JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 7, ISSUE 17, 2020

A SECURE CLOUD-BASED EHR FRAMEWORK FOR THE SECURITY AND PRIVACY OF MEDICAL DATA USING HIERARCHICAL CP-ABE

Dr. Meka Anuradha[1], Mrs.P.Srividdhya [2], Rakheeba Taseen [3] Devika Rani Roy [4].

[1]Associate Professor, Department of Computer Science and Engineering, St. Martin's Engineering College, Survey no. 98 & 100, Dhulapally, Secunderabad, Telangana-500100, India. manuradha595@gmail.com
[2]Assistant Professor, Department of Electronics and Communication Engineering, Mailam Engineering College, Mailam, Villupuram district, Tamil Nadu-604304,india. professorsrividdhya@gmail.com
[3]Assistant Professor, Departmenrt of Information Science and Engineering, HKBK College of Engineering, No.22/1, Opposite to Manyata Tech Park Road, Vyallikaval Society, Govindpura, Nagavara, Bengaluru, Karnataka-560045, India. rtaseen2017@gmail.com
[4]Assistant Professor , Department of Information Technology, K. C. College of Engineering and Management Studies and Research (Affiliated to Mumbai University), Sadguru Gardens, Mithbunder Rd, Near, Kopri, Thane, Maharashtra 400603, roydevika1992@gmail.com

Received: 22.04.2020 Revised: 24.05.2020 Accepted: 19.06.2020

ABSTRACT: The growing technological world health care industries are moving towards adaptation of software development and cloud storage. The rapid growth and high demand are the two important factors for cloud-based Electronic Healthcare records. In this paper, we propose flexible, reliable, secure and low-cost privacy preserved cloud environment for healthcare industries. The cloud-based EHR framework is used for data security, privacy of patient date, accessibility and overall performance. Hierarchical Cipher text Policy – Attribute Based Encryption method is proposed for encrypting healthcare information and stored in cloud. This paper provides Hierarchical CP-ABE based Cloud EHR framework model. The proposed framework will gives effective decision making and analyze existing records of users. The paper motivates and explains cipher text policies and attribute based authentication method for analyzing healthcare data and experiments are done for effective implementation of cloud based EHR framework.

KEY WORDS: Cloud Computing, Electronic healthcare records, Cipher test policies, Attribute based Encryption, Security

I. INTRODUCTION

The healthcare industries are changing conventional method into technology based record and maintenance for monitoring patients. According to 2019 WHO survey, today the world are facing high rate health issues and 70% of people regularly visiting hospital for several reasons. Healthcare industries are required major demand for storing and analyzing patient records. Each time they need to keep record and update the status. There is lack of availability in hospital information system and they are not ready to change rapidly [1]. It requires technical and administrative support activities. The healthcare activities are needed to monitor and full control given to user and administrator with security enabled customization policies.

The success story behind this advanced cloud based record maintenance system is provides review of patient record and keep track all the status. This kind of electronic methods enable comparative studies and effective decision making capabilities [2]. The selection of storage and software is the toughest process and leads security as major concern. It depends and suitable for all the users such as healthcare providers, doctors, patient, nurses, medical shop and administrator. Also different customization and access privileges are need for each kind of users[3].

According to U.S healthcare, the all the healthcare records are stored in electronically and improves the quality in healthcare services. Cloud computing platform is used for cost effective services including storage, administration, computation, reliability, data management, virtual provisioning and security [4][5]. Security and privacy issues are important factors to manage cloud based EHR system. Many of the healthcare industries are provided legal issues, insurance policies and accountability. It is a trusted system and providers may enable access controls in all the places.

ISSN- 2394-5125 VOL 7, ISSUE 17, 2020

The development cloud computing technologies which enables platform, storage and infrastructure based computing feature are major concern for implementing security. The IT and ITeS are ruling the world and it is increased day by day [7]. Clinical and Patient information are stored in EHR means it reduces the infrastructure maintenance. The sharing of healthcare information via internet leads the security issues. Our proposed method provided attribute based encryption for securing information. This paper organized as follows, section 2 give related works, section 3 explain various methodology and formulas for implementing cloud security, section 4 describes experimental results and discussions.

II. RELATED WORK

Symmetric key encryption a technique is used in EHR system with the additional method of apply access control. Shuhair et al, healthcare industries use shared key for encryption and decryption. This method leads the key can be compromised and EHR record can be trapped [8]. Public key encryption is provided and RSA algorithm is applied for secure EHR storage. Shanna et al, public key infrastructure is to be maintained for distributing keys and managing encryption and decryption. The digital certificate is required for all generated data and reports. The above methods are inadequate for handling cloud based EHR and various motivations are discussed for implementing cloud based record keeping system [9].

In this literature, there is no efficient method or algorithm for recording healthcare data. We found need of interrelationship between cloud and healthcare. For implementing this, several researchers are discussed and improve the framework [10]. The solutions are needed for adoption of cloud healthcare and providers using cloud. Cheng et al, the conventional healthcare system has been related by electronic based record keeping system [11].

The system provides efficient infrastructure and keep record of all date. The cloud based electronic healthcare provides cost effective, scalable and flexible solutions. This kind of cloud based models provides reducing maintenance cost, operational expenditure, infrastructure implementation, licensing and general issues [12]. In this paper provides Cipher text policy attribute based encryption method is used for secure handing healthcare data electronically. The major contributions are secured electronic healthcare records and cloud based accessing system.

III. CLOUD BASED ELECTRONIC HEALTHCARE SYSTEM

Cloud based electronic healthcare system has following contributions, 1. Provides secure, cost effective and privacy preserve cloud framework for implementing healthcare recording system. 2. Encryption and Decryption methods are applied for securing information in the cloud. 3. Achieve scalability and reliability in each data exchange stage. 4. Universal access through internet and access privileges are enabled for all users. 5. Provides effective decision making solution and multiuser authentication feature. 6. Two use trusted mechanism for managing cloud and centralised certificate authority for security concern. This method majorly focuses on security requirement in cloud environments.

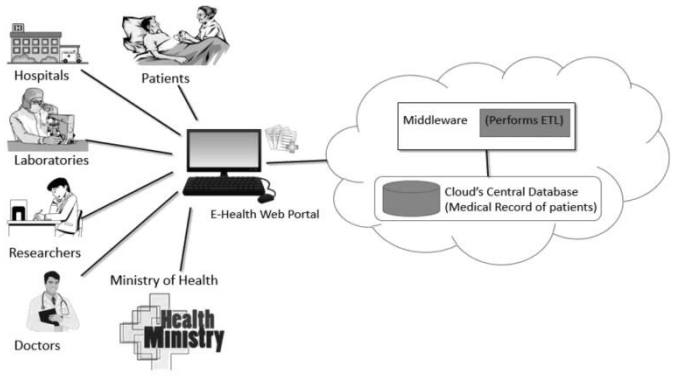


Fig 1: Cloud based EHR System

A cloud based framework is designed for recording healthcare data electronically. This method will allow decision making and benefit for all kind users like doctors, patient, researchers, government, laboratories, medical shops, etc. Figure 1 shows the proposed model and which has major entities. These entities are interacting with directly/indirectly to EHR framework. Nowadays government is also recording electronically using e-governance method. This method is responsible for reliable, highly effective and safe cloud environment. The proposed framework uses cloud based model and suitable for all type for health care industries.

ISSN- 2394-5125 VOL 7, ISSUE 17, 2020

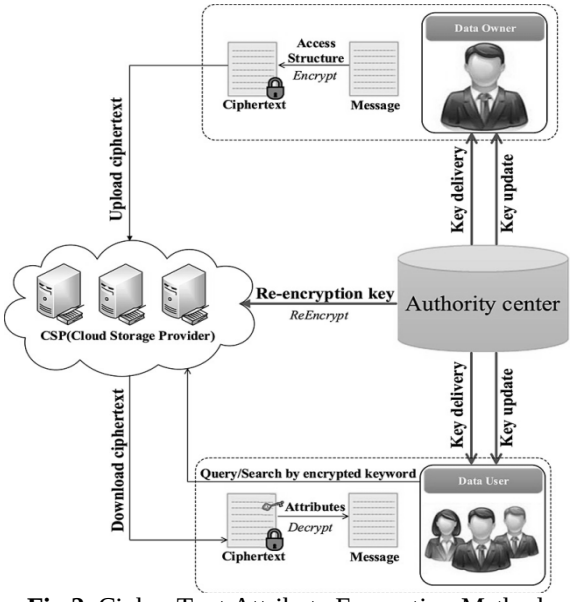


Fig 2. Cipher Text Attribute Encryption Method

Figure 2 shows that, cipher text attribute based encryption method for generating key pairs and query generated for authority center. In this model Patient, Healthcare industries, Cloud based EHR are three important cornerstones.

a). Patient: For each patient identification number generated based on their primary data. Using that ID, patient can track their records. Each patient, history record is created and stored. It is fully secured and provides access policy using attributed based encryption method.

b). Healthcare Providers: This mode available for those who are all working healthcare or set of community peoples. Each member can access by using their ID or Patient ID. It is customized portal so the people can access their privileges like doctors, nurses, administrator, pharmacy, surgeons and specialist category. It is trusted service and secret key shared for each transaction. Encryption and Decryption process are done by same key.

c). Trusted Authority: The role of trusted authority is responsible for interaction, authentication and issue certificates. The key pair generated using this module and handling all cryptographic operations.

Procedure : Cloud based HER

The proposed cloud based EHR consist of following implementations

Case 1: Data Repository – storing encrypted files in EHR and generated authenticated access policy reports

Case 2: Each access policies has certain attributes and key pair values to accessing the records

Case 3: Set of computing resources are needed for efficient key management and web based portal access

Case 4: Keep record all the accessing modules and everything internet based access modules

Case 5: Backup and IDS provided for security and reliability

Hierarchical Cipher text Policy – Attribute Based Encryption

Proofing Sequence

Step 1: The digital certificate issued to all healthcare industries and enrolment process in monitored by government or trust authority

Step 2: Proofing is set all requested services and issue the ID for all type users

Step 3: Healthcare Industry monitor the request and generate key pair. Access privilege issued to all users

Algorithm

Step 4: Setup K-Key values – Generate Public key (P_k) and master key (M_k)

RSA based Elliptic cryptography method is used for generating public key and Diffie Hellman exchanging key. Input 164-bit key and 1024-bit master key. $K = x^2 + ax + b$ over P_k is the set of solutions $(x,y) \in K$

Step 5: Create Attribute Authority (P_k, A_a) – This is used to find the identifier of all user and generate attribute key for accessing record. Here access policies given to all kind of users.

Attribute key Generator (P_k, A_a, ID_x) is created using following method

ISSN- 2394-5125 VOL 7, ISSUE 17, 2020

G1 and G2 are cyclic groups of prime order P_k; K generator of G1 & G2 bilinear map and Bilinearity: ∀ P,Q ∈ G1, ∀ a,b ∈ Z ∗ p, e(aP, bQ) = e(P, Q) ab

Step 6: KeyGeneration (K, S) – The key pair is generated via private key and AttributeKeyGenerator. • Encrypt(P_K, M, A_a): This encryption models is used to find message and key pair. Based on this cipher text is created and stored.

Decrypt(P_K, C, S_K): This decryption stage is used to convert cipher text into original message. Delegate(S_K, S_o): Delegate is used to generate secret key pair for set of attributes when the different user can access the HER

d). Cipher text policy – attribute based encryption method is flexible and fine-grained approach to access healthcare records. In this method, if secret key compromised means EHR can be decrypt the key and it is protected the record.

IV. EXPERIMENTAL SETUP AND DISCUSSIONS

a).Key management

The Attribute Authority method is used for key generation and distribution. This model provides public and master key setup. The set of key pair is generated and associated with their attributes. The distinct key pair is stored and randomly generated with expiration period. The key store and generation process are handled by Attribute Authority model. Secret key generation is done securely and check system parameters. In this model, there is no need of backward secrecy and in case new inputs it is automatically keep record. Access policies are managed and associated with all users. In cloud-based EHR model provided ease of access during emergency situation.

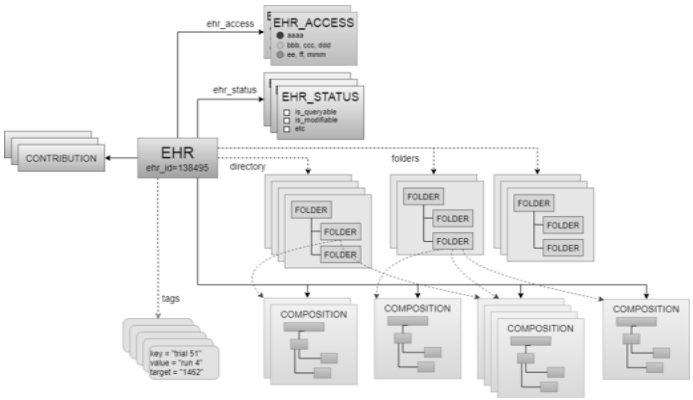


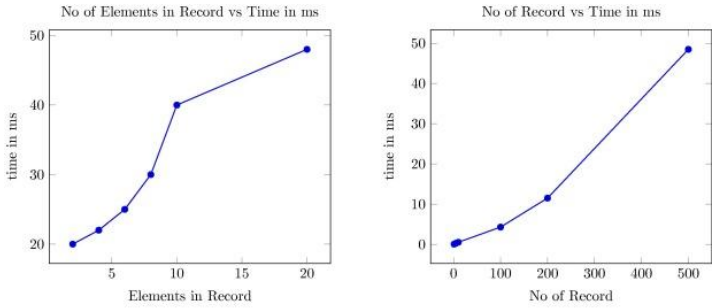
Fig 3: Key management and evaluation

b). Revocation Policies

This Cloud based EHR requires forward and backward policies to access EHR related information. The key pairs accessed by user when they required. The encryption and decryption process are monitored and re-distributing process also taken care.

The experiments are done VMs in Fedora 14 with 2GB RAM and hosted in Intel i3 2.45Ghz processor. The CP-ABE implementation is done in VM Cloud and 164-bit elliptic curve group applied and 1024 bit key pair generated. The efficiency is obtained from input of five images like 1MB, 5MB, 10MB,20MB and 30 MB and encrypted using ten attributes of key pairs. Each attributes can be set by access structure and decision model is set each pair. The encryption and decryption time is calculated using single key pair and process done by repeatedly.

ISSN- 2394-5125 VOL 7, ISSUE 17, 2020



(a) No of Elements in Record vs Time in ms (b) No of Records vs Time in ms

Figure 4: No. of records and attribute encryption and decryption

The above figure 4 shows that the EHR systems can be test 2MB dataset and encrypted below 2.5ms accordingly and same as follows for decryption. The above results shows time performance and belongs to Attributes based Encryption. The same result can be analyzed by using storage modules. This case storage overhead can be found using different intervals such as 10MB to 50MB.

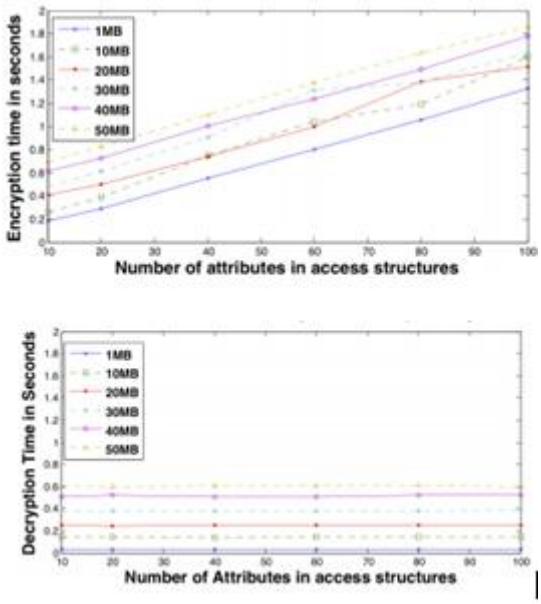


Fig 5: Storage overhead with respect to time and access structure

The above results are analyzed by using Redshit model and storage overhead is negligible in cloud based-electronic healthcare record system. It is suitable for all type cloud service providers. The EHR system manages health record and authorized by administrator. The different EHR model is available but our proposed model provides secure access and attribute based encryption model for data accessing. The access privilege is another factor in our model and we can make effective decision from recorded information. The EHRs are stored encrypted data and patient can upload their entries with their policy rule. Also we can find metadata entry such as location, time, usage, report generation and certificate authority at time.

CONCLUSION

In this work, we proposed Cipher text-Attribute based encryption method for securing healthcare records electronically in cloud. This is hierarchical based storage mechanism and it provides privacy, secretary and access policies. This is multi-authority model which enables access control list for high level integration, interoperability and distributed networks. The EHR records are accessed by patient, healthcare, doctors, pharmacy and researchers. The attribute authority is used for managing all key pair and work independently. There is no computational delay and overhead issues in this model. Multifactor authentication model is applied for treatment and services. This proposed model is applied for all type of user and future it is implemented for real world environments.

REFERENCES

[1] Sanaa Sharaf and Nidal F. Shilbayeh, A Secure G-Cloud-Based Framework for Government Healthcare Services, IEEE Access Special section on Healthcare Information Technology for the

ISSN- 2394-5125 VOL 7, ISSUE 17, 2020

Extreme and Remote Environments, 2169-3536 2019 IEEE, Digital Object Identifier 10.1109/ACCESS.2019.2906131

[2] M. Parekh and B. Saleena, ‘‘Designing a cloud based framework for healthcare system and applying clustering techniques for region wise diagnosis,’’ Procedia Comput. Sci., vol. 50, pp. 537–542, Jan. 2015

[3] S. Alshehri, S. Radziszowski, and R. K. Raj, ‘‘Designing a secure cloud-based EHR system using ciphertext-policy attribute-based encryption,’’ in Proc. Data Manage. Cloud Workshop, Washington, DC, USA. 2012, pp. 1–5.

[4] P. Junod and A. Karlov. An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies. In Proceedings of the 10th Annual ACM Workshop on Digital Rights Management, DRM ’10, 2010.

[5] Suhair Alshehri, Stanisław Radziszowski, and Rajendra K. Raj, Designing a Secure Cloud-Based EHR System using Ciphertext-Policy Attribute-Based Encryption, (In press ACM)

[6] J.Abinaya , R.Ranjitha, S.Swetha and S. Manikandan, "An Efficient Identity Based Group Key Distribution Scheme for Client Side Security in Web Applications,"Einstein International Journal Organization (EIJO), Volume – 1, Issue – 1, Page No. 49-53

[7] M. Masrom and A. Rahimli, ‘‘A review of cloud computing technology solution for healthcare system,’’ Res. J. Appl. Sci., Eng. Technol., vol. 8, no. 20, pp. 2150–2155, 2014.

[8] S. Manikandan, K. Raju, R. Lavanya, R.Hemavathi, "Energy Efficiency Controls on Minimizing Cost with Response Time and Guarantee Using EGC Algorithm",International Journal of Information Technology Insights & Transformations, Vol. 3, No. 1, 2017.

[9] N. Khan and A. Al-Yasiri, ‘‘Identifying cloud security threats to strengthen cloud computing adoption framework,’’ Procedia Comput. Sci., vol. 94, pp. 485–490, Jan. 2016

[10] D. Hankerson and A. Menezes. Elliptic Curve Cryptography. New York, NY, USA: Springer, 2011

[11] G. Wang, Q. Liu, and J. Wu, ‘‘Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,’’ in Proc. 17th ACM Conf. Comput. Commun. Secur., 2010, pp. 735–737.

[12] S Manikandan, "An Adaptive Lsb Pattern Substitution For Detecting Bio-Metric Inputs", Applied Science Reports, Progressive Science Publications, E-ISSN: 2310-9440 / P-ISSN: 2311-0139, DOI: 10.15192/PSCP.ASR.2018.22.1.2731, Volume 22, Issue 1, pp. 27-31, 2018

[13] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy (SP), May 2007, pp. 321–334.

[14] Z. Yu, C. Wang, C. Thomborson, J. Wang, S. Lian, and A. V. Vasilakos, ‘‘A novel watermarking method for software protection in the cloud,’’ Softw.-Pract. Exper., vol. 42, no. 4, pp. 409–430, 2012.

[15] M. Li, ‘‘Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,’’IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013