ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

EHR Cloud Security in Smart Cities

P. Sailaja, Harini.J, Haripriya.K, Srividhya.H

Department of Information Technology, Velammal Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT: Cloud computing paradigm is one of the popular health IT infrastructure. **Electronic Health Record** (**EHR**) is the systematized collection of patient data such as the medical history, X-rays, ultrasounds, CT scans, MRI reports, personal statistics (age and weight) and billing information which are electronically-stored in a digital format over cloud platform. Sharing of EHRs enables physicians to remotely monitor patients' health and enables individuals to manage their own health data more easily. However, these scenarios face significant challenges regarding security and privacy of the extremely sensitive information contained in EHRs. In this paper, the main focus has been given to secure healthcare private data in the cloud which prompts the idea of using fog computing and RSA encryption technique.

KEYWORDS: Cloud computing**,** Fog computing, Cloud security and privacy, RSA

I. INTRODUCTION

The way of digitizing healthcare workflows by moving towards Electronic Health Records (EHRs) has seen a paradigm shift in the healthcare industry. Maintaining paper-based records of patients in the healthcare organizations can become strenuous with time. To attain smooth flow of information within a healthcare infrastructure HER systems can completely digitize. Data in healthcare refers to sets of electronic medical health data that are large and complex with security issues when they are in third party cloud servers. This pops up the use of Fog computing which is used to protect the real, sensitive data by providing a “fog'” of misinformation which confuses the attackers and makes them believe that they have the real, useful data when they actually do not. So for such privacy to be maintained there is urgent need to take the required measures to protect the health records by allowing only authorized users to view these records. So here we are proposing RSA encryption technique for protecting the confidential data.

II. LITERATURE REVIEW

Researchers have examined the pros and cons of EHRs by considering clinical outcomes. Many clinical outcomes relate to quality of care and privacy of records is the major concern. The author in the paper throws light on how modern healthcare environments where healthcare providers are more agreeable to migrate their electronic medical record systems to clouds. This enables to achieve lower operational cost and excellent interoperability. The author of the paper focuses on moving patients’ medical information to the Cloud that implies several risks related to the security and privacy of sensitive health records. The risks of hosting Electronic Health Records (EHRs) on the cloud servers of third-party Cloud service providers are reviewed. Some suggestions for healthcare providers regarding the protection of confidentiality of patient information and process facilitation are made by the use of encryption techniques. Analysis of arising security and privacy issues in access and management of EHRs is discussed in the paper
In the previous systems, data classification was not performed on medical information. Hence, we propose “SECURE” to secure medical healthcare records before outsourcing these records to public that will in turn help in maintaining data security, availability and integrity.

III. PROPOSED SYSTEM

The objective of proposing a system for maintaining EHRs is to secure them before deploying them for sharing among healthcare providers.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

The proposed system is based on the following:

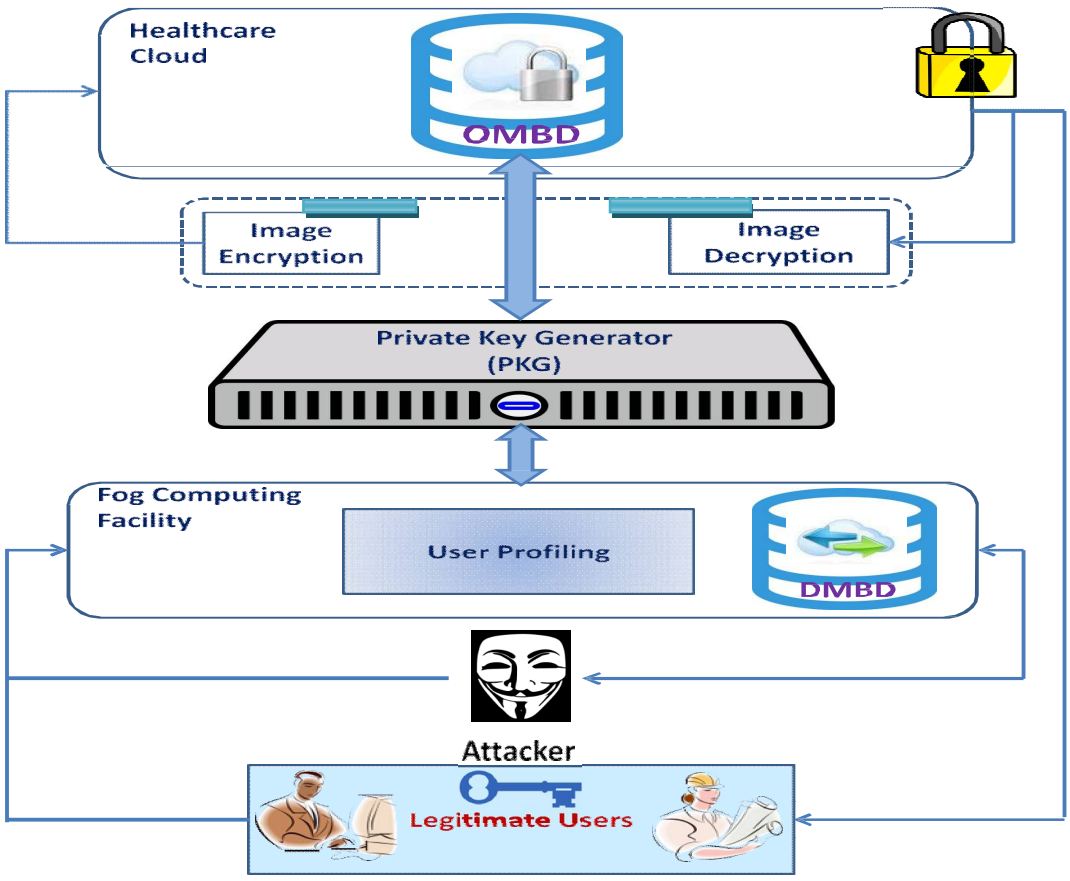
- A web-based system with secure login and registration.
- Cloud storage for flexible retrieval and is a feasible alternative
- Data Security using Encryption algorithm.

Web-Based System With Secure Login And Registration: A web-based system can be accessed anywhere, anytime with the help of good internet connectivity. The system will be designed in such a way that only authorized users to access the relevant information. Patients and doctors have to first register. After registration, they will be a given a Unique Key(sent to their mail) that will be used by them to avail the information.

Cloud Storage For Flexible Retrieval And Is A Feasible Alternative: Cloud storage provides rapid deployment. It has greater accessibility and reliability, also data backup and disaster recovery is possible. The overall storage costs are low because there is no need of purchasing, managing and maintaining expensive hardware that makes Cloud storage economically feasible.

Data Classification and Encryption:.. Data will be classified as authentication information, personal details and medical tests and reports. Medical tests and reports need highest security from exposure to unauthorized access. This will be done using cryptographic technique like Rivest-Shamir-Adleman (RSA) Algorithm to provide security.

ARCHITECTURE DIAGRAM:



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

KEY WORDS:

- MDB-Medical Big Data
- OMDB-Original Medical Big Data
- DMDB-Decoy Medical Big Data

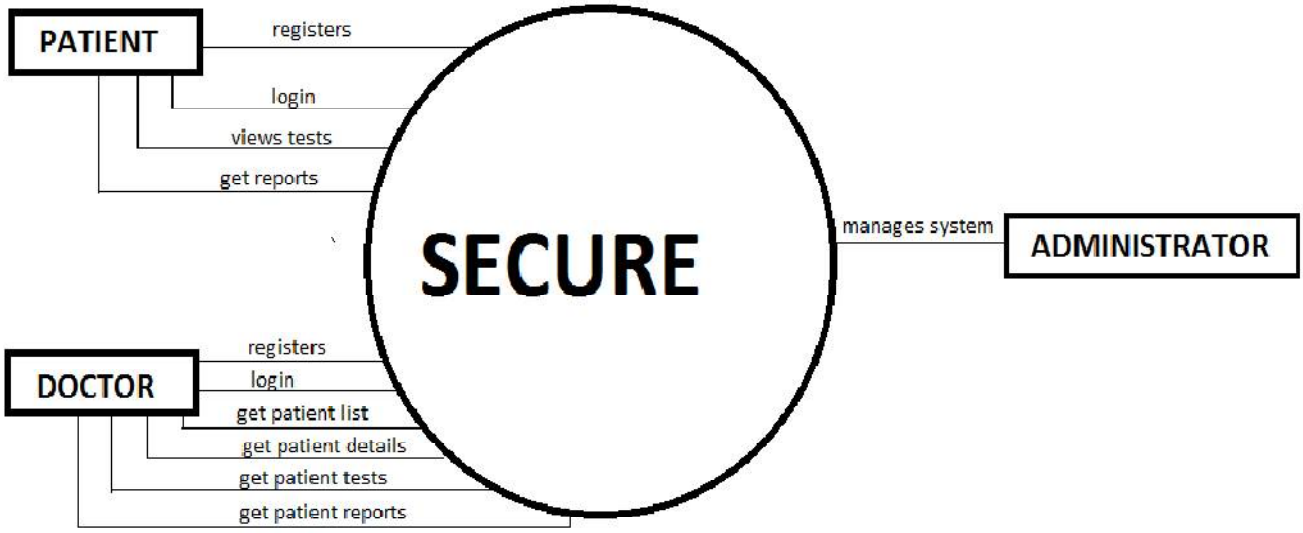
This technique can be considered as an illusion technique, as it makes the attacker believe that he/she has accessed the user's MBD while in fact it is just a decoy gallery. In our proposed system,once the user accesses his/her account, by default the DMBD is shown. Thus, both authorized and unauthorized users will be referred to the DMBD as the first step, while authorized legitimate users,as a second step, will be referred to the OMBD after being verified. We believe that by setting the default value of the DMBD as shown and the OMBD as hidden, we keep the original MBD more secure. Also, we believe that verifying that the user is legitimate is much easier than detecting the attacker.

The DMBD contains fake MBD, which are supposed to make an attacker believe that he/she has accessed the user's photos/medical image while in fact it is just a decoy gallery. The legitimate user already knows that the gallery he/she accessed is not his/her original one, so would move on to the next step. Moving to the next step, the legitimate user can access his/her OMBD after being verifiedby passing the security challenge. The security challenge in our system is key send to mail which user need to provide for viewing original data. Thus, if he/she passes the security challenge, that means he/she is the legitimate user, so will be able to access the OMBD which is located on the cloud computing layer.

In the event of the user accessing only the DMBD, an SMS or email will be sent to the legitimate user to inform him/her that his/her account has been accessed.

DATAFLOW DIAGRAM:

The EHRs to be stored on cloud framework. The framework should provide Platform as a Service (PaaS) so that the whole system is deployed in the cloud itself. Cloud provides with multiple benefits that best suit the system to be implemented like easy sharing, reduces capital costs and provides flexibility.The whole system is deployed on the cloud platform where the EHRs can be shared with ease and decrypt it.



SECURE DATA FLOW DIAGRAM

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

We propose SECURE a central unified platform for doctors and patients of all the hospitals where the system is able to store electronic healthcare records in encrypted form on cloud using various cryptographic techniques and using relevant data classification on those records. Data classification enables the record's data to be classified into various levels of varying sensitivity. The need to segregate data based on such levels of sensitivity was due to the need to maintain confidentiality of those records since the doctor patient privileges are of utmost concern. A patient would not want any outsider to view his/her records. And as such records are leased on cloud where cloud is accessible by everyone, security becomes a major concern. The most plausible way to provide security to these records is via encryption. Therefore SECURE as a unified system is accessible by different types of people ranging from a receptionist at a hospital or to a doctor or an administrator but with different privileges to access the resources of the system to ensure the authoritative limitations are maintained and thus security is availed by the system. An electronic healthcare record has various types of information in it. Classifying the information is a step forward in making the record more secure and achieving confidentiality of records from interceptors and attackers

IV. RESULTS

Encryption algorithm:
Various algorithms were studied in the process to encrypt the EHRs that are to be stored on cloud. As every encryption algorithm has different encryption and decryption time. The encryption and decryption formula for RSA is given as **C= (Pe mod n)** and **P= (Cd mod n)** respectively which follows the polynomial time complexity whereas for attacker it is e√C mod n which follows modular exponential complexity. With usual implementations, doubling the RSA key length means that encryptionwill be four times slower, and decryptionwill be eight times slower. RSA encryption is much faster than RSA decryption. The theory says that for a *n*-bit key, computational effort for encryption is proportional to *n2*, while effort for decryption is proportional to *n3***.**

Table specifying RSA encryption-decryption time[12]:

Operation	Milliseconds/Operation	Megacycles/Operation
RSA1024Encryption	0.08	0.14
RSA1024Decryption	1.46	2.68

RSA Encryption and Decryption Results on different file sizeinputs[9]:

Recordno.	EncryptionTime(seconds)	DecryptionTime(seconds)	InputFileSize(KB)
Recordno.1	5.637362	5.637362	15
Recordno.2	11.27472	11.27472	30
Recordno.3	16.91209	16.91209	45
Recordno.4	22.54945	22.54945	60
Recordno.5	28.18681	28.18681	75

RSA EncryptionThroughput:2.660819KB/Sec
RSA DecryptionThroughput:2.660819KB/Sec

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

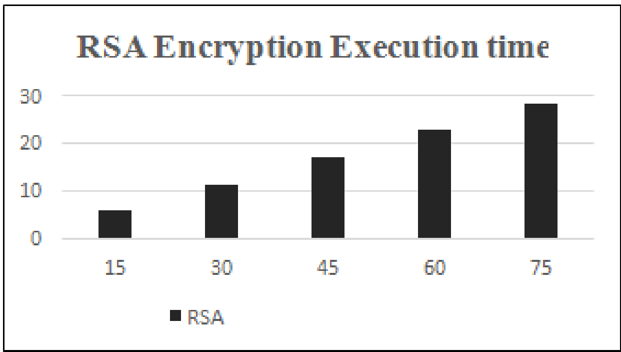


Figure: RSA Encryption Execution Time

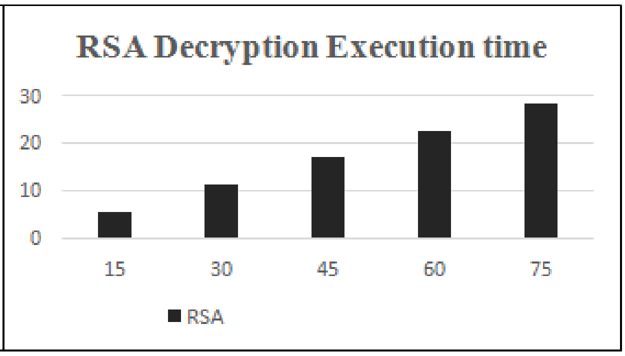


Figure: RSA Decryption Execution Time

ENCRYPTED AND DECRYPTED SAMPLES:

PATIENT DETAILS:

Patient Name: Ì•ú"È»éÏ—b»Áá" . 61Œ È 9‰QßÕÀ‹™f ¶rðUó ô] •Üiâ_ÛÇ

Birthdate: ÃµœvÌ¿qT0T#•@†

Age: kHg|3,€áS Ó é'Ò

Gender: ,±–Ì00+»C*\x•ÂC

REPORT DETAILS:

Report Name: Report2313

Report Type: GGGGQL

Report Date-Time: ˜IÝû„lÃ¤Öp® #b4¥

RESULTS:

ITEM TESTED	LABORATORY RESULTS	REFERENCE VALUES
Color	ÿ'ÏÖ 2NÅ9 7 Ö{	Yellow
Appearance	ÒlÅ$ûê*×Uw "² ¦	Clear
Glucose	¶K'Ö ŻyË Áðr• Y"	Negative
Bilirubin	¶K'Ö ŻyË Áðr• Y"	Negative
Ketone	¶K'Ö ŻyË Áðr• Y"	Negative
Spec Gravity	1	1.003 - 1.035
Blood	¶K'Ö ŻyË Áðr• Y"	Negative
PH	28	5.0 - 8.0
Protein	¶K'Ö ŻyË Áðr• Y"	Negative
UROBILINOGEN	1	0.1 - 1.0 mg/dL
Nitrite	¶K'Ö ŻyË Áðr• Y"	Negative
LEUK ESTERASE	¶K'Ö ŻyË Áðr• Y"	Negative

PATIENT DETAILS:

Patient Name: Andy Bret Caine

Birthdate: 1993-01-01

Age: 23

Gender: male

REPORT DETAILS:

Report Name: Report2313

Report Type: URINE

Report Date-Time: 0000-00-00 00:00:00

RESULTS:

ITEM TESTED	LABORATORY RESULTS	REFERENCE VALUES
Color	yellow	Yellow
Appearance	hazy	Clear
Glucose	negative	Negative
Bilirubin	negative	Negative
Ketone	negative	Negative
Spec Gravity	1	1.003 - 1.035
Blood	negative	Negative
PH	7	5.0 - 8.0
Protein	negative	Negative
UROBILINOGEN	1	0.1 - 1.0 mg/dL
Nitrite	negative	Negative
LEUK ESTERASE	negative	Negative

V. CONCLUSION

In the EHRs, OMBD is kept secretly in the cloud and the DMBD is used as a honey pot and is kept in the fog. Thus, the original multimedia data become more secure by setting the default value of the DMBD, while the OMBD is kept in a hidden gallery. RSA algorithm is used for confidentiality and integrity of data with secrete key being send to authorized user mail for viewing original documents. Currently we are working on the Integrity algorithms and will deploy our algorithms on cloud.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 2, March 2018

REFERENCES

[1] M. Chen, J. Yang, Y. Hao, S. Mao, and K. Hwang, ``A 5G cognitive system for healthcare," Big Data Cognit. Comput., vol. 1, no. 1, p. 2, 2017, doi: 10.3390/.bdcc1010002.
[2] Frost & Sullivan: Drowning in Big Data? Reducing Information Technology Complexities and Costs for Healthcare Organizations.
[Online]. Available: http://www.emc.com/collateral/analyst-reports/frost- sullivan-reducing-information-technology-complexities-ar.pdf
[3] M. Chen, S. Mao, and Y. Liu, ``Big data: A survey," Mobile Netw. Appl., vol. 19, no. 2, pp. 171_209, Apr. 2014.
[4] M. S. Hossain and G. Muhammad, ``Healthcare big data voice pathol-
ogy assessment framework," IEEE Access, vol. 4, no. 1, pp. 7806_7815, Dec. 2016.
[5] M. Chen, Y. Hao, K. Hwang, L. Wang, and L. Wang, ``Disease prediction by machine learning over big data from healthcare communities," IEEE Access, vol. 5, no. 1, pp. 8869_8879, 2017.
[6] M. Chen, P. Zhou, and G. Fortino, ``Emotion communication system," IEEE Access, vol. 5, pp. 326_337, 2017.
[7] M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C.-H. Youn,``Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems," IEEE Commun., vol. 55, no. 1, pp. 54_61, Jan. 2017.
[8] J. Bian, U. Topaloglu, and F. Yu, ``Towards large-scale twitter mining for drug-related adverse events," in Proc. SHB, Maui, HI, USA, 2012, pp. 25_32.
[9] M. S. Hossain and G. Muhammad, ``Cloud-assisted industrial Internet of Things (IIoT)_Enabled framework for health monitoring, " Comput.Netw., vol. 101 pp.
192_202, Jun. 2016.
[10] W. Raghupathi and V. Raghupathi, ``An overview of health analytics,"J. Health Med. Informat., vol. 4, no. 3, pp. 1_11, 2013.
[11] M. S. Hossain, G. Muhammad, S. M. M. Rahman,W. Abdul, A. Alelaiwi, and A. Alamri, ``Toward end-to-end biomet rics-based security for IoT infrastructure," IEEE Wireless Commun.
Mag., vol. 23, no. 5, pp. 45_51,October 2016
[12] I. Foster, Y. Zhao, I. Raicu, and S. Lu, Cloud computing and grid computing 360-degree compared," in Proc. Grid Comput. Environ. Workshop, Austin, TX, USA, Nov. 2008, pp. 1_10.
[13] P. T. Grance. (Oct. 2009). The NIST De_nition of Cloud Computing. [Online]. Available:csrc.nist.gov/groups/SNS/cloud-computing
[14] D. Sangita, C. Ankita, and P. Reshamlal, ``A review on issues and challenges of cloud computing," Int. J. Innov. Adv. Comput. Sci., vol. 4, no. 1, pp. 81_88, 2015.
[15] B. A. Akyol, ``Cyber security challenges in using cloud computing in the electric utility industry," Paci_c Nortwest Nat. Lab., Washington, DC, USA, Tech. Rep. PNNL-21724, Sep. 2012.