ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

Survey on Securing Medical Big Data in Healthcare Cloud

Rohan Rajoriya, Rupesh Kumar Dharne, Shuchita Mudgil

Lecturer, Department of Information Technology, Kalaniketan Polytechnic College Jabalpur, India

ABSTRACT: Cloud computing is a model that provides high-quality services with an improved appearance which enables users to store their data in distant servers that are operated by some third party. Cloud computing is a new thought for providing flexible infrastructure and ease of access but it is still lacking due to its security issues. The main purpose of our research is to understand the cloud architecture, cloud models, security issues and challenges. In this paper, we have studied the complete analysis of cloud security issues along with the three main cloud security aspects: Confidentiality, Integrity and Availability and have also discussed approaches in order to enhance and to preserve security aspects.

KEYWORDS: Medical Big Data, Cloud, EMR, Fog Computing

I. INTRODUCTION

Big data in the health industry is the infinite set of medical data which will be huge and complicated in nature. Therefore, it will be impossible to manage those medical records with the help of traditional software or hardware.

In the e-heath service there is a need of transmission of the patient data or any records to the health professionals as per the requirement. The data includes test reports, scan reports, medical history etc. and they are send to the health professionals through the internet which is not at all secure. The cloud platform makes this process much simpler if the patient visits some other hospital, he doesn't need to carry all his medical records instead everything will be available in the cloud.

The healthcare cloud is a platform which allows the communication of service providers, hospitals, pharmacies and many different clients via the servers. It has got several problems or the disadvantages same as that of cloud computing, among which security breaches are the most common and the important ones. It includes legal and policy issues (copyright, liability etc.), data protection, privacy protection (protecting the personal information of the user) , lack of transparency (the user doesn't know what happens to the data or where it is stored), cyber security issues, absence of security standards, and software licensing [14].

Therefore, novel solutions are required for offering security and privacy to the EMR.

II. LITERATURE SURVEY

A. Harnessing healthcare data security in cloud [1]

Most of the important records of patients are the multimedia. So, we have to take some security measures in order to protect the multimedia data. In this paper, two different algorithms are used to encrypt the text data as well as the images.

In case of the images, first the image is converted into pixels. Then the array of those pixels is converted to form a matrix depending upon its size. Then those matrix is encrypted using an algorithm called Paillier Cryptosystem, which is a asymmetric cryptosystem of homomorphic encryption. The main advantage of using that algorithm is that no change will happen to the orientation of the input. It allows to perform computation on the cipher text.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

Now, for the text data, encryption performed is AES (Advanced Encryption Standard). After encryption data is stored in the cloud. Decryption I performed using the private key. Availability of the key to the doctors or the specialists can be decided by the hospital as per the requirements. Decryption is performed after the retrieval of the data from the cloud.

The components of the architecture are:

- Data Owners- The user whose details are to be stored in the cloud will be the owner of the his/her data. If a patient visits a clinic or any hospital for any purpose, it would have been easy if the hospital or the clinic has already the records of that particular patient, if so no time will be wasted in the communication telling about his medical history .
- EHRs -They are the records or data of a patient which is stored in a digital format. The details including both the personal as well as the hospital records.
- Encryption- It is performed before storing the data into the cloud.
- Cloud storage and retrieval- After the completion of the encryption process, the encrypted records can be placed directly to the cloud. It serves as the storage for all the data as per the requirement.
- Decryption- The decryption of the data are performed only when those data or the records are retrieved from the cloud . The files are decrypted with the help of a key which will be present with the doctor.

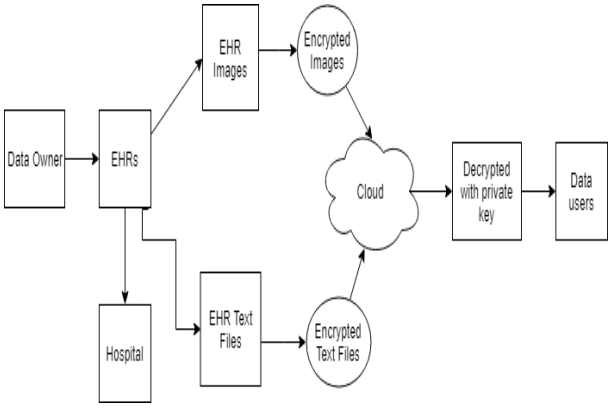

Figure: 1. Architecture

B. Secure Access for Healthcare data in Cloud using CPABE [3]

CPABE (Cipher text Policy Attribute-Based Encryption) is used for the encryption of electronic health records. It consists of certain policies which say which key can be used to decrypt a particular cipher text. Each doctor will have a key which is labelled using certain attributes and access policies are defined for each cipher text. Decryption is possible in case the attributes embedded in doctor's key will match the access policies. One of the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

major benefits of this methodology will be, if a key is hacked, the records which can be decrypted by that key only gets affected and the remaining health records will remain safe.

The architecture consists of mainly 3 components, a cloud where the EHRs is stored, an attribute authority, and the users i.e., the healthcare providers.

The cloud consists of two functionalities, one is the data storage and the other is the computing resources. The cloud can be accessed via a web portal and by any number of clients in medical field who are professionals. The cloud also generates the access policies for every cipher texts.

Users can use the services only after the authentication process. They are responsible for the uploading of the records as well as the encryption of the data. The keys are generated by the attribute authority. After the generation of the keys, the keys are distributed to the healthcare providers. Using those keys the data can be accessed. As the name indicates, the encryption is based on the attributes.

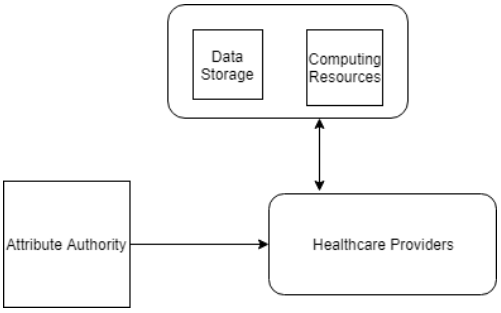

Figure: 2. Architecture

This system provides forward secrecy, i.e., if a user's access permission is banned or denied, he cant access the EHR that the user had the permission to access earlier
,which is considered as one of the main advantage of this system.

C. Secure Medical Data Sharing via an Authorized Mechanism

This paper basically deals with a scheme for authentication. In order to obtain the services, all the users should register with the key generation center. The key generation center then will provide two keys to the users to communicate with each other. One key will be a private key and other one will be a public key. The only security measures used in this system are biometric fingerprint and the digital signature which is a disadvantage also. This system allows the user to authorize health professionals. Patients fingerprint is obtained via mobile phone. Patients can use their mobile phone to access their health information. It consists of mainly 5 entities, the patient, the doctor, key generation centre, cloud, and the hospital.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

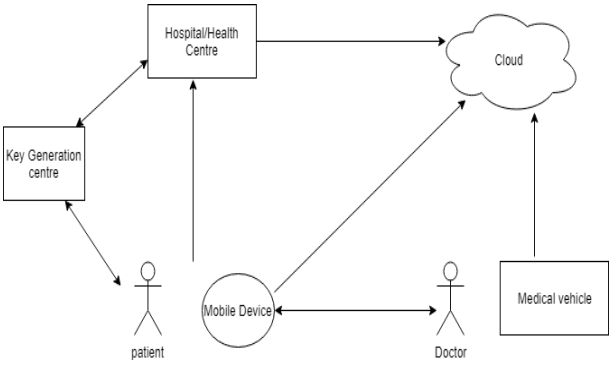

Figure: 3. Architecture

D. Cloud-based service for Secure EMR Exchange

This paper proposed a data exchange methodology. The healthcare professionals, hospitals , patients , and organizations like insurance companies, medical shops are brought under a single platform instead of having several platforms to access data and for their exchange.

This system focuses on securing single platform than multiple. A single login page is provided for the access.. Cloud acts as a storage as well as the means of data exchange.

The data exchange can be between the hospitals, insurance companies, medical shops or any other organizations. Patients are the one who grants access permission to others for accessing his/her data. The documents should be in XML format. These XML documents are digitally signed before exchange.

E. Preserving Privacy of Medical Big Data in Healthcare Cloud Using Fog Computing

In this paper, the concept of telemedicine is used. A DMBD (Decoy Medical Big Data) is created using the decoy technique and it will be stored in the fog computing layer. The Decoy Document Distributor tool is used to generate the decoy documents which will be similar to the original data of the user, which will be stored in the OMBD (Original Medical Big Data). OMBD will be located in the cloud.

A decoy is a dummy of the original data which won't be similar. Even the legitimate user will find it difficult to differentiate between the original document and decoy document if given together.

The architecture of fog computing is given below. It is also known as edge computing. It is considered as an illusion technique. The idea is to place a dummy data near to the original data in order to protect the original one.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

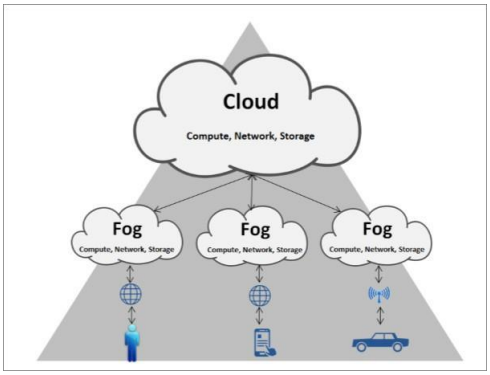

Figure: 4 Fog Computing Architecture

The user will be directed to the DMBD after login as the first step. After verification, either using a verification code and a security question, the user will be directed to his original account i e, OMBD. If it is a malicious user who somehow able to login to DMBD, an alert is send to the authorized individual by the means of an email or SMS.

The DMBD serves as a honeypot which will be placed in the fog computing layer. Blowfish algorithm is used for the encryption. Since it can be used to encrypt any images either black and white or color and of any size.

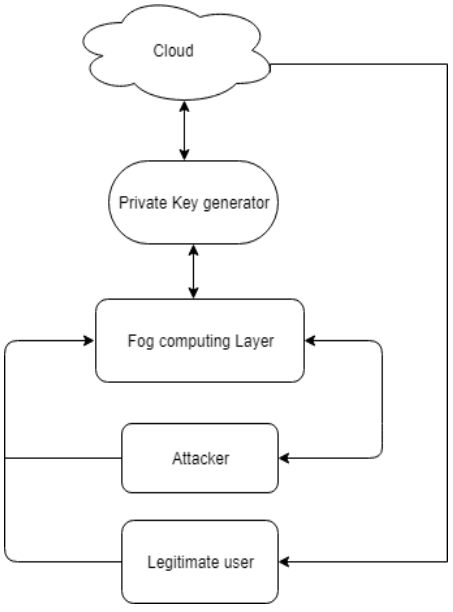

Figure: 4. Architecture

User Profiling is applied in the fog computing layer, which is to monitor the users by which it is possible to differentiate whether the user is genuine one or malicious. Private Key Generator generate the keys for the users. After encryption, the encrypted records will be saved in the cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

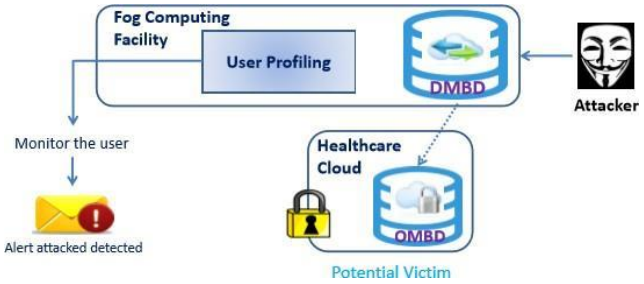

Figure: 5 Working of Fog Computing layer

A HMAC key is generated for each data before uploading and that key will help to differentiate the original data and the decoy data, which will be unique for each data. It uses Elliptic Curve Cryptography combined with the Diffie-Hellman algorithm for the key generation and management purpose.

IV. COMPARISON

The table1 shows the comparison of different methods discussed. Of all the methods discussed, the fog computing technique is effective one.

TABLE 1: Comparison

Name	Method	Advantage	Disadvantage
Harnessing healthcare data security in cloud	Images encrypted using Paillier Cryptosystem and Texts using AES.	Less memory required, Easy to implement	Doesn't support videos like ultrasound scan
Secure Access for Healthcare data in Cloud using CPABE	Uses policies to specify which secret key can decrypt which cipher text	If a secret key compromised, only EHRs decrypted with that key is affected	Computations should be performed by the one who creates the EHR
Secure Medical Data Sharing via an Authorized Mechanism	Biometric fingerprint feature is used to ensure the security	Easy to implement	Not secure
Cloud-based service for Secure EMR Exchange	Provide a single platform to access records Data exchanges are based on XML	Is completely interoperable Patients EMR will be stored in various HIS	High maintenance cost
Preserving Privacy of Medical Big Data in Healthcare Cloud Using Fog	It uses the decoy technique with a fog computing facility	User. not responsible for adding the decoy	Complex in nature,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

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

Website: www.ijircce.com

Vol. 7, Issue 6, June 2019

VI. CONCLUSION

A comprehensive study on various methods of securing medical big data is done. During the study, it was clear that due to the power of user profiling, decoy technique, fog computing is capable of producing effective results. In order to support efficient access and mobility, the medical data are stored in the cloud. The study proposes a fog computing facility to secure patient's data. Two photo galleries are created, one will be located in the cloud, which is the original one and other will be located in the fog layer.

REFERENCES

[1] Aiswarya, R., R. Divya, D. Sangeetha, and V. Vaidehi. "Harnessing healthcare data security in cloud." In Recent Trends in Information Technology (ICRTIT), 2013 International Conference on, pp. 482-488. IEEE, 2013.

[2] Hadeal Abdulaziz Al Hamid, Sk Md Mizanur Rahman, M. Shamim Hossain, Ahmad Almogren, Atif Alamri. "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography", IEEE Access, 2017

[3] Alshehri, Suhair, Stanislaw P. Radziszowski, and Rajendra K. Raj. "Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption." In 2012 IEEE 28th InternationalConference on Data Engineering Workshops, pp. 143-146. IEEE, 2012.

[4] Radwan, Asmaa S., Ayman A. Abdel-Hamid, and Yasser Hanafy. "Cloud-based service for secure electronic medical record exchange." In Computer Theory and Applications (ICCTA), 2012 22nd International Conference on, pp. 94-103. IEEE, 2012.

[5] Solanke Vikas, Kulkarni Gurudatt, Katgaonkar Pawan, and Gupta Shyam. Mobile Cloud Computing: Security Threats. In International Conference on Electronic and Communication Systems, Coimbatore,2014.

[6] Etikala Aruna, Dr. Ch Prasad, and Malla A Reddy. Securing the cloud using Decoy Information Technology to preventing them from distinguishing the Real Sensitive data from Fake Worthless data. International Journal of Advanced Research in Computer Science and Software Engineering 2013, Volume 3, pp. 292-299.

[7] Dnyanesh Patil, Suyash Patil, Deepak Pote, and Nilesh Koli. Secured Cloud Computing With Decoy Documents. International Journal of Advances in Computer Science and Cloud Computing 2014, Volume 2, pp. 43-45.

[8] Sonali Khairnar and Dhanashree Borkar. Fog Computing: A New Concept to Minimize the Attacks and to Provide Security in Cloud Computing environment. International Journal of Research in Engineering and Technology 2014, Volume 3, pp. 124-127

[9] M. Sriram, V. Patel, D. Harishma, and N Lakshmanan. A Hybrid Protocol to Secure the Cloud from Insider Threats. In Cloud Computing in Emerging Markets (CCEM), IEEE International Conference, Bangalore, 2014.

[10] Arabat Rashmi Vinod, Bhalke Sumit Sunidatta, Kumari Uma Rani, and Pillai Preethy Sasidharan. Hindering Data Theft Attacks Through Fog Computing. International Journal of Research in Engineering and Technology 2014, Volume 3, pp. 427-429.

[11] Wentao Liu. Research on cloud computing security problem and strategy. In IEEE Conference, Yichang, 2012

[12] Jonathan Voris, Jermyn Jill, Angelos Keromytis, and Salvatore Stolfo. Bait and Snitch: Defending Computer Systems with Decoys. Columbia University Academic Commons, 2013.

[13] J. Stolfo Salvator, Malek Ben Salem, and D.Angelos Kero. Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud. In IEEE CS Security and Privacy Workshops, 2012

[14] Das Sargita, Chandrakar Ankita, and Pradhan Reshamlal. A Review on Issues and Challenges of Cloud Computing. International Journal of Innovations and Advancement in Computer Science 2015, Volume 4, pp. 81-88.