International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Need of Security in Health Care Automation: Survey Report

Soniya Raghu[1], Amit Saxena[2], Kaptan Singh[3]
[1]*PG Scholar,* [2, 3]*Associate Professor, CSE Department, Truba Institute of Engineering and Information Technology Bhopal, India*

Abstract: ***Cloud computing goals at providing security measures with the aim of pay-per-use function, where users have to pay only for what they use. Security models in cloud are based on model of authentication like data protection model and data access management model. Storing on cloud is the big issue due to the security of data and storing of data. Many researches have provided many solutions and is still continued. Presented work focused on privacy protection of electronic medical records in cloud environment. Therefore, data needs to be protected from intruders and attackers and should have private storage. For privacy preservation some techniques are used in proposed work, these techniques are RBAC, and ABAC, which establishes a mitigation approach called RABAC, access matrix with RABAC is applied for the advancement and improvement in preserving electronic health records.***

Keywords: Data security, Electronic hospital record, ECC, BLOWFISH, Access Matrix, RABAC.

I. INTRODUCTION

Cloud computing falls into different categories of service layer and deployment models. These service layers are called as cloud computing stack due to its design of layers on top of one another. After it comes up with deployment model, it serves with the feature of storing and using resources individually or through organizations or by community. Privacy is the specific process for isolated environment. Security features are implemented for security purpose of applications. For establishing trust, important principles are confidentiality, integrity and authentication.

Patient's data is exchanged between different entities effectively through electronic health services. These entities are doctors, technicians, nurse, insurance companies etc. Data owner outsource there data on cloud and their contents are store and represented as a health record for sharing in cloud environment. Cloud computing models with great possibilities for flexible and management of information exchange. Serious challenges are possessed in cloud due to the issue of confidentiality, authentication, hashing and access control which obstruct the health services in cloud. For instance, exchange of information between communicating entities worst the security issues. HIPAA policy is a primary policy to preserve unauthorized access in cloud. Problems related to these issues address the security of cloud and security of outsourced data. For storing sensitive data on cloud by data owner, cryptographic approach is also enough.

A. Advantages of EHR

1) Stores accurate data.
2) Captures current state of patient every time.
3) Does not need to track previous records of patient.
4) Decreases paper work.
5) Does not replicate data by reducing modification of data.
6) Decrease processing time for billing and generates accurate bill.

Figure 1: Advantages of EHR

©IJRASET: All Rights are Reserved

II. RELATED WORK

R.Manoj et al. In[1] implemented a system which replaces AES technique by using Attribute based encryption technique. Because of the use of AES, fine grained access control is not good for system also with the increase in file size processing time increases. This issues are overcome using ABE technique and is used for encryption of records. ABE uses Key policy (KP-ABE) encryption scheme and Multi authority (MA-ABE) scheme for the encryption of identifiers. Key policy based is used in public domain to manage secret key for personal domain in Multi authority.

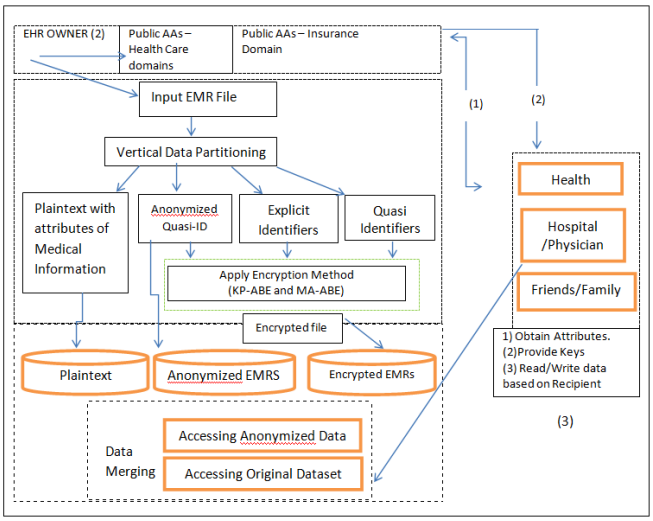

Figure 2: Existing Work by R.Manoj

M. N. Shrestha et al. In[2] suggested security and privacy in accessing data efficiently with encryption and authentication algorithm. Numerous solutions have been proposed by many researchers in this field with providing integrated solution of encryption and authentication.

Z. Liu [3] research about data storage in cloud by aiming at secure storage in public verifiable cloud. Here, privacy-protection method Orutha is used on the basis of ring signature. For auditing data in cloud, authentication and computational process is used which does not retrieve data sets.

R. Ranchal [4] introduces a dynamic capacity system with heterogeneity awareness called as harmony. Which optimize energy saving and minimize scheduling delay in data centers. Heterogeneity for both the workload and physical machine are needed to implement and fully researched.

III. PROBLEM DOMAIN

Traditional system works as taking input source and then splitting data into chunks, after that data is divided into chunks, key is generated for every chunk. Then, the chunk data are encrypted using key pairs with forming C1, C2, C3 ...Cn cipher chunks. These chunk cipher text are stored and then there key pairs are identified as C1K1, C2K2 ...CnKn. Using these key pairs chunks are decrypted.

This system works till one end but with the change in trends it fails to achieve privacy. Due to the confidentiality of data, its protection is must because of the insecurity of sensitive Electronic Hospital Record, it is sensitive to mislead the information so privacy of the data is not safe.

ABE Attribute Based Encryption concept, which is used in the existing work, suffers with some challenges like:

1) Revocation
2) Escrow
3) Coordination

Non-efficiency and non-existence are the two drawbacks with which ABE suffers. These drawbacks are for the mechanism of attributes.

Existing system uses KP-ABE & MA-ABE. KP-ABE is the prolonged form of traditional ABE. KP deals with the cipher text that are accompanied with the attributes for decryption. It has the drawback that it does not determine is who will decrypt the data which is encrypted. This scheme works only for descriptive attributes.

©IJRASET: All Rights are Reserved

IV. PROPOSED APPROACH

Proposed Approach will implement a secure and preserved system for the safety, confidentiality and authentication of stored data. Using access control matrix describes the solution for insecure and sensitive data of electronic hospital record. Data source taken is from Electronic Hospital Record, patients' health data is stored in it, which is confidential and is insecure and due to this sensitivity information may misled. Therefore, implementation is required for preserving health data from intruders and maintains privacy of health data. Using access matric with attribute based access control and role based access control proposed approach will be implemented.

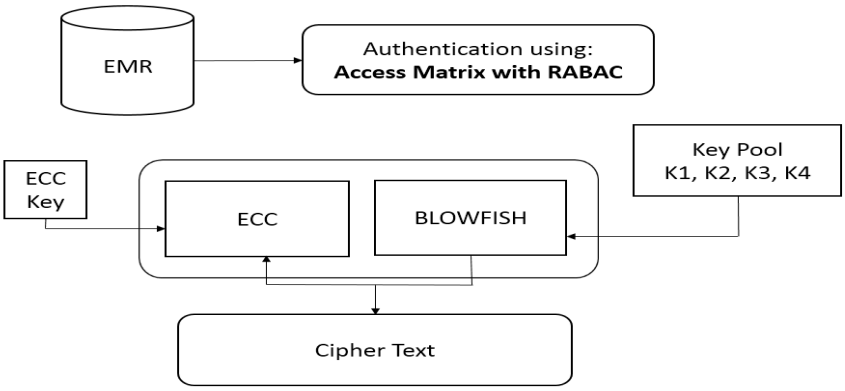

Figure 3: System Architecture

Attribute based and Role based both techniques are combined to form RABAC called as Role-Attribute based access control and this access control is used as a matrix. Forming so under called as Access Matrix with RABAC. Role of access control is to update every operation of the one who can access the data and which role is assigned to which attribute. Mapping is done for role and attribute, where not every role is assigned with every attribute.

The sequence for the proposed work where the database consisting of Electronic hospital record, which is sensitive to misled for the privacy protection of that sensitive data verification process is applied for the purpose of authentication. In this process user first login, and then login request is verified, verification is done for authenticating the user id and password. For achieving confidentiality, ECC and Blowfish algorithm are used. Now, for accessing data, access control check the role and attribute of user. From the RABAC Table, every role and every attribute is checked for the purpose of operations to hold. This role-attribute table is used for the operation update, that who can access which role and attribute. Not every user has permission to access every attribute.

V. ALGORITHMS

A. Elliptic Curve Cryptography

ECC stands for Elliptic Curve Cryptography, this technique works on asymmetric key which works as public and private key cryptography over finite fields. ECC is used for key generation, digital signature and other responsibilities. Public and private key are used for encryption and decryption process. It works on large prime factors with public and private key cryptography. Elliptic curve cryptography serves with the advantages of small key size, transmission and reduce storage, also with the level of security.

B. Blowfish

Blowfish is a symmetric key algorithm, where encryption and decryption of message is performed using same key. It uses a block size of 64 bit. Encryption and decryption

VI. CONCLUSION

Proposed work deals with the privacy preservation of health records and contributes its study towards secure storage of data in cloud environment. Security and privacy is the important concern in every fields, and if talking about outsourced data than the issue becomes more complicated. So, a framework for preservation of privacy is based on multi-authority and key-based encryption. Where, Multi-authority works for public domain and Key-based works for personal domain. They together combined to form secure data access for user.

©IJRASET: All Rights are Reserved

REFERENCES

[1] R. Manoj, Abeer Alsadoon, P.W.C. Prasad, “Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud,” 2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering.
[2] M. N. Shrestha, A. Alsadoon, C. P. Prasad and Houran, "Enhanced e-Health Framework for Security and Privacy in Healthcare". IEEE, pp. 75-79., 2016
[3] Z. Liu, J. Weng, J. Li, J. Yang, C. Fu and C. Jia, "Cloud-based electronic health record system supporting fuzzy keyword search" Soft Computing, vol. 20, no. 8, p. 3243–3255, 2016.
[4] R. Ranchal, “Cross-domain data dissemination and policy enforcement,” PhD Thesis, Purdue University, 2015.
[5] S. Suresh, "Highly Secured Cloud Based Personal Health Record Model". International Conference on Green Engineering and Technologies (IC-GET), pp. 1-4, 2015.
[6] J. J. Yang, J. Li and Y. Niu, "A Hybrid solution for privacy preserving medical data sharing in cloud computing". Future Generation computer systems, vol. 43, no. 44, pp. 74-86, 2015.
[7] S. Lu, R. Ranjan and P. Strazdins, "Reporting an experience on design and implementation of e-Health systems on Azure cloud". CSIRO Computational Informatics., vol. 27, no. 10, pp. 2602-2615., 2015.
[8] B. Bhargava, “Privacy – preserving data dissemination and adaptable service composition in trusted and untrusted cloud”. NGCRC Project Proposal, CERIAS, Purdue University, Aug.2015
[9] Y. Chen, J. Lu and J. Jan, "A Secure EHR System Based on Hybrid Clouds". Journal of Medical System, vol. 36, no. 5, p. 3375–3384, 2014. J. Clerk Maxwell, a Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.
[10] B. Coats and S. Acharya. S, "Bridging Electronic Health Record Access to the Cloud". IEEE 47th Hawaii International Conference on System Science, pp. 2948-2957, 2014.
[11] K. Nagaty, "Mobile Health Care on a Secured Hybrid Cloud". Cyber Journals, vol. 4, no. 2, 2014.

©IJRASET: All Rights are Reserved