t\_t_k)^{Z_T}.E(n1*n2))^{Z_s}$$

$$ct2 = (E(G_1 + t\_t_k)^{E(n1*n2)})^{Z_s(s)}$$

In this setup process, a hybrid multi-user policy based master-key and public-key are generated using the randomized cyclic group elements. The multi-user master and public key elements of the setup process are constructed based on the bilinear pairing elements.

4.Experimental Results

Experimental results are executed in real-time cloud server with java environment. In this work, a real-time Amazon AWS server and multi-user data are used to implement hash framework. In the work, different third party libraries such as apache math, JAMA, java pairing and AWS JDK are used to implement integrity and security algorithms. In the experiment evaluation, hash bit change, hash runtime(ms), cloud encryption runtime(ms) and decryption runtime(ms) are computed on the cloud transactions data. Hash bit change represents the measuring the impact on the integrity bits by changing input data bits. In the experimental evaluation, traditional integrity algorithms such as SHA, MD5, linear chaotic, polynomial chaotic and non-linear chaotic approaches. Also, proposed encryption model is compared to the traditional models such as KP-ABE,CP-ABE, multi-authority CP-ABE in the experimental evaluation. In the experimental results, 2D and 3D images as shown in fig 3,fig 4 and fig 5 are used to evaluate the performance of the proposed model using runtime and bit change rate.

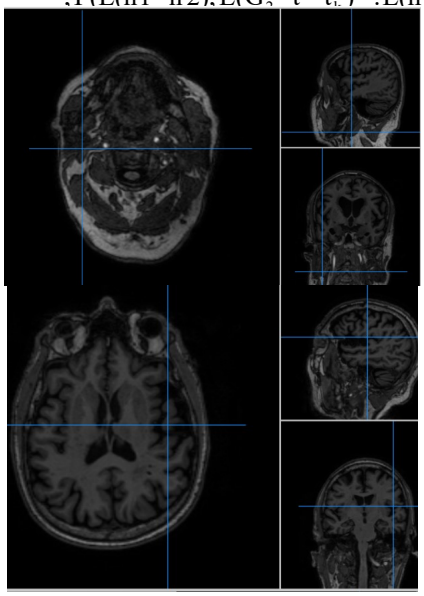


Figure 3: 3D View Of ADNI DICOM Image.

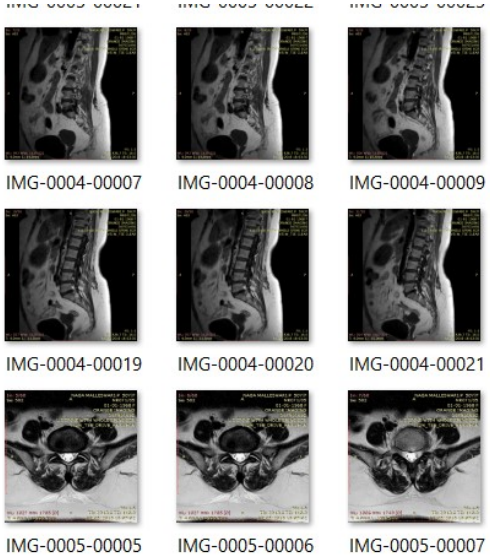


Figure 4: 2D Slices Of Patient Spinal Cord.

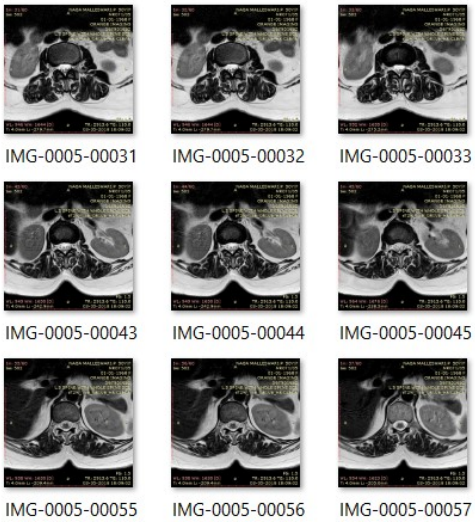


Figure 5: 2d Slices Of Patient Adni.

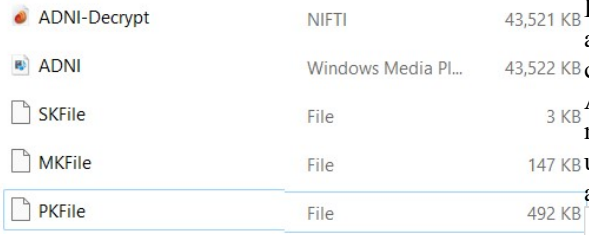


Figure 6: Secret Key , Master Key And Private Key Files Of Proposed Encryption Scheme.

Table 1: Runtime(Ms) Comparison Of Proposed Non-Linear Token Generation To The Conventional Approaches On 2D Brain Slices.

MedicalFile	SHA512	MD5	linearChaotic	PolyChaotic	ProposedTokenGen
EHR2DFile-1	3519	3533	3777	3312	3022
EHR2DFile-2	3805	3563	3596	3242	3012
EHR2DFile-3	3836	3850	3484	3096	3003
EHR2DFile-4	3513	3602	3697	3069	3014
EHR2DFile-5	3559	3608	3462	3324	3034

Table 1, represents the comparative runtime(ms) analysis of proposed key generation approach to the conventional approaches on 2D brain slices. As presented in table, it is noted that the proposed non-linear token key generation has better multi-user key generation approach than the conventional approaches on 2D brain images.

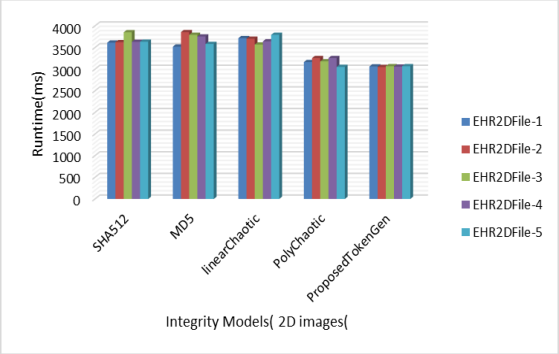


Figure 7: Runtime(Ms) Comparison Of Proposed Non-Linear Token Generation To The Conventional Approaches On 2d Spinalcord Slices.

Figure 7, represents the comparative runtime(ms) analysis of proposed key generation approach to the conventional approaches on 2D spinalcord slices. As presented in figure, it is noted that the proposed non-linear token key generation has better multi-user key generation approach than the conventional approaches on 2D spinalcord images.

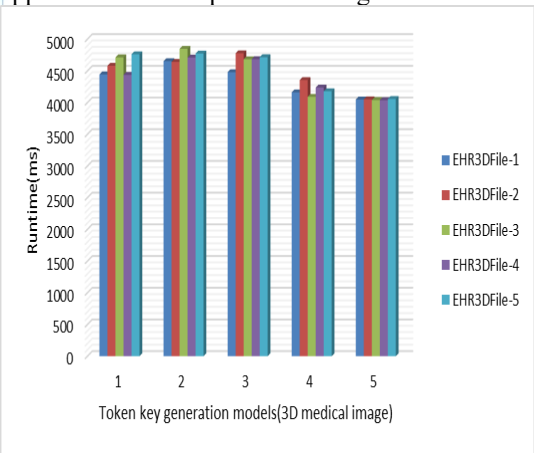


Figure 8: Runtime(Ms) Comparison Of Proposed Non-Linear Token Generation To The Conventional Approaches On 3d Adni Images.

Figure 8, represents the comparative runtime(ms) analysis of proposed key generation approach to the conventional approaches on 3D ADNI images. As presented in figure, it is noted that the proposed non-linear token key generation has better multi-user key generation approach than the conventional approaches on 3D ADNI image.

Table 2: Average Encryption And Decryption Runtime(Ms) Of Proposed Non-Linear Token Generation To The Conventional Approaches On 2D Brain Images.

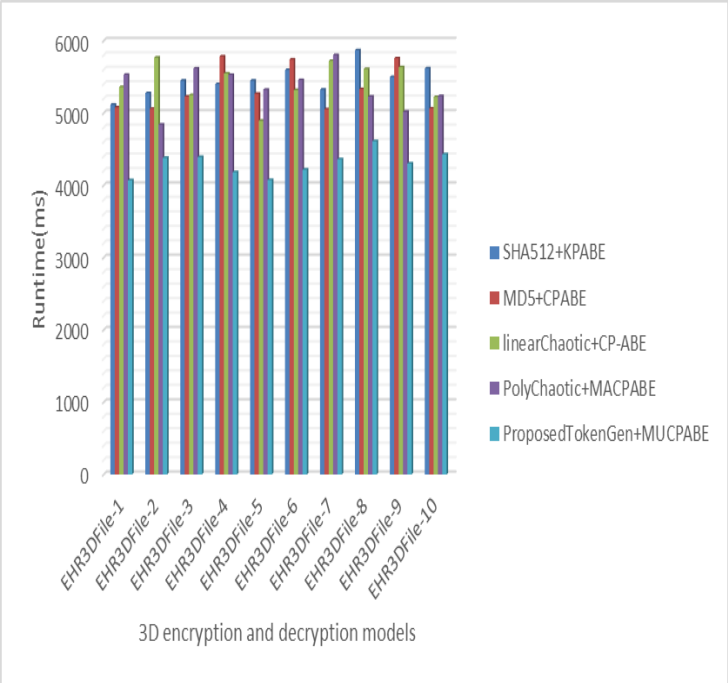
EHRTransactions	SHA512ABE	MD5ABE	WhirlpoolABE	Parallel_Chaotic-ABE	Proposed
MEDEHR-1	5141	5793	5478	5472	4332
MEDEHR-2	5428	4918	5009	5456	4361
MEDEHR-3	5183	5758	4943	4997	4770
MEDEHR-4	5141	5044	5240	5843	4233
MEDEHR-5	5176	5055	4972	5005	4243
MEDEHR-6	4924	5263	5456	5107	4274
MEDEHR-7	5609	5170	5105	5730	4563
MEDEHR-8	5152	5134	5700	5421	4374
MEDEHR-9	5765	5705	5045	5243	4384
MEDEHR-10	5351	5676	5468	5529	4344

Table 2, represents the comparative runtime(ms) analysis of proposed encryption and decryption approach to the conventional approaches on 2D brain slices. As presented in table, it is noted that the proposed non-linear token key generation has better multi-user key based encryption and decryption approach than the conventional approaches on 2D brain slice images.

Table 3: Average Encryption And Decryption Runtime(Ms) Of Proposed Non-Linear Token Generation To The Conventional Approaches On 2D Spinalcord Images.

MedicalFile	SHA512+KPABE	MD5+CPABE	linearChaotic+CP-ABE	PolyChaotic+MACPABE	ProposedTokenGen+MUCPABE
EHR 2DFile-1	5760	4885	5375	5800	4452
EHR 2DFile-2	5391	5685	4838	5149	4230
EHR 2DFile-3	5738	5729	5284	5284	4383
EHR 2DFile-4	5814	5462	5867	5802	4671
EHR 2DFile-5	5125	5702	5090	4897	4249

Table 3, represents the comparative runtime(ms) analysis of proposed encryption and decryption approach to the conventional approaches on 2D spinalcord slices. As presented in table, it is noted that the proposed non-linear token key generation has better multi-user key based encryption and decryption approach than the conventional approaches on 2D spinalcrod images.



EHRTransactions	SHA512ABE	MD5ABE	WhirlpoolABE	Parallel_Chaotic-ABE	Proposed
MED-1	5141	5793	5478	5472	4332
MED-2	5428	4918	5009	5456	4361
MED-3	5183	5758	4943	4997	4770
MED-4	5141	5044	5240	5843	4233
MED-5	5176	5055	4972	5005	4243
MED-6	4924	5263	5456	5107	4274
MED-7	5609	5170	5105	5730	4563
MED-8	5152	5134	5700	5421	4374
MED-9	5765	5705	5045	5243	4384
MED-10	5351	5676	5468	5529	4344

Figure 9: Average Encryption And Decryption Runtime(Ms) Of Proposed Non-Linear Token Generation To The Conventional Approaches On 3D Adni Images.

Figure 9, represents the comparative runtime(ms) analysis of proposed key generation approach to the conventional approaches on 3D ADNI images. As presented in figure, it is noted that the proposed non-linear token key generation has better multi-

user key generation approach than the conventional approaches on 3D ADNI images images.

5. CONCLUSION

In this paper, a hybrid multi-user tokenkey generation based multi-user ciphertext policy encryption and decryption framework is proposed on the cloud medical records. Since, most of the conventional key generation models are difficult to create variable size key for the encryption and decryption process. Also, conventional attribute based encryption models are independent of token key for the user's authentication and security verification process. In this work, an advanced user authentication based medical data encryption and decryption is proposed on the cloud medical records. Experimental results are evaluated on different medical records using token bit change and runtime computation. The main differences of existing and proposed frameworks are summarized below:

Sno	Existing commercial block chain approaches	Proposed Approaches
1	Supports traditional integrity approaches such as MD5,SHA family.	Supports traditional and new integrity approach
2	Supports limited datasize	Supports large datasize
3	Integrity size is fixed to 512	Integrity key is large
4	Limited access control	Fully access control

LIMITATIONS OF WORK:

The main limitations of the work are :

1. Require high computational memory in order to process large size HER files.
2. If the data size is large(>5GB), then this model require cloud services for data processing.

REFERENCES

[1]M. Alloghani et al., "A systematic review on the status and progress of homomorphic encryption technologies," Journal of Information Security and Applications, vol. 48, p. 102362, Oct. 2019, doi: 10.1016/j.jisa.2019.102362.

[2]S. Belguith, N. Kaaniche, M. Laurent, A. Jemai, and R. Attia, "PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT," Computer Networks, vol. 133, pp. 141–156, Mar. 2018, doi: 10.1016/j.comnet.2018.01.036.

[3]W. Briguglio, P. Moghaddam, W. A. Yousef, I. Traoré, and M. Mamun, "Machine learning in precision medicine to preserve privacy via encryption," Pattern Recognition Letters, vol. 151, pp. 148–154, Nov. 2021, doi: 10.1016/j.patrec.2021.07.004.

[4]L. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," Future Generation Computer Systems, vol. 95, pp. 420–429, Jun. 2019, doi: 10.1016/j.future.2019.01.018.

[5]B. D. Deebak, F. H. Memon, K. Dev, S. A. Khowaja, and N. M. F. Qureshi, "AI-enabled privacy-preservation phrase with multi-keyword ranked searching for sustainable edge-cloud networks in the era of industrial IoT," Ad Hoc Networks, vol. 125, p. 102740, Feb. 2022, doi: 10.1016/j.adhoc.2021.102740.

[6]G. Dhanalakshmi and V. S. George, "Security threats and approaches in E-Health cloud architecture system with big data strategy using cryptographic algorithms," Materials Today: Proceedings, Mar. 2022, doi: 10.1016/j.matpr.2022.03.254.

[7]M. A. C. Dizon and P. J. Upson, "Laws of encryption: An emerging legal framework," Computer Law & Security Review, vol. 43, p. 105635, Nov. 2021, doi: 10.1016/j.clsr.2021.105635.

[8]C.-I. Fan and S.-Y. Huang, "Controllable privacy preserving search based on symmetric predicate encryption in cloud storage," Future Generation Computer Systems, vol. 29, no. 7, pp. 1716–1724, Sep. 2013, doi: 10.1016/j.future.2012.05.005.

[9]Q. He, N. Zhang, Y. Wei, and Y. Zhang, "Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems," Computer Networks, vol. 140, pp. 163–173, Jul. 2018, doi: 10.1016/j.comnet.2018.01.038.

[10]H.-B. How and S.-H. Heng, "Blockchain-enabled searchable encryption in clouds: A review," Journal of Information Security and Applications, vol. 67, p. 103183, Jun. 2022, doi: 10.1016/j.jisa.2022.103183.

[11]H. Huang, X. Sun, F. Xiao, P. Zhu, and W. Wang, "Blockchain-based eHealth system for auditable EHRs manipulation in cloud environments," Journal of Parallel and Distributed Computing, vol. 148, pp. 46–57, Feb. 2021, doi: 10.1016/j.jpdc.2020.10.002.

[12]S. H. Islam, N. Mishra, S. Biswas, B. Keswani, and S. Zeadally, "An efficient and forward-secure lattice-based searchable encryption scheme for the Big-data era," Computers & Electrical Engineering, vol. 96, p. 107533, Dec. 2021, doi: 10.1016/j.compeleceng.2021.107533.

[13]T. Kanwal, A. Anjum, S. U. R. Malik, A. Khan, and M. A. Khan, "Privacy preservation of electronic health records with adversarial attacks identification in hybrid cloud," Computer Standards & Interfaces, vol. 78, p. 103522, Oct. 2021, doi: 10.1016/j.csi.2021.103522.

[14]H. Ku, W. Susilo, Y. Zhang, W. Liu, and M. Zhang, "Privacy-Preserving federated learning in medical diagnosis with homomorphic re-Encryption," Computer Standards & Interfaces, vol. 80, p. 103583, Mar. 2022, doi: 10.1016/j.csi.2021.103583.

[15]N. Li, Z. Chen, J. Nie, X. Fu, and X. Jia, "Complementary set encryption for privacy-preserving data consolidation," Information Sciences, vol. 593, pp. 271–288, May 2022, doi: 10.1016/j.ins.2022.02.002.

[16]W. Li, L. Xu, Y. Wen, and F. Zhang, "Conjunctive multi-key searchable encryption with attribute-based access control for EHR systems," Computer Standards & Interfaces, vol. 82, p. 103606, Aug. 2022, doi: 10.1016/j.csi.2021.103606.

[17]J. Liang, Z. Qin, S. Xiao, J. Zhang, H. Yin, and K. Li, "Privacy-preserving range query over multi-source electronic health records in public clouds," Journal of Parallel and Distributed Computing, vol. 135, pp. 127–139, Jan. 2020, doi: 10.1016/j.jpdc.2019.08.011.

[18]Y. Liu, Y. Ren, C. Ge, J. Xia, and Q. Wang, "A CCA-secure multi-conditional proxy broadcast re-encryption scheme for cloud storage system," Journal of Information Security and Applications, vol. 47, pp. 125–131, Aug. 2019, doi: 10.1016/j.jisa.2019.05.002.

[19]M. Mandal, "Privacy-preserving fully anonymous ciphertext policy attribute-based broadcast encryption with constant-size secret keys and fast decryption," Journal of Information Security and Applications, vol. 55, p. 102666, Dec. 2020, doi: 10.1016/j.jisa.2020.102666.

[20]K. S. Patil, I. Mandal, and C. Rangaswamy, "Hybrid and Adaptive Cryptographic-based secure authentication approach in IoT based applications using hybrid encryption," Pervasive and Mobile Computing, vol. 82, p. 101552, Jun. 2022, doi: 10.1016/j.pmcj.2022.101552.

[21]A. M. Vengadapurvaja, G. Nisha, R. Aarthy, and N. Sasikaladevi, "An Efficient Homomorphic Medical Image Encryption Algorithm For Cloud Storage Security," Procedia Computer Science, vol. 115, pp. 643–650, Jan. 2017, doi: 10.1016/j.procs.2017.09.150.

[22]X. Wang, L. Bai, Q. Yang, L. Wang, and F. Jiang, "A dual privacy-preservation scheme for cloud-based eHealth systems," Journal of Information Security and Applications, vol. 47, pp. 132–138, Aug. 2019, doi: 10.1016/j.jisa.2019.04.010.

[23]L. Wu, Y. Zhang, K.-K. R. Choo, and D. He, "Efficient and secure identity-based encryption scheme with equality test in cloud computing," Future Generation Computer Systems, vol. 73, pp. 22–31, Aug. 2017, doi: 10.1016/j.future.2017.03.007.

[24]X. Xiang and X. Zhao, "Blockchain-assisted searchable attribute-based encryption for e-health systems," Journal of Systems Architecture, vol. 124, p. 102417, Mar. 2022, doi: 10.1016/j.sysarc.2022.102417.

[25]X. Yang, J. Wang, W. Xi, T. Tian, and C. Wang, "A blockchain-based keyword search scheme with dual authorization for electronic health record sharing," Journal of Information Security and Applications, vol. 66, p. 103154, May 2022, doi: 10.1016/j.jisa.2022.103154.

[26]G. Zhang, Z. Yang, and W. Liu, "Blockchain-based privacy preserving e-health system for healthcare data in cloud," Computer Networks, vol. 203, p. 108586, Feb. 2022, doi: 10.1016/j.comnet.2021.108586.

[27]X. Zhang, Y. Tang, S. Cao, C. Huang, and S. Zheng, "Enabling identity-based authorized encrypted diagnostic data sharing for cloud-assisted E-health information systems," Journal of Information Security and Applications, vol.

54, p. 102568, Oct. 2020, doi: 10.1016/j.jisa.2020.102568.

[28]X. Zhang, Y. Tang, H. Wang, C. Xu, Y. Miao, and H. Cheng, "Lattice-based proxy-oriented identity-based encryption with keyword search for cloud storage," Information Sciences, vol. 494, pp. 193–207, Aug. 2019, doi: 10.1016/j.ins.2019.04.051.

[29]Y. Zhang, R. Zhao, Y. Zhang, R. Lan, and X. Chai, "High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system," Journal of King Saud University - Computer and Information Sciences, Apr. 2022, doi: 10.1016/j.jksuci.2022.04.001.

[30]M. Zhao E and Y. Geng, "Homomorphic Encryption Technology for Cloud Computing," Procedia Computer Science, vol. 154, pp. 73–83, Jan. 2019, doi: 10.1016/j.procs.2019.06.012.