International Journal for Rapid Research in Engineering Technology & Applied Science
Vol 5 Issue 12 Dec. 2019
ISSN Online: (2455-4723)

Strong Security Architecture for Hospital Cloud Environment

Yashi Soni*, Mohit jain**
M. Tech Student, B.M. College Of Technology, RGTU, Indore, Madhya Pradesh, India*
HOD, Computer Science, B.M. College Of Technology, RGTU, Indore, Madhya Pradesh, India**
Yashisoni92@gmail.com, hod.computers@bmcollege.ac.in***

Abstract: Many different digital health records are observed now-a-days, likewise electronic medical record, healthcare record and health-related document system, other systems are also observed for. With the increase in data, paper work becomes cost increasing and unsecure medium but in another way dealing with electronic medium is safe for bulk amount of data with accessing of authorized person.

In this paper is implemented on Hospital Cloud Environment, which share health record with individuals who have access rights. In addition, an algorithm Rc6 and Blowfish is used to provide data security and privacy. For access control ABAC and RBAC is used.

Keywords: Cloud computing, Electronic health record, Rc6, Blowfish, ABAC, RBAC.

I Introduction

Cloud computing enables convenient, on-demand network access to a shared pool of configurable computing resources. Essential characteristics of cloud promoting capabilities including on-demand self-service, ubiquitous network access, location-independent resource pooling, rapid elasticity, and measured service. It offers computing services though three delivery models [8] including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

Cloud computing has grown as a new service model leading to the establishment of numerous cloud based data centers as cost-effective platforms for hosting largescale service applications. However, notwithstanding considerable benefits and services, the problem of security and privacy of medical data access has been significant for service providers. To mitigate this, researchers have proposed numerous techniques and methods. [9] Have proposed a practical hybrid solution for secure data access in cloud, which ensures high data reliability, security and integrity by combining statistical and cryptographic techniques.

Electronic health (e-health) services provide efficient exchange of the patient's data between different entities including nurses, doctors, lab technicians, receptionists, and insurance companies. In e-Health, the data owner represents a content provider who can store and publish health records in the cloud environment for sharing. The cloud-computing paradigm provides great opportunities to support flexible and controlled information exchange. However, authentication and access control issues in the cloud pose serious challenges that hinder the wide adoption of cloud-based e-Health services.

A strong and safe e-Health security solution that complies with Health Insurance Portability and Accountability Act (HIPAA) policies is essential to protect patients' data from unauthorized access in cloud environments. Several methods have been proposed to address the problems related to cloud security and outsourced data (e.g., [10], [11], [12]). Existing cryptographic approaches are sufficient if data owners want to just store their sensitive data on the cloud.

II RELATED WORK

R. Manoj et al. In[1] proposed the integral operation in cloud computing for health operations. Moreover, there is an issue in terms of privacy and security of medical records. Author introduces a secure hybrid electronic health record by framing two-encryption method, Multi-authority and Key-based encryption. These encryption algorithm together formed to provide secure data access.

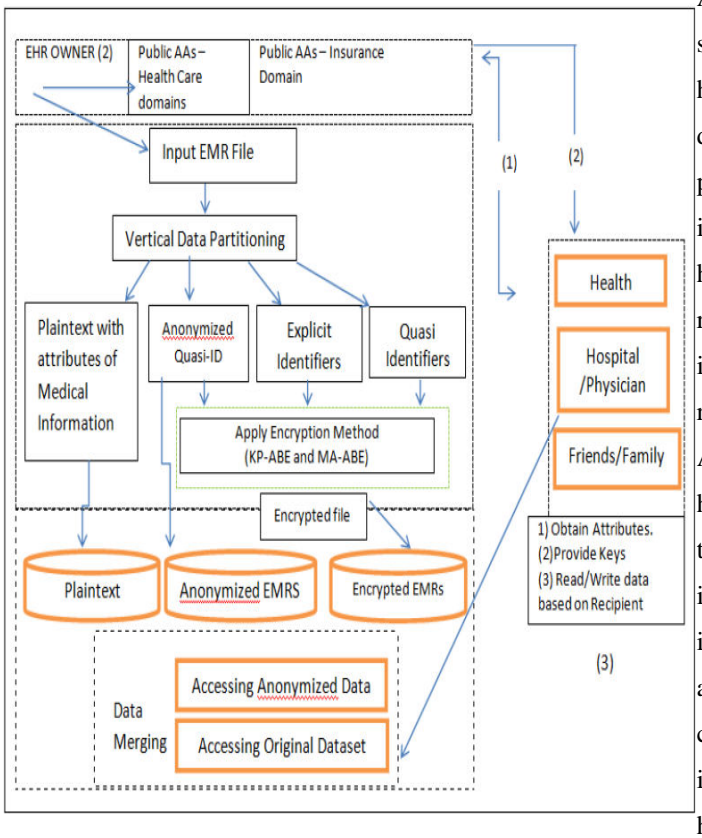

Figure 1: Existing Work

Anees Ara et al. In[2] introduces Secure Privacy Preserving Data Aggregation scheme. Frame the security model based on bilinear pairing with efficient privacy of data. For the remote health monitoring system, this framework is done. A combination of Bilinear Elgamal cryptosystem and aggregate signature is used under the condition of confidentiality, privacy and authenticity.

Mohamad Ali Sadikin et al. In[3] Proposed two scheme for the protection and verification with testing. Zhang et al. In[4] Implemented a healthcare system with proposing electronic medical record with core components.

According to Health Insurance Portability and Accountability (HIPAA) [5], it is mandatory to protect all sensitive medical data pertaining to a particular patient's health. Therefore, privacy preservation of sensitive health data is a legal requirement. Hence, it is very important to protect sensitive health data against eavesdropping, false injections and forgery. Unrestricted access to personal health data leads to privacy violations, while selective reporting, impersonating and masquerading leads to incorrect diagnosis and treatment of the patient who is remotely monitored.

An EHR should only be accessed and shared by authorized health care providers such as doctors, nurses, lab technicians due to its function to record any critical information considering for every patient. That critical information such as the enforcement of diagnosis, therapy, avoids allergic reactions and drug duplication. [6]. This is consistent with ethical considerations in the application of information technology, where all health care providers have a moral code that need to balance patient privacy with care needs, including access to records of patients [7].

III Benefits of Hospital Cloud Environment:

With the implementation of hospital cloud environment, tracking of patient data has become easier. It can be tracked for prolonged period by using different and many healthcare suppliers. It is beneficial for those who are

under preventive checkups. It measure up the monitoring of every individual patient for certain necessities like blood pressure, blood sugar, vaccination etc. It helps to provide with efficient designed organization.

Hospital cloud environment records are significant records, these records are worldwide. They serve with the benefit of healthcare chart with different facilities. Patient's information can be accessed from any healthcare through electronic medium using Hospital Cloud Environment.

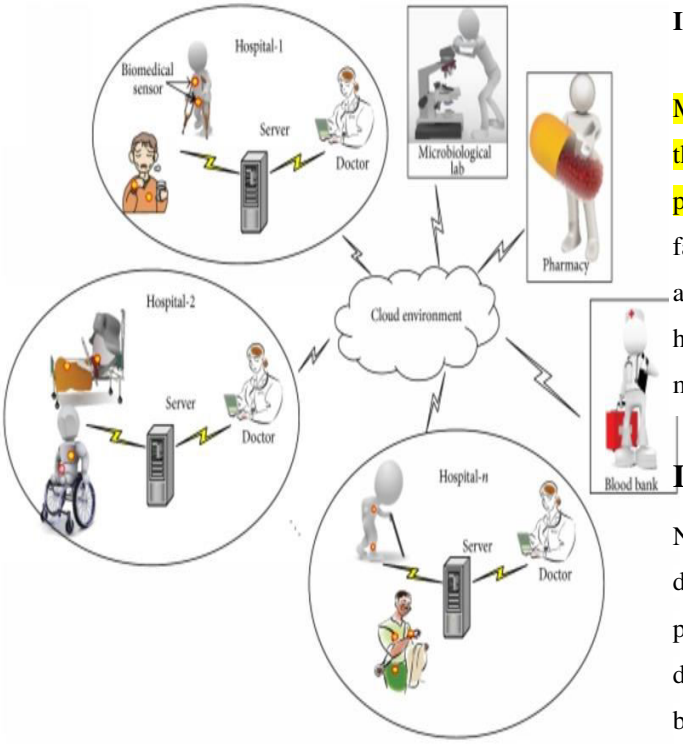

Figure 1: Cloud Architecture for Healthcare [5]

Financial Benefits:

Hospital cloud Environment decreases the expenditure of overall experience. Using the hospital cloud system instead of paper records decreases physical work, return positive results. It improves safety of information stored in hospital cloud environment with boosting quality of services. Doctor can access online patients information and recommend the diagnosed medication to patient safely, even other physician can check information through hospital cloud environment.

Improve Patients Healthcare:

Main objective is to improve patient's record and make their family member more aware of the concern which patient need to be assist for. Even both patient and their family member can explore the issue and become educate about the problem, situation and system regarding healthcare. Technology involves to improve decisions and medical procedure of patient.

IV PROBLEM DOMAIN

Numerous challenges are faced while securing any kind of data either in text form or in image form. Challenges like privacy, security, data transfer from one place to other, data storage and protection of data needs to be worked for better results. Problem claims privacy and confidentiality concern with facing challenges to secure confidential data and information. Privacy preservation of medical health records contributes its study towards secure storage of data in cloud environment. Many different digital health records are observed now-a-days, likewise electronic medical record, healthcare record and health-related document system, other systems are also observed for.

With the increase in data, paper work becomes cost increasing and unsecure medium but in another way dealing with electronic medium is safe for bulk amount of data with accessing of authorized person.

4. SYSTEM ARCHITECTURE

Proposed work describes the solution for sensitive data by using encryption algorithm RC6 and Blowfish. Proposed solution works for encrypting image and text data.

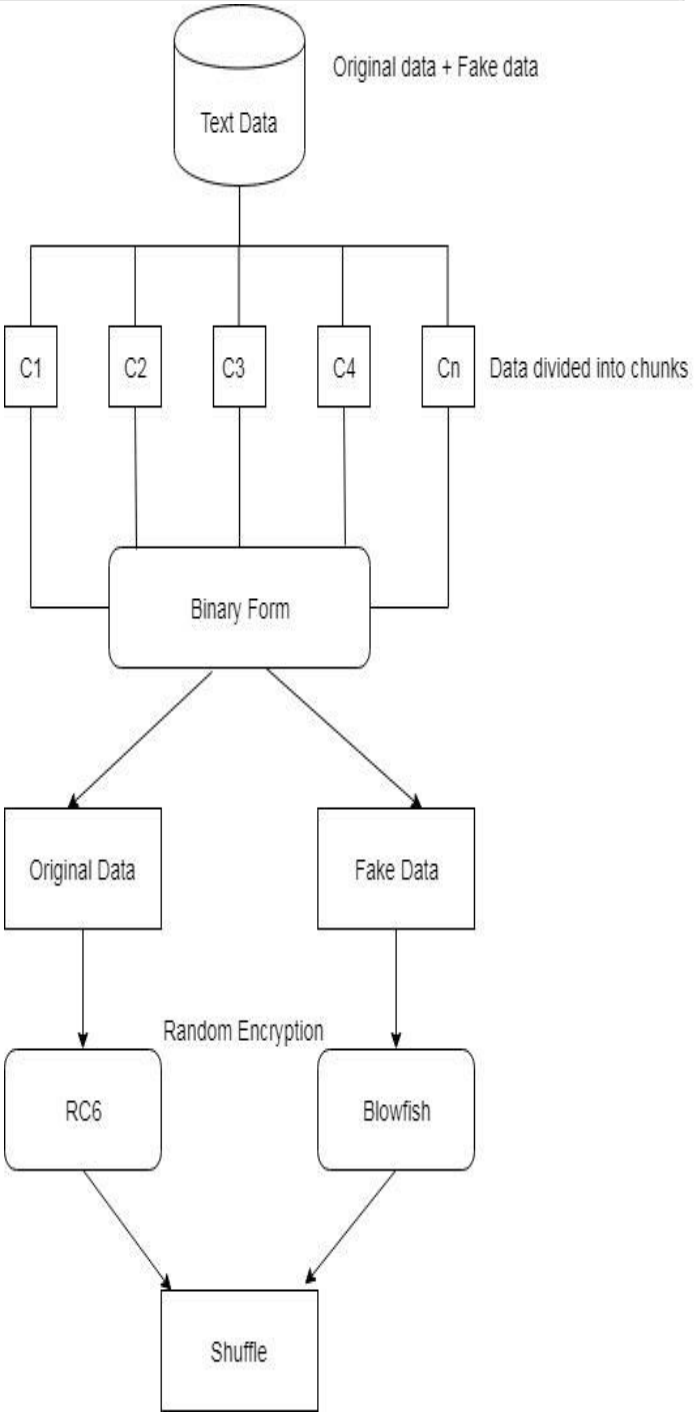

Figure 2: System architecture for text data

- Dataset: (Electronic Medical Record) Data source is taken form Electronic Medical record. Here, data stored is the record of patient's health information, which is confidential. Patient's health information is the sensitive information, if gets in the hand of unauthorized or suspicious person then will be dangerous.
- First, data is taken, which can be in text or image form.
- It is divided into chunks and converted into binary form.
- Afterwards, data is encrypted and decrypted using RC6 and Blowfish algorithm.
- RC6 and Blowfish: They are the encryption algorithm, which are used to encrypt data as to maintain confidentiality. RC6 encrypt original data and Blowfish encrypts fake data.
- ABAC and RBAC is used for privacy preservation of health data. They are the access control, which preserves unauthorized access.
- Original data and fake data is encrypted using RC6 and Blowfish. RC6 is used to encrypt original data whereas Blowfish is used to encrypt fake data.
- Random encryption is performed using both the algorithm
- At last, data is shuffled.

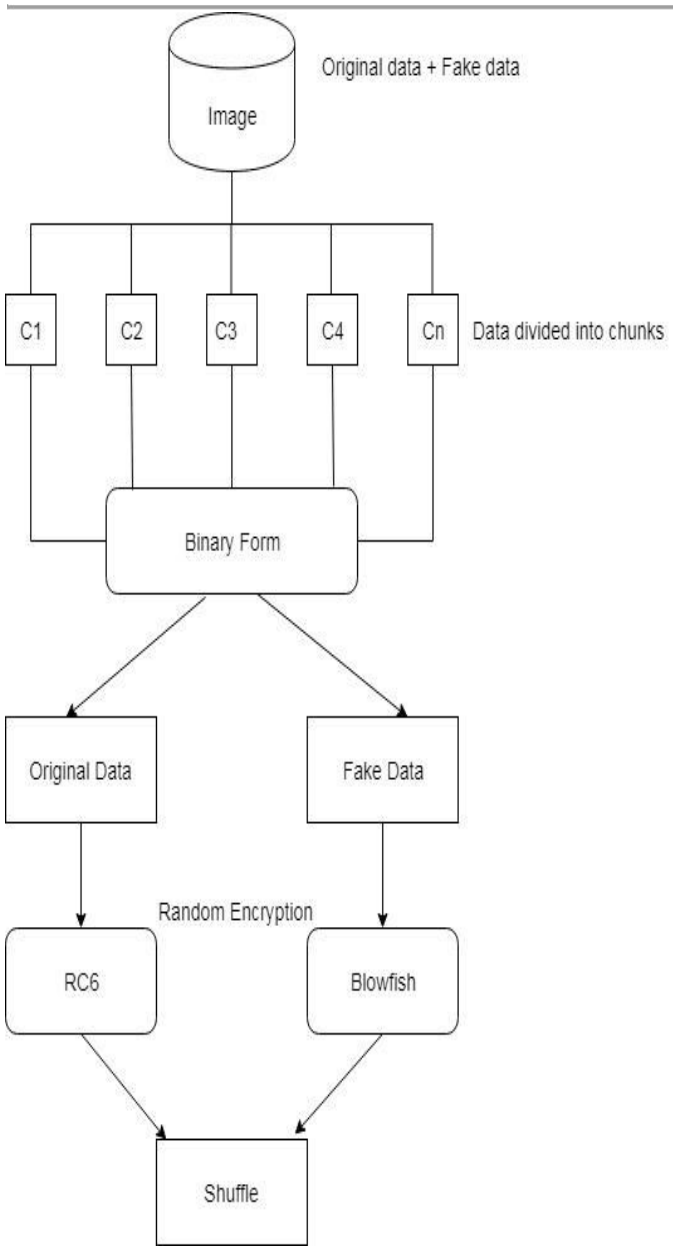

Figure 3: System architecture for image data

5. RESULT ANALYSIS

Result of the given work shows the comparison between proposed work and existing work for the compared results.

Table 1. Existing Work

File Size (MB)	Encryption time (ms)
1	4126.8
5	18378.4
10	19671.9
20	21899.3
50	24470.7
70	27442.4
100	29906.6

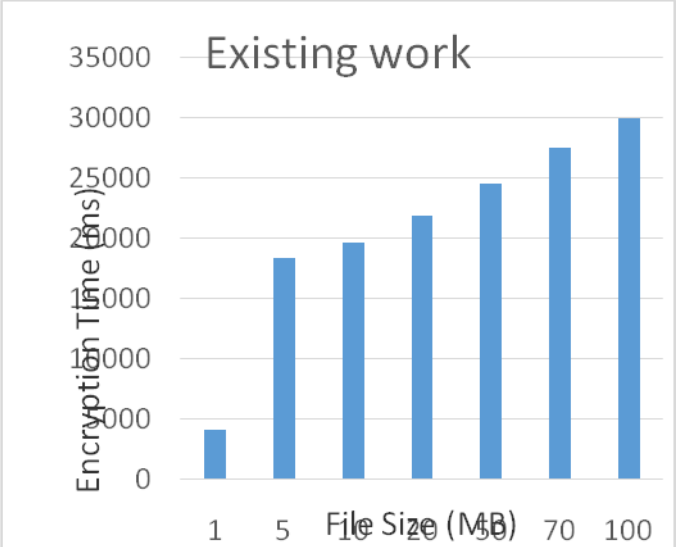

Figure 4: Graph representing existing work

Table 2. Proposed Work

File Size	Proposed Work
1	1124
5	2203.4
10	2373.3

20	4938.7
50	6357
70	9506.6
100	10123.3

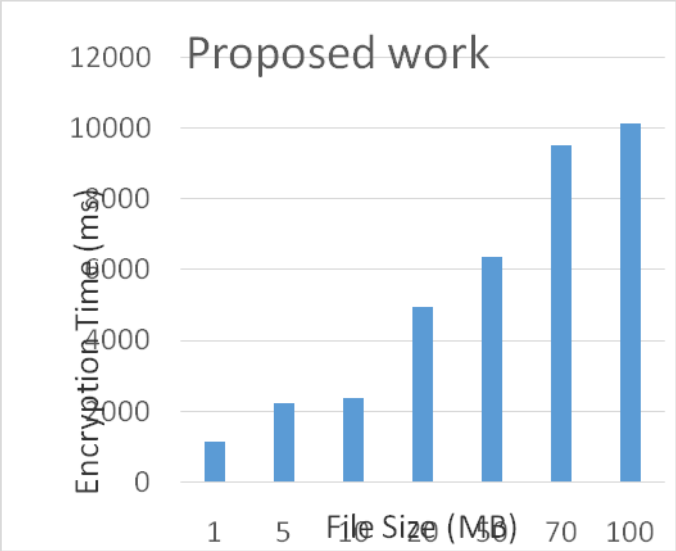

Figure 5: Graph representing proposed work

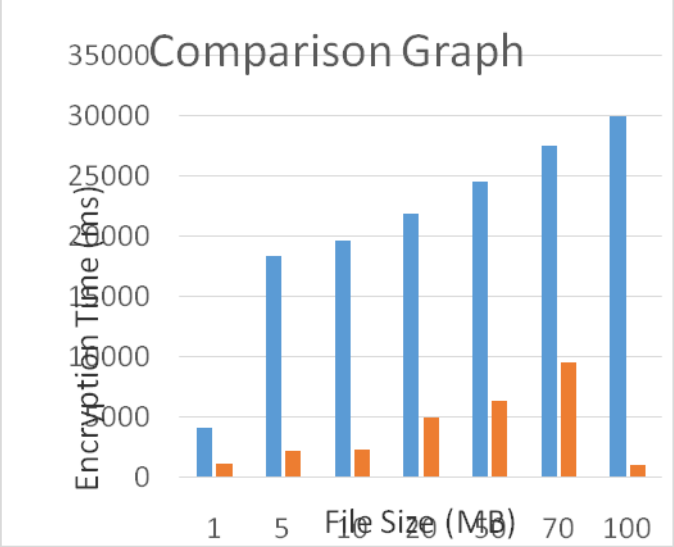

Figure 6: Comparison graph

V Conclusions

Privacy preservation of medical health records 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 based on Hospital Cloud Environment is proposed using RC6 and Blowfish algorithm. For preserving access ABAC and RBAC is used.

References

[1] R. Manoj, Abeer Alsadoon, P.W.C. Prasad, Nectar Costadopoulos, Salih Ali, "Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud". 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, 2017.

[2] Anees Ara, Mznah Al-Rodhaan, Yuan Tian and Abdullah Al-Dhelaan, "A Secure Privacy-Preserving Data Aggregation Scheme based on Bilinear ElGamal Cryptosystem for Remote Health Monitoring Systems". Volume:5, Page: 12601 – 12617, IEEE 2017.

[3] Mohamad Ali Sadikin, Rini Wisnu Wardhani, "Implementation of RSA 2048-bit and AES 256-bit with Digital Signature for Secure Electronic Health Record Application". International Seminar on Intelligent Technology and its Application.

[4] Zhang, Rui, Ling Liu. Security Models and Requirements for Healthcare Application Clouds: Georgia Institute of Technology

[5] R. Nosowsky and T. J. Giordano, "The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule: Implications for Clinical

Research," Annu. Rev. Med., vol. 57, no. 1, pp. 575–590, Jan. 2006.

[6] Garets & Davis. (2006). Electronic Medical Records vs. Electronic Health Records: Yes, There Is a Difference. Diperoleh melalui http://www.himssanalytics.org. Diakses tanggal 30 October 2011.

[7] Kozier, B. (2007). Praktik Keperawatan Professional: Konsep dan Perspektif, Jakarta: EGC

[8] National Institute of Standards and Technology, Computer Security Resource Centre. Available: http://csrc.nist.gov

[9] 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.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE Proceedings, INFOCOM, pp. 1-9, March 2010.

[11] L. Yibin, W. Dai, Z. Ming, and M. Qiu, "Privacy protection for preventing data over-collection in smart city," IEEE Transactions on Computers, vol. PP, pp. 1, 2015.

[12] N. Kahani, and H. R. Shahriari, "An approach for providing privacy and access control in outsourced databases," 14th International CSI Computer Conference, 2009.

[13] National Center for Health. (2006). Electronic Health Records Overview. Diperoleh melalui www.himss.org/. Diakses tanggal 15 October 2011

[14] Nafiseh Kahani, Khalid Elgazzar, James R. Cordy, "Authentication and Access Control in e-Health Systems in the Cloud". 2016 IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, IEEE International Conference on Intelligent Data and Security.

[15] Myers, Glenford J., The art of software testing, Publication info: New York: Wiley, c1979. ISBN: 0471043281 Physical description: xi, 177 p.: ill.; 24 cm.

[16] Hetzel, William C. The Complete Guide to Software Testing, 2nd ed. Publication info: Wellesley, Mass.: QED Information Sciences, 1988.

ISBN: 0894352423.Physical description: ix, 280 p.: ill ; 24 cm.

[17] McConnell, S. (2004). Code Complete, A Practical Handbook of Software Construction: 2nd Edition. Microsoft Press.

[18] Pressman, R. S. (2010). Software Engineering: A Practitioner's Approach, (7th Ed). New York: McGraw-Hill Companies.