International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

Security Model for Preserving the Privacy of Medical Big Data in Healthcare Cloud using Fog Computing Facility

Ann Mary Jens[1], K S Soorya[2], Reshma M R[3] , Prof. Eldo P Elias[4] , Prof. Preethi Mathew[5]

[1,2,3]B.Tech student, Computer Science, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India
[4,5]Professor, Computer Science, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India

---

Abstract -. *Nowadays, telemedicine is an emerging healthcare service where the healthcare professionals can diagnose, evaluate, and treat a patient using telecommunication technology. To diagnose and evaluate a patient, the healthcare professionals need to access the electronic medical record (EMR) of the patient, which might contain huge multimedia big data including x-rays, ultrasounds, CT scans, MRI reports, etc. For efficient access and supporting mobility for both the healthcare professionals as well as the patients, the EMR needs to be kept in big data storage in the healthcare cloud. In spite of the popularity of the healthcare cloud, it faces different security issues; for instance, data theft attacks are considered to be one of the most serious security breaches of healthcare data in the cloud. In this paper, the main focus has been given to secure healthcare private data in the cloud using a fog computing facility. To this end, a tri-party one round authenticated key agreement protocol has been proposed based on the bilinear pairing cryptography that can generate a session key among the participants and communicate among them securely. Finally, the private healthcare data are accessed and stored securely by implementing a decoy technique. nt)*

Key Words: Key Management, Security and Privacy, Medical Big Data, Fog Computing, Pairing-based cryptography, Decoy Technique

1. INTRODUCTION

1.1 Background Information

Big data in healthcare refers to sets of electronic medical health data that are large and complex. Due to their huge volume and complexity, it is difficult (or infeasible) to manage those data sets using traditional software and/or hardware. The diversity and volume of multimedia medical big data (MBD) and efficient accessibility of these datasets make it irresistible. MBD in the healthcare industry includes patient data in electronic patient records (EPRs), clinical data from computerized physician order entries (CPOEs), machine generated data, such as from monitoring vital signs, non-patient-specific information, including emergency care data. In the telemedicine service, EMRs including MBD, images, and multimedia medical data are transmitted on the fly over insecure internet connections as they are required by the remote doctors. The healthcare cloud infrastructure would make it much easier to pull all different healthcare information together for a patient while the patient moves from one hospital to another. As a result, the patients' information can be managed and tracked easily. Healthcare cloud computing offers the benefit of both software and hardware through the provision of services over the Internet. Healthcare cloud computing has different issues related to its security, the most important of which are: legal and policy issues, data protection, privacy protection, lack of transparency, cybersecurity issues, absence of security standards, and software licensing.

1.2 Rationale

Because information technology has developed rapidly in recent years, data protection is more necessary than ever. Tampering with data has been a serious threat these days. There has been many cases registered recently regarding medical data breach as shown in figure 1. As a part of securing the cloud data mission, our project focuses on securing user's multimedia data within the cloud by using fog computing.

Fig -1: Cases on Data Breach

To this end, two photo galleries are generated. The OMBD is kept secretly in the cloud and the DMBD is used as a honeypot and is kept in the fog. Therefore, instead of retrieving the DMBD only when any unauthorized access is discovered, the user, by default, accesses the DMBD. The OMBD is only accessible by a user after verifying the authenticity of the user. 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. To facilitate the above process, an efficient tri-party authenticated key agreement protocol has been proposed

among the user, the DPG, and the OPG based on paring cryptography.

1.3 Objectives

A methodology is presented to secure patients' MBD in the healthcare cloud using the decoy technique with a fog computing facility. It serves as a second gallery to contain decoy MBD (DMBD) that appear to the attacker as if it is the original MBD (OMBD).In our proposed methodology the decoy files are retrieved from the beginning to ensure better security. Additionally, it uses a double security technique by encrypting the original file when an attacker recognizes that he/she is dealing with a decoy gallery. He/she would need to figure out how to decode the original gallery. As a result, our methodology ensures that the users' MBD are 100% secure and shortens the process.

2. LITERATURE REVIEW

2.1 Cloud Computing

Cloud computing has different service models, which are divided into three categories: (1) IaaS, which allows users to take advantage of the infrastructure without mentioning the hardware running behind it; (2) PaaS, which builds on IaaS and provides clients with access to basic operating software and optional services to develop and use software applications without software installation and (3) SaaS, which enables clients to use software applications without having to install them on their personal computer, by offering these as a service through the Internet. We can categorize cloud computing consistent with the deployment model into: (1) a public cloud, in which the resources are sold or rented to the public by the service provider, who at the same time is the owner (2) a private cloud owned or rented by an organization (3) community clouds, in which some closed communities share the same cloud resources and (4) a hybrid cloud, which has the characteristics of two or more deployment models

2.2 Fog Computing

Fog computing is an emerging paradigm that provides storage, processing, and communication services closer to the end user. It reduces latency, provides location awareness, and supports high-density wireless networks. Providing data and putting them on the edge of a network to be nearer to the user are considered among the main tasks of fog computing. The end user is connected to different nodes, which are referred to as the "edge," thus the term "edge computing." Fog computing does not replace cloud computing. Rather, it extends the cloud to the edge of the network. Creating decoy information and locating it beside the real information in the cloud to hide the true data of the user is also called fog computing. This architecture offers a number of services that are related to the use of decoys. Hence, fog computing can be considered as an alternative name for the Decoy Document Distributor (D3), which is a tool for generating and monitoring decoys. This strategy is used to protect the real, sensitive data by providing a "fog" of misinformation. Decoy information, such as decoy documents, honey files, and honeypots, among others, can be generated when unauthorized access is detected. This confuses the attackers and makes them believe that they have the real, useful data when they actually do not. Decoys can be created manually by the user him/herself.

2.3 Decoyfile

The basic idea behind this technique is to limit the damage caused by stolen data by decreasing the value of the stolen information. A Decoyfile should be believable. In the absence of any additional information, a perfectly believable decoy should make it impossible for an attacker to figure out that the data are not real. The decoy should be enticing enough to attract the attention of the attacker and make him/her open the file. It should be conspicuous, that is, how easy a decoy is to access. It should be differentiable so that the real user can distinguish between the real and the decoy file. The decoy should be non-interfering so that the real user will not accidentally misuse the bogus information contained in the decoy. The decoy should be detectable. This refers to the ability of decoys to alert their owners once they have been accessed.

2.4 Bilinear Pairing Function

A bilinear pairing is a map between cyclic groups. Let G1, G2, and GT be cyclic groups with a prime order q. We consider G1 and G2 as additive groups and GT to be a multiplicative group. A bilinear pairing is defined as: e: G1×G2 → GT. The properties are: (1) Bilinear: It holds the important property e (aP, bQ) = e (P, Q) ab, where ∀P, Q ∈ G1 and ∀a, b ∈ Z. (2) Non-degenerate: e (P, P)! =1. (3) Computability: A mapping is said to be computable if an algorithm exists which can efficiently compute e (P, Q) for any P, Q ∈ G1

2.5 Elliptic Curve Diffie-Hellman

Elliptic curve Diffie-Hellman (ECDH) is a key-agreement protocol, more than an encryption algorithm. This means that ECDH defines how keys should be generated and exchanged between parties, and how actual data using such keys are encrypted is up to us. Based on our system, we will encrypt the photos using the Blowfish algorithm while the key authentication and exchange will be done using ECDH. Thus, the key is generated by the Elliptic Curve Cryptography (ECC) Private Key Generator (PKG) key generator and then the key agreement can be done by Diffie-Hellman (DH). The combination of these two concepts is ECDH.

3. DESIGN

3.1 System Design

Fog Computing facility help to implement a security model for preserving the privacy of medical big data using Decoy technique. In the system, when the user accesses his/her account, whether he/she is a legitimate user or an attacker, his/her first step would be accessing the DMBD. User profiling is done side by side. User profiling can help to determine whether a user is legitimate or not. The DMBD contains fake MBD, which are supposed to make an attacker believe that he/she has accessed the user's photos/medical image. If the user is legitimate he/she would move on to the next step. Moving to the next step, the legitimate user can access his/her OMBD. 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.

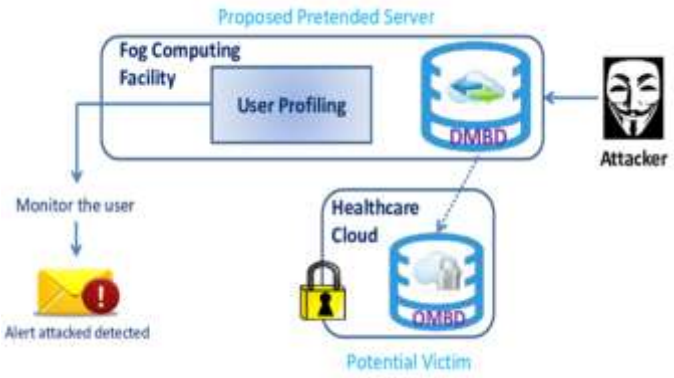

Fig -2: Proposed System Design

3.2 Process

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. The DMBD is located in the fog computing layer side by side with user profiling. 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 verified by passing the security challenge. The security challenge might be a challenging security question or even a verification code. 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. The message will contain the attacker's information. Each time the legitimate user uploads a new photo/medical image on his/her account, a decoy photo from fog computing will be uploaded to his/her DMBD. When the user uploads the photo, he/she is supposed to recognize the photo category which will help fog computing to add the photo that belongs to the same category on the DMBD. This would make it closer to the original photo, so that the attacker would not differentiate between the real user's photo and the fake one. The user is not responsible for adding the decoy photo in his/her DMBD, since it will be added automatically while he/she is uploading the original photo to the OMBD.

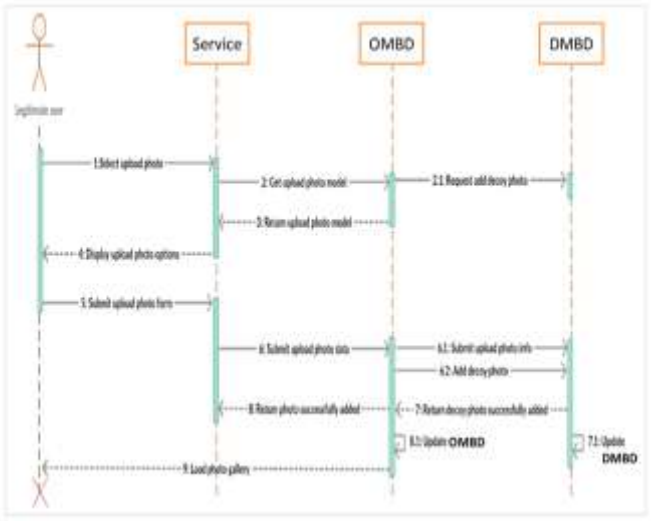

Fig -2: Process

4. CONCLUSIONS

As a part of securing the cloud data mission, the user's multimedia data within the cloud is secured by using fog computing. To this end, two photo galleries are generated. The OMBD is kept secretly in the cloud and the DMBD is used as a honeypot and is kept in the fog. Therefore, instead of retrieving the DMBD only when any unauthorized access is discovered, the user, by default, accesses the DMBD.

The OMBD is only accessible by a user after verifying the Authenticity of the user. 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.

REFERENCES

[1] M. Chen, J. Yang, Y. Hao, , S. Mao, K. Hwang, "A 5G Cognitive System for Healthcare", Big Data and Cognitive Computing, Vol. 1, No. 1, DOI:10.3390/ bdcc1010002, 2017.

Frost & Sullivan: Drowning in Big Data? Reducing Information Technology Complexities and Costs for Healthcare Organizations.

M. Chen, S. Mao, Y. Liu, "Big Data: A Survey", Mobile Networks and Applications, Vol. 19, No. 2, pp. 171-209, April 2014.

M. S. Hossain, and G. Muhammad, "Healthcare Big Data Voice Pathology Assessment Framework," IEEE Access, vol. 4, no. 1, pp. 7806-7815, December 2016.

M. Chen, Y. Hao , K. Hwang, L. Wang, L. Wang, "Disease Prediction by Machine Learning over Big Healthcare Data", IEEE Access, Vol. 5, No. 1, pp. 8869-8879, 2017.

M. Chen, P. Zhou, G. Fortino, "Emotion Communication System", IEEE Access, Vol. 5, pp. 326-337, 2017.

M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, C. Youn, "Wearable 2.0: Enable Human-Cloud Integration in Next Generation Healthcare System", IEEE Communications, Vol. 55, No. 1, pp. 54-61, Jan. 2017.

Bian J, Topaloglu U, Yu F, Yu F. Towards Large-scale Twitter Mining for Drug-related Adverse Events. Maui, Hawaii: SHB; 2012.

M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT) - enabled framework for Health Monitoring," Elsevier Computer Networks, Vol. 101, No. (2016), pp.192-202, June 2016.

Raghupathi W, Raghupathi V. An Overview of Health Analytics. 2013.

M. S. Hossain, G. Muhammad, Sk. M. M. Rahman, W. Abdul, A. Alelaiwi and A. Almari, "Towards End-to-End Biometrics-Based Security for IoT Infrastructure," IEEE Wireless Communication magazine, vol. 23. no. 5, pp. 45-51, October 2016

I. Foster, Yong Zhao, I. Raicu, and Shiyong Lu. Cloud Computing and Grid Computing 360-Degree Compared. Grid Computing Environments Workshop, Austin, 2008.

BIOGRAPHIES

Ann Mary Jens is currently a final year B.Tech student in Mar Athanasius College of Engineering under APJ Abdul Kalam Technological University.

K.S.Soorya is currently a final year B.Tech student in Mar Athanasius College of Engineering under APJ Abdul Kalam Technological University.

Reshma M R is currently a final year B.Tech student in Mar Athanasius College of Engineering under APJ Abdul Kalam Technological University.