ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 5 , May 2018

Hybrid Access-Control and Cryptography Model for Preserving Privacy of Electronic Medical Record

Pallavi Kala Anand Rajavat

P.G. Student, Department of Computer Science, Shri Vaishnav Vidhyapeeth Vishwavidhyalaya, Indore, Madhya Pradesh, India
Professor, Department of Computer Science, Shri Vaishnav Vidhyapeeth Vishwavidhyalaya, Indore, Madhya Pradesh, India

ABSTRACT: Multi variant data are stored in EMR, consisting of patient's personal and medical history. Medical history like laboratory reports, demographic data, billing data and other test reports. Personal details like name, weight, gender etc. are the attributes stored in medical records. 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 and these techniques are AES and MD5, which establishes a mitigation approach for the advancement and improvement in preserving electronic health records.

KEYWORDS: Data security; Electronic medical record; AES; MD5;Privacy

I.INTRODUCTION

EMR, Electronic Medical Record or Electronic Health Record (EHR), is the collection of records of patients and the health detail of a person which is stored through electronic medium in digital form. Sharing of these records can be possible in different health care centers through the medium of networks and other exchanges. Data stored in EMR is a multi variant data with medical history of patient, laboratory test reports, demographic data, with persons personal information like age, name, gender, weight etc., billing data etc. are stored in electronic health record.

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 there 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 authentication and access control which obstruct the health services in cloud. For instance, exchange of information between communicating entities worst the security issues. Mechanism of authentication and access control are not properly defined in cloud environment. A safe electronic health services solution is required for the act of HIPAA called as Health Insurance Portability and Accountability Act. This 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 [2] [3] [5]. For storing sensitive data on cloud by data owner, cryptographic approach is also enough. Nevertheless, data exchange is required between health care providers and patients. For this secure and safe data communication is addressed on the basis of two entities:

1. How to authenticate with transferring entities?
2. How to manage communicating entities?

For the first entity a secure, safe and accurate authentication is required for authorized entities for the preservation of user information. This protocol for authentication permits user access on the basis of user policies. Second entity that is the second concern, traditional mechanism for access control [6] is not applied in cloud environment, as they suppose that servers belonging to the same domain are completely trusted with control policies. Thus, cloud environment posses

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 5, Issue 5 , May 2018

that servers are user friendly domain and hence, to protect sensitive data unauthorized access must be controlled. In real time health care services, security are the biggest challenge.

Benefits of EMR:

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

Privacy in EMR:

The information related to health care can be threated by the following ways:

- Intruders that are the human threats, can be hacker.
- Threats through natural disasters like earthquakes, fire etc.
- Technical issues and failures like damage of system and crashing.

II. SIGNIFICANCE OF THE SYSTEM

This paper mainly focused on some mitigating approach and diagnosing the existing work. Objective of this work is analyzed as:To simulate the mapping of role and attribute based access control.. To diagnose the issue of information mislead because of the insecure and sensitive information.. It determine which roles can be accessed by which attributes.. For privacy maintenance the complete work is contributed.ABAC and RBAC are combined to form RABAC.

III. LITERATURE SURVEY

The literature survey describing the working of algorithm and techniques used in this paper and also the mitigation approach discovered, explaining the methods evolved for the improvement of basic versions.

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.

Y. Chen et al. In[2] proposed “A Secure EHR System Based on Hybrid Clouds”. Concluded about security requirements in cloud for the protection of health records. Security requirements like availability, integrity, confidentiality, and privacy should be achieved. Author explained that due to heavy data, need of cloud is required, which stores this large data and share it globally in a useful manner in health industry.

J. J. Yang et al. In[3] introduces “A Hybrid solution for privacy preserving medical data sharing in cloud computing”. Author proposed a hybrid solution to ensure data security, reliability and integrity for secure access of data. Author created this hybrid solution by integrating statistical and cryptographic techniques.

B. Coats et al. In[4] explained about “Bridging Electronic Health Record Access to the Cloud”. Author implemented a secure system called as electronic health record system. This system fulfills the requirements of health insurance. Also

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 5 , May 2018

defines about a framework for health which is user-friendly in providing secure access to health records using hybrid deployment model of cloud.

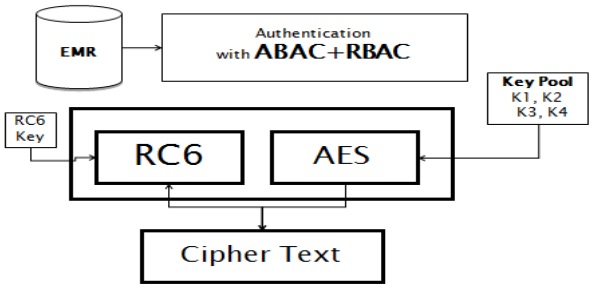
K. Nagaty et al. In[5] "Mobile Health Care on a Secured Hybrid Cloud". Described about mobile health application for cloud environment by using role based access control with mobile application and cryptography. This system helps in providing medical services.

IV. METHODOLOGY

System architecture defines the proposed work through some steps and these steps are cited below as:
Electronic medical record data is taken as a dataset. On that dataset authentication is achieved using access control techniques ABAC and RBAC. Attribute based access control and Role based access control is combined to achieve RABAC (Role-Attribute Based Access control).Authentication should be achieved because of sensitive electronic medical data.For accessing data, access control check the role and attribute of user. Every role and every attribute is checked for the purpose of operations to held.This role-attribute table is used for the operation update, that who can access which role and attribute.

PROPOSED METHODOLOGY USED:

- The study of existing solutions explore that it uses symmetric key cryptographic algorithm for encryption and attribute based access control for rights enforcement. .
- Attribute based access control allocate common permission for all role, similarly single encryption policy generates same pattern cipher text for all encryption iteration.
- Non-efficiency and non-existence are the two drawbacks with which ABE suffers. These drawbacks are for the mechanism of attributes.
- Existing system uses Key policy Attribute Based Encryption and Multi-Authority Attribute Based Encryption.



System Architecture

KP-ABE is the prolonged form of traditional ABE. KP deals with the cipher text which are associated with set of attributes and for decrypting, it is related with tree access structure. Cipher text with the set of attributes satisfies the access structure of tree then only user can decrypt the cipher text. It has the drawback that it does not determine who will decrypt the data which is encrypted. This scheme works only for descriptive attributes.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 5 , May 2018

Sample Access Matrix:

Role: Operator

1= True
0 = False

Operation	Doctor id	Disease	Investigation	Patient Id	Patient Name
Read	1	0	0	1	1
Write	1	0	0	1	1

Role: Doctor

Operation	Doctor id	Disease	Investigation	Patient Id	Patient Name
Read	1	1	1	1	1
Write	1	1	1	1	0

Sample Access Matrix

PROPOSED ALGORITHM:

Proposed algorithm is based on improved AES technique with encryption and decryption strategy. Step by step explanation of algorithm is as:

AES Encryption:

1. Sub byte transformation
2. Shift row transformation
3. Mix column
4. Add Round key
5. Key Expansion

AES Decryption:

1. Inv shift row transformation
2. Inv sub byte transformation
3. Inv Mix column transformation
4. Inv AddRound key

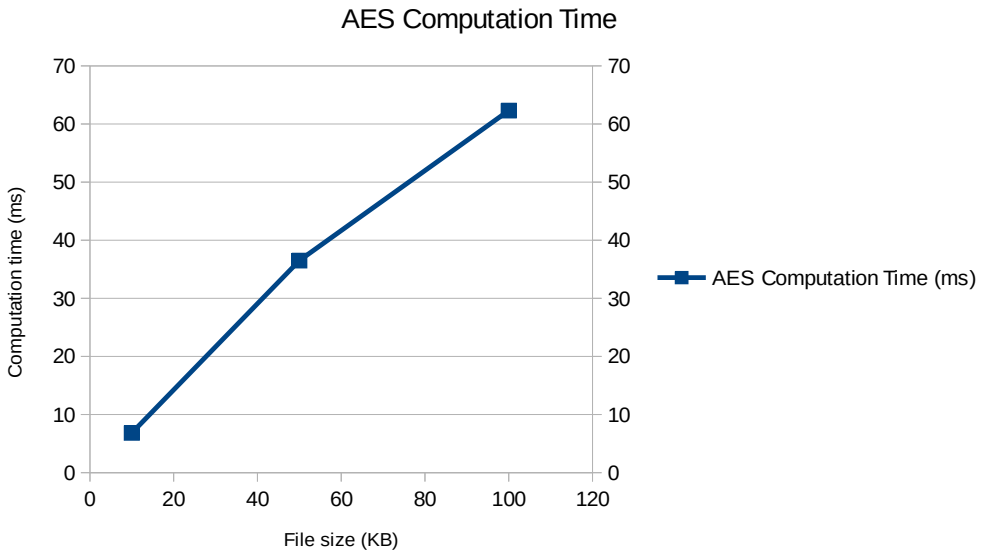
V. EXPERIMENTAL RESULTS

Result Analysis for the proposed work is defined on the basis of File size which is in KB and computation time which is in ms. Proposed work for plain text file size in comparison to AES computation time is represented in the form of graph figure in 5.1 and its table is also designed in

File Size (KB)	AES Computation Time (ms)
10	6.8392
50	36.49
100	62.309

AES Computation time for Proposed Work

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 5, Issue 5 , May 2018

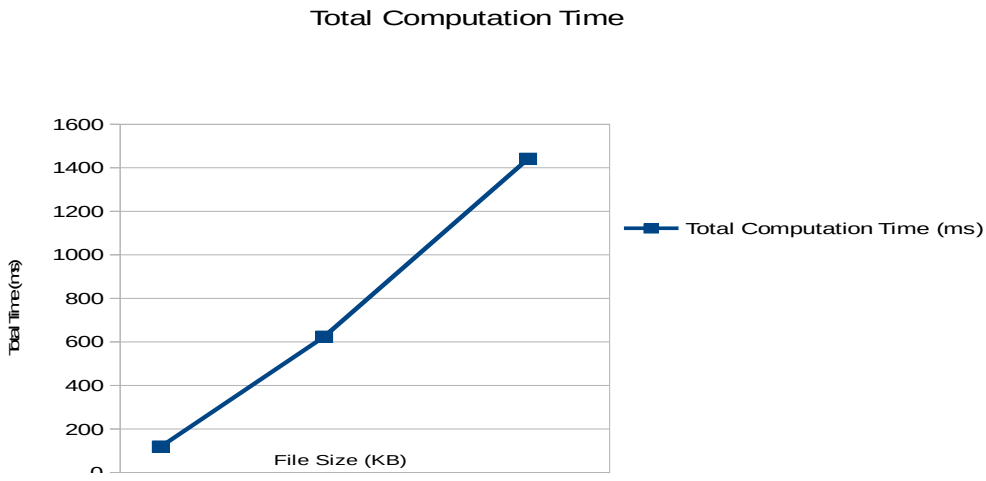


AES Computation Time graph for proposed work

Proposed work for file size in comparison to Total computation time is represented in the form of graph in figure and its table is also designed in Table.

File Size (KB)	AES Computation Time (ms)
10	118.98
50	623.71
100	1441

Table 6.2: Total Computation time for Proposed Work



Total Computation Time graph for proposed work

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 5, Issue 5 , May 2018

Comparison between proposed work and existing work is elaborated below on the basis of file size and computation time and is represented in the form of graph in figure 6.3 and its table is also designed in Table

File Size (KB)	AES Computation Time (ms)	Proposed Work
1	1593	598
5	4403	3749
100	159.93	62.309

VI. CONCLUSION AND FUTURE WORK

This proposed work deals with the privacy preservation of medical health records and contributes its study towards secure storage of data in cloud environment. Security and privacy is the important concern in every field, 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.

The complete work observe certain conclusions which are written below:
1. There is strong need to provide security and privacy to sensitive data in cloud computing. 2. Provided privacy on data at the time of storage will using improved AES encryption algorithm to avoid information leakage issue.
3. Implement MD5 to maintain originality of data.
4. Two Encryption Algorithm will not only help to improve security level but will also create confusion during cryptanalysis using different cipher text pattern.

FUTURE WORK:

- In future implementation modified AES can be replaced by Blowfish algorithm for better performance.
- Strong Authentication can be implemented in future scope.
- Image data can also be implemented in future work.

REFERENCES

[1] Agarwal S, Jain. K “Hybrid Approach For Spam Detection using Support Vector Machine and Artificial Immune System”, First International Conference on Network and Soft Computing”, Aug 2014, pg no: 05-09.
[2] Selamat, Mohammed .M, “ An Evaluation on Efficiency of Hybrid Features for Spam Email Classification”,2015 International Conference on Computer Communication and Control Technology ,April 2015, pg no : 227-231
[3] “A Hybrid Approach for Spam Filtering using Local Concentration and K- means Clustering”, 2014, 5th International Conference, pg no: 194-199.
[4] Salehi, Solmat. A “Hybrid Simple Artificial Immune System and Particle Swam Detection”, “5th Malaysian Conference In Software Engineering”, Aug 2011, pg no: 124-129.
[5]Xin Liu, ZhaojunXin, Leyi Shi, Yao Wang “A Decentralized and Personalized Spam Filter Based on Social Computing” IEEE 2014.
[6]Vipin N S, Abdul Nizar M “A Proposal for Efficient Online Spam Filtering” First International Conference on Computational Systems and Communications 2014.
[7]ZhipengZeng, XianghanZheng, Guolong Chen, Yuanlong Yu “Spammer Detection on Weibo Social Network” 2014 IEEE 6th International Conference on Cloud Computing Technology and Science.
[8] A.H. Wang, Don't follow me: spam detection in Twitter, Security and Cryptography (SECRYPT), in: Proceedings of the 2010 International Conference on. IEEE, 2010
[9] H. Gao, Y. Chen, K. Lee, D. Palsetia, A. Choudhary, Towards online spam filtering in social networks, in: Proceedings of the Symposium on Network and Distributed System Security (NDSS), 2012.
[10] F. Benevenuto, G. Magno, T. Rodrigues, V. Almeida, Detecting spammers on Twitter, in: Proceedings of the Seventh Annual Collaboration, Electronic messaging, Anti-abuse and Spam Conference (CEAS), 2010.
[11] Y. Zhu, X. Wang, E. Zhong, N.N. Liu, H. Li, Q. Yang, Discovering spammers in social networks, in: Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence (AAAI), 2012.