SECURE SHARING OF EHR WITH 2 LEVEL SECURITY USING CLOUD COMPUTING

Dr. Mrs. Shraddha Dudhani[1], Dr. Meghana Bhilare[2], Dr. Mayank R. Kothawade

Article History: Received: 10.05.2023 **Revised:** 20.06.2023 **Accepted:** 28.07.2023

Abstract:

Now a day's cloud computing is used in all emerging area like banking sector, automobile, finance, agricultural sector, health sector etc. It changes the scenario of IT industry by providing services in cost effective and continuous manner without administrative hassle. By using service model of cloud in the form of SAAS, PAAS, IAAS any one can build their infrastructure, worked on any application and any platform without financial impact on any organization that's make cloud computing more popular in small and mediums scale industry. Cloud technology is emerged and applied to health care sector also in many forms. The main application of these is to centralized storage of Electronic Health Record (EHR) or Electronic Medical Record (EMR). Centralized storage of EHR in cloud is innovative concept but at the same time it arises many security issues related to sharing of , Access control ,privacy issues of EHR .so our main motive is to designed such innovative model for exchange of EHR among Health care organization and Hospitals that it can be user friendly easily share among all Health care organization (HCO) and Hospitals cloud as data sharing vehicle and particularly achieving highest level of security by designing appropriate algorithm and apply on EHR

In our work we designed a fragmented EHR Model and two tire security of encryption level at the same time for EHR to be more secure we apply access control on EHR to enhance secrecy.

The cloud based model to be proposed to offer secure sharing of EHR between inters HCO which is geographically lactated differently. It is patient centric model (Patient having right to share their EHR

Keywords: EHR, EMR HCO, secure sharing,

[1]Assistant Professor, Dr. D.Y. Patil Institute of Management & Research
[2]Professor, Dr. D.Y.Patil Institute of Management & Research

Email: [3]mayank.kothawade@gmail.com

DOI: 10.31838/ecb/2023.12.s3.763

1.

2. Introduction:

Medicinal services frameworks are exceedingly intricate, divided and utilize various data innovation frameworks. With sellers joining diverse guidelines for comparative or same frameworks, it is little ponder that inside and out wastefulness, waste and mistakes in medicinal services data and conveyance the board are very typical an event. Therefore, a patient's medicinal data frequently gets caught in storehouses of in EHR frameworks, powerless to be imparted to individuals from the human services network. These are a portion of the few inspirations driving a push to energize institutionalization, reconciliation and electronic data trade among the different social insurance suppliers. Formative Origins of Health and Diseases (DOHAD) have effectively demonstrated the significance of formative records of people in foreseeing or potentially clarifying the maladies that an individual is experiencing. In the current to a great extent paper-based therapeutic records world, significant information is as a rule inaccessible at the ideal time in the hands of the clinical consideration suppliers to allow better consideration. This is to a great extent because of the wasteful aspects inalienable in the Paper-based framework. In an electronic world, it is particularly conceivable, gave certain critical advances are taken already, to guarantee the accessibility of the correct data at the opportune time .In request to be important, the wellbeing record of an individual should be from origination (better) or birth (in any event). As one advances through one's life, each record of each Clinical experience speaks to an occasion in one's life. Every one of these records might be immaterial or huge relying upon the present issues that the individual experiences. Consequently, it winds up basic that these records be masterminded sequentially to give a rundown of the different clinical occasions in the lifetime of an individual. Electronic wellbeing records are a synopsis of the different electronic medicinal records that get produced amid any clinical experience. EMR/EHR, proprietorship, protection and security viewpoints, medicinal services informatics guidelines, and the different coding frameworks are completed trailed by the itemizing of the base informational collection that any Indian EMR must have. A foundation on EMR and EHR and its utilization is given, trailed by a rundown of the different Stakeholders

3. Literature Review

This section offers literature survey of the research topic that is divided into three parts as per our title of research. It also gives systematic approach to finds research gap so that we can execute our research activity in correct direction

1. Critical review of prior studies relevant to electronic Health Records (EHR)
2. Security issues and challenges
3. Deployment of E-health on cloud

Electronic health record (EHRs). Firstly, the chapter provides an overview of EHRs followed by EHR systems and lastly security models, which are the main research areas the thesis contributes. The related work on EHR is described under three general themes, namely: EHR systems models, legal and system standards, and security models with the goal of identifying and re-applying a security model that fits within the constraints of developing countries. OtEHR subsections of this chapter are identifying key research gaps and explore the design and usability of interactive security issue and challenges on cloud and deployment of E-health on cloud technologies for patients. Based on the results, the chapter sets out a research

agenda for the thesis, and justifies the selection of the security model that we used in our EHR system.
Literature review for this work was conducted online research mainly engrossed on peer review article found in Google scholar, ASM digital library, various known journals and article of EBISCO, Springer, Elsevier; PubMed, etc.

1. Secure Data Sharing in the Cloud byDananThilakanathan, Shiping Chen, Surya Nepal and Rafael A. CalvoS. Nepal and M. Pathan (eds.), Security, Privacy and Trust in Cloud Systems, 45 DOI: 10.1007/978-3-642-38586-5_2, © Springer-Verlag Berlin Heidelberg 2014. He discussed about the privacy issues of cloud computing also dicussed about Privacy and Confidentiality of data in Healthcare:

2. A Dynamic Cloud Computing Platform for eHealth Systems by Mehdi Bahrami 1 and MukeshSinghal 2 of Cloud Lab University of California Merced, USA2015 IEEE 17th International Conference on e-Health Networking, Applications and Services (Healthcom) This paper discussed vendor lock-in issue that causes a healthcare system rely on a cloud vendor infrastructure, and it does not allow the system to easily transit from one vendor to anotEHR.

3. Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform by Zhuo-Rong Li1, En-Chi Chang1, Kuo-Hsuan Huang1, Feipei2011 IEEE 15th International Symposium on Consumer Electronics Most hospitals and clinics now have their own databases to manage electronic medical records. The exchange of electronic medical records is easier within the same electronic medical record system. However, the exchange of electronic medical records slows down between different electronic medical record systems .Some of the smaller hospitals or clinics do not have the relevant servers to manage their electronic medical records, or to provide the electronic medical record exchange capability. The cloud platform can provide an exchange platform that all hospitals and clinics can use, and can serve as an electronic medical record storage center. This can simplify the complex electronic medical record exchange procedure between different systems, and save the equipment setup expenses for smaller hospitals. An Impact of Digital Technologies Transforming In Healthcare Using Cloud Computing by M.Gnanavel1,Dr.E.R.Naganathan,R.Saravanakumar,R.J.Poovaraghan,P.Sasikala5 International Journal of Innovative Research in Computer and Communication Engineering(An ISO 3297: 2007 Certified Organization) Vol. 2, Issue 2, February 2014.
This paper emphasis on increased medical knowledge has brought about more technological advancements in treatment and devices that require computer support. Increases in medical/research data has brought about the need for highly complex computer support systems to analyze and retrieve information.

4. Impact of Cloud Computing on Healthcare November,2012 by cloud standard customer council guide. The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers of the healthcare industry as they analyze and onsider the implications of cloud computing on their business. The paper includes guidance and strategies, designed to help these decision makers evaluate and compare cloud computing offerings in key areas from different cloud providers, taking into account different requirements from various actors including medical practices, hospitals, research facilities, insurance companies and governments.

5. Health Records Protection in Cloud Environment by Doan B. Hoang, Lingfeng Chen in 2014 IEEE 13th International Symposium on Network Computing and Applications 978-1-4799 5393-6/14. This paper discusses the concept of active electronic health records (or active data cubes) and technologies that ensure the integrity and the welfare of EHRs this paper focus on the protection of EHRs in Cloud environment with the support of the proposed framework.

6. Protection of Electronic Health Records (EHRs) in Cloud by AbdulatifAlabdulatif, Ibrahim Khalil, Vu Mai School of Computer Science and Information Technology RMIT university 35th Annual International Conference of the IEEE EMBS Osaka, Japan, 3 - 7 July, 2013 This paper discussed about the protection of electronic health record in cloud Designing an access control model for encrypted EHRs in the cloud relies mainly on various aspects, including the encryption scheme, the key management mechanism of encrypted EHRs and the natural flow of communication between the different participants.

7. Secret Sharing for Health Data in Multiprovider Clouds by Tatiana Ermakova, Benjamin Fabian by 2013 IEEE International Conference on Business Informatics 978-0-7695-5072 This paper proposed a novel architecture for sharing electronic health records in a multi-cloud environment, i.e., wEHRe data is not only stored at a single CP, but at several independent providers in parallel. This architecture satisfies many of the requirements derived from expert interviews during an ongoing case study and a thorough literature analysis.

8. Secure Sharing of Electronic Health Records in Clouds RuoyuWul, Gail-JoonAhnl, Hongxi**n**Hu2 8th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing , Collaboratecom 2012 Pittsburgh, PA, United States, October 14-17, 2012. In this paper, we focus on access control issues in electronic medical record systems in clouds. They proposed a systematic access control mechanism to support selective sharing of composite electronic health records (EHRs) aggregated from various health care providers in clouds.

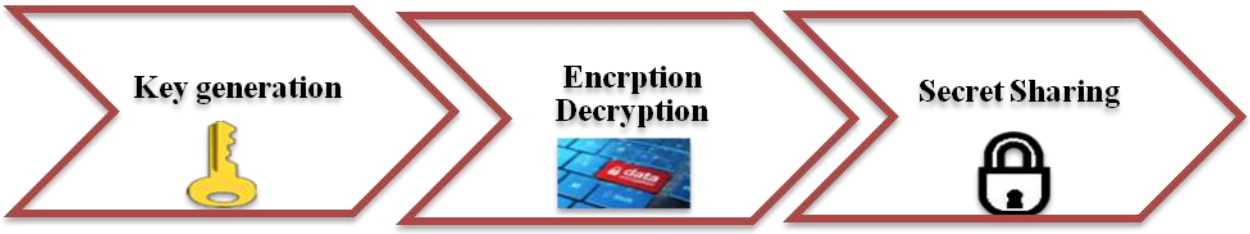
9. Asymmetric Key Cryptography Based Technique to Detect and Isolate Zombie attack in Cloud Architecture International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 3, March 2016 ISSN: 2277 128X, this paper emphasis on Security of the Major anxieties when planning to adopt the cloud. Providing a security of data in cloud is important to achieve users trust on cloud provider. This involves virtualization security, distributed computing, application security, identity management, access control and authentication.

10. Secure Key for Authentication and Secret Sharing in Cloud Computing by Dr. Santosh Lomte, Shraddha Dudhani International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 6, June 2015 ISSN: 2277 128X. In this paper the security provided to the cloud with the help of Kerberos it is authentication protocol it works on four parties. In this paper we focused about the need of authentication in cloud computing .it is narrative approach of authentication by Kerberos and threshold cryptography so that encryption technique is more robust

4. Proposed Work:

The proposed work architecture for sharing electronic health records (EHR) in a multi-cloud environment, i.e. where data is not only stored at a single cloud provider (CP), but at several independent

providers in parallel. The approach of work is particular based on sharing EHR, where we apply the security on EHR by using AES algorithm the encrypted electronic health records (EHR) stored at different CPs. generated key is further encrypted by MD5 algorithm and converted in to message digest and store in cloud, when stakeholder wants to revel record first it converted message digest into normal key which is generated during AES encryption further key is Decrypted and unlock EHR



5. Guideline for Electronic Health Record (EHR) as Per India Government Regulations

In this section we discussed guidelines for EHR as per Indian government regulation tEHRe are A Survey Conducted by Medical Informatics Group, C-DAC, Pune as part of Project for Building Distributed National EHR funded by DIT, MCIT, Govt. of India

In this section we discussed guidelines for EHR as per Indian government regulation tEHRe are A Survey Conducted by Medical Informatics Group, C-DAC, Pune as part of Project for Building Distributed National EHR funded by DIT, MCIT, Govt. of India

Table 2:Country-wise Usage of Standards

	Australia	Austria	Canada	Denmark	England	Hongkong	NetEHRlands	Sweden	Singapore	Taiwan
HL7 V 2.5	N	N	N	N	N	Y	N	N	N	N
HL7 V3 ONLY	N	Y	Y	N	Y	Y	Y	Y	N	N
CDA	Y	Y	Y	N	Y	Y	N	N	N	Y
ASTM CCR	N	N	N	N	Y	N	N	N	N	N
CCD	N	N	N	N	Y	N	N	N	N	N
OPEN EHR	Y	N	N	Y	N	N	N	Y	N	N
IHE	N	Y	Y	N	N	N	N	N	N	N
DICOM	N	Y	Y	N	N	N	N	N	N	N
EDIFACT	N	N	N	Y	N	N	N	N	N	N
EHRCOM	N	N	N	N	N	N	N	Y	N	N

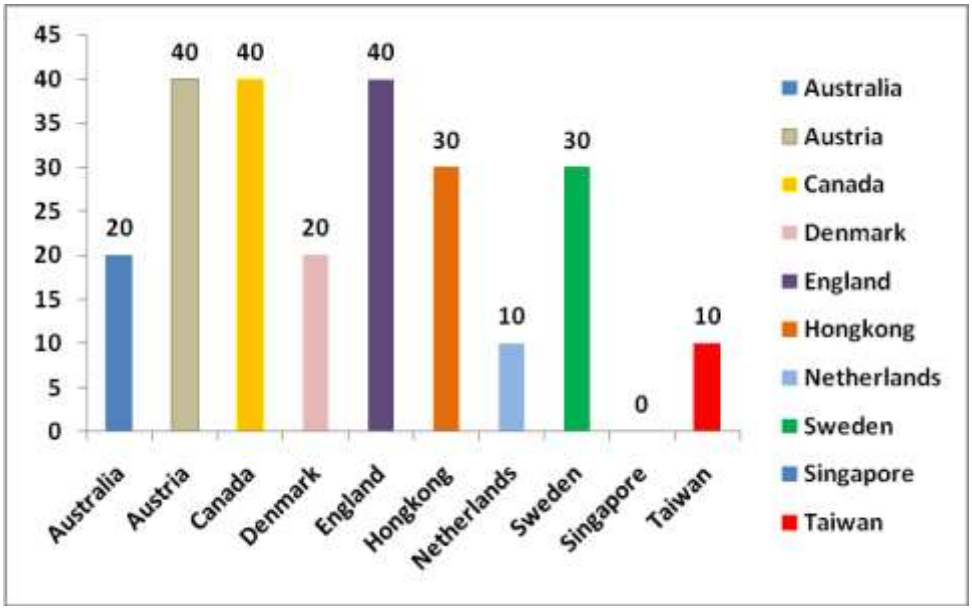


Figure 1: Country-wise Data Exchange Standards Usage

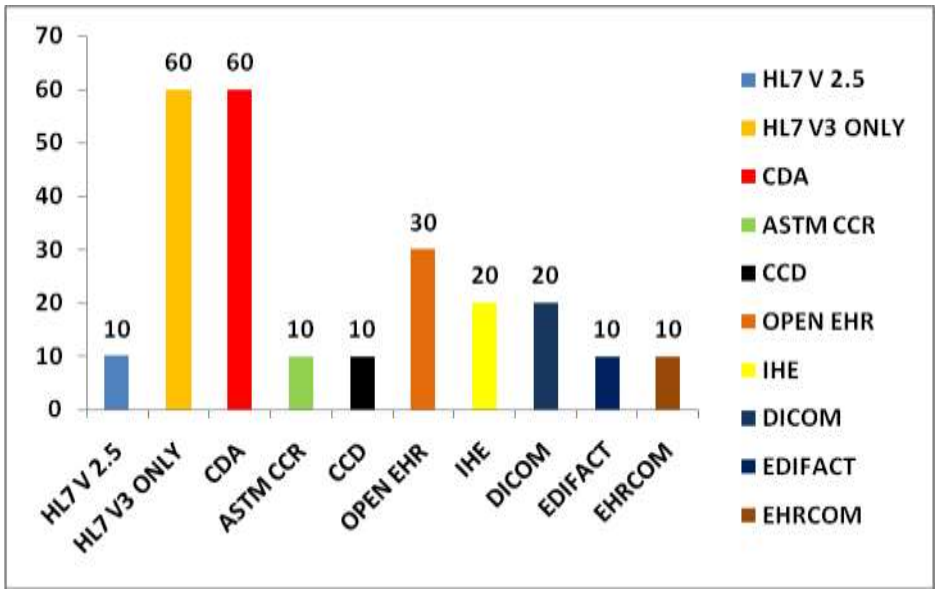


Figure 3: Country-wise Standards Adoption Statistics

5.1 **Recommended Healthcare IT Standards (for India) is given as below using is this recommendation we are created our own EHR format**

Table 3: EHR format for India

Name	**Class**	**Comments**
Phase 1		
UHID	Unique Health Identifier – to act as Patient Identifier	UID as a unique (primary or secondary) patient identifier. The UID should be used to identify a particular patient across all organizations (and their EMR systems); Aadhar number is recommended for use in EMR as eitEHR the primary or secondary, wEHRe the primary is an internal unique health identifier used by the healthcare provider organization.
XML (Extensible Markup Language)	for data capture, integration and presentation layer	To access via SOAP-simple object access protocol
CCD (HL7/ASTM)	Clinical Data for Inter Department documents (the CDA CCD)	Likely to be used for exchanging the clinical documentation between two EHR solutions both within an organization and outside.
RXNORM/ATC Pharmacologic-TEHRapeutic Classification/NDC - national drug classification, FDB-first databank (USA) Indian Drugs – MIMS/CIMS from CMP medical	Medicines	Needs to be researched as tEHRe is no universal drug reference database. The WHO Drug Dictionary ATC – anatomic tEHRapeutic classification) may be a good choice to begin with
Dictionary of Medicine & Devices, UK	Medicines & Medical devices	UK standard used in NHS includes devices & drugs

Name	Class	Comments
LOINC	Clinical Observations Laboratory	Published and maintained by the Regenstrief Institute, USA, this is a universally accepted code for laboratory observations.
HL7 V2.x	Messaging	Propose V2.3
HL7 V3.0 RIM	Reference Model Information	As this version is being superceded by FHIR from HL7, it would be preferable to adopt FHIR instead of V3.0 RIM
DICOM 3.0-2004	Medical Images	The latest version
CPT 4 or 5, US	Procedure classification & TEHRapy	As this will involve paying a licensing fee, this is optional
OPCS4, UK	Procedure classification & tEHRapy	
SNOMED-CT	Clinical Terminology	Provide comprehensive clinical granularity, used to capture problem list, allergies, diagnosis, procedures etc. – will immensely aid in clinical analytics, clinical decision support systems, automated clinical care pathway management systems, support evidence based practice etc
WHO ICD 10	Disease classification	WHO is actively working with IHTSDO to converge SNOMED-CT with ICD
WHO – PCS	Procedure coding system	
WHO – ICF	International classification of functioning, disability health &	
Phase 2		
DSM	Psychiatric conditions	Diagnostic & statistical manual of mental disorders
NIC/NOC/NANDA	Nursing interventions classification	
CDT 2, US	Dental Procedures	

Name	Class	Comments
Unknown	AYUSH clinical terminology, treatment planning including medication details	Ayurveda, Yoga, Unani, Siddha, Homeopathy systems of medicine as distinct from the allopathic (Western) system of medicine

1. Performance Analysis of the System

For simplicity each experiment was run 100 times in crypto tool .crypto tool is one libraray file in java through which we measure performance of our algorithm as well as we can implement algorithm for comparative analysis and the average was calculated in order to eliminate the influence of possible random outlines for performance analysis we divided our analysis in two parts

- Performance analysis of AES and MD5 algorithm for different size of data size.

Performance analysis of AES and MD5 algorithm for different size of data size

As the flow chart of in figure indicate complete work flow of system first. EHR will be created and encrypted with AES and MD5 algorithm for performance analysis of AES and MD5 algorithm we have considered different size of EHR record and performed and checked it on different parameters mentioned below. We are measuring encryption time and decryption time for different file size of EHR as per table given below each file was ran for 100 times and then average of the run time was considered.

a. Encryption time

The time taken to convert plaintext to cipEHR text is encryption time. Encryption time depends upon key size, plaintext block size and mode. In our experiment we have measured encryption time in milliseconds (ms). Encryption time impacts performance of the system. Encryption time must be less making the system fast and responsive.

Table 6: Encryption Time

Sr no	File size	Time taken (MS)	Standard deviation
1	1 MB	128.4	25.68
2	10 MB	581.4	102.96
3	30 MB	1489.2	307.10
4	50 MB	4231.2	408.98

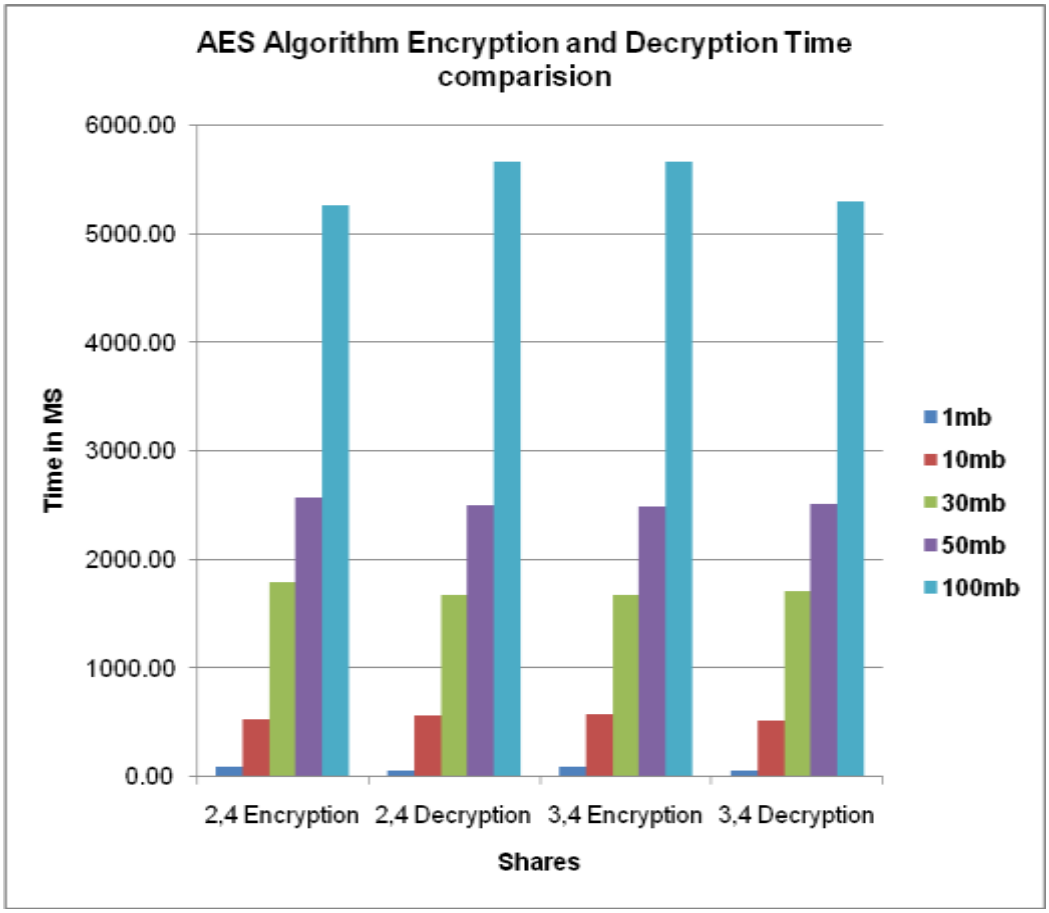
b. Decryption time

The time to recover plaintext from cipEHRtext is called decryption time. The decryption time is desired to be equivalent to encryption time to make system responsive and fast. Decryption time impacts performance of system. Inour experiment, we have measured decryption time is milliseconds(ms) on same file size used for encryption.

Table7: Encryption Time

Sr no	File size	Time taken (MS)	Standard deviation
1	1 MB	81.6	11.61

2	10 MB	570.8	139.34
3	30 MB	1539	350.80
4	50 MB	4313.11	456.71



6. Conclusion

Cloud computing has emerged out as an ideal data sharing medium to share patient data. The concept of encryption aims to safeguard the privacy of outsourced information and users queries. Sensitive attributes can be protected by encryption store them with different fragments on multiple cloud service providers. Next, encryption enhances the security level furtEHR. The projected system is a novel patient-centric framework with a set of mechanisms for information access management to EHRs kept in cloud severs. The proposed system strives to lend trustworthy and scalable cloud storage and key management at a much reduced cost. The privacy is assured by means of confidentiality constraints recitation the sensitiveness of attributes and their relationships.

Future scope

In this work if message digest value will be change we can not decrypt the key properly so unable to reconstruct record The future scope defines that identification and detection of cheater (shareholder) in secret sharing scheme using Shamir's lag ranges polynomial method more over health care Centre will be integrated with smart device for quick communication

The future scholar can explore their work for creation of EHR on basis of real time

data (like pulse rate, sugar level, pulmonary function)

7. References:

1. Li, D., Yang, M., Zhang, X., & Jin, H. (2017). A secure and efficient EHR sharing scheme based on attribute-based encryption in cloud computing. Future Generation Computer Systems, 67, 433-445.
2. Mo, Y., Li, F., & Zhu, Y. (2018). A novel EHR sharing system based on blockchain and attribute-based encryption in cloud computing. Journal of Medical Systems, 42(8), 141.
3. Singh, A., Chatterjee, J. M., & Mukherjee, J. (2016). Secure and privacy-preserving EHR sharing scheme using cloud-based attribute-based encryption. International Journal of Medical Informatics, 94, 103-115.
4. Choudhury, O., & Garg, S. (2016). Ensuring privacy and security of EHR using two-level encryption in cloud computing. Journal of Cloud Computing: Advances, Systems, and Applications, 5(1), 10.
5. Wang, Q., Zhang, Y., & Zhang, X. (2016). A secure and efficient EHR sharing system based on multi-authority attribute-based encryption in cloud computing. IEEE Access, 4, 3070-3079.
6. Zou, D., & Wang, S. (2015). A secure EHR sharing scheme based on identity-based encryption in cloud computing. In Proceedings of the 2015 International Conference on Cloud Computing and Big Data (CCBD), 69-74.
7. Wang, G., Zhang, Y., & Zhang, L. (2015). A secure and efficient EHR sharing scheme based on lightweight attribute-based encryption in cloud computing. Journal of Medical Systems, 39(12), 182.
8. Wang, H., Zhang, H., & Zhang, Y. (2014). Secure EHR sharing based on ciphertext-policy attribute-based encryption in cloud computing. Journal of Medical Systems, 38(12), 148.
9. Jiang, X., Duan, H., & Xie, Y. (2014). A lightweight EHR sharing scheme based on attribute-based encryption in cloud computing. In Proceedings of the 11th IEEE International Conference on e-Business Engineering (ICEBE), 147-152.
10. Li, X., & Zhang, L. (2014). Secure EHR sharing in cloud computing: a patient-centric approach and issues. Journal of Medical Systems, 38(9), 101.