Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

A SURVEY ON SECURITY TECHNIQUES IN A HEALTHCARE CLOUD FOR PROTECTING THE PRIVACY OF MEDICAL BIG DATA

T S Vinutha, Dr.Shambavi B R,

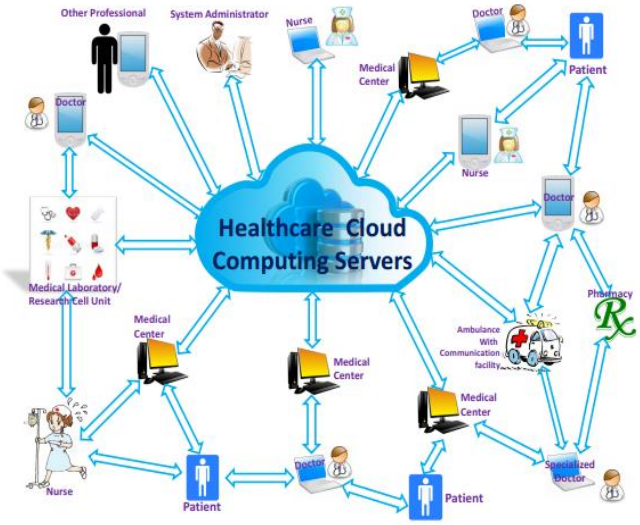
[1]*PG student, Department Information Science and Engineering, BMSCE*
[2]*Associate professor, department of Information Science and Engineering, BMSCE*

Abstract—*The healthcare big data is fast growing and plays a major role in providing a healthcare service such as telemedicine. Telemedicine is a telecommunication technology, where the healthcare professionals diagnose and evaluate to treat a patient. The healthcare professionals need to access the electronic medical record(EMR) of the patient ,which contains huge big data such as X-rays, CT scan, MRI reports etc. For efficient access and support the EMR needs to be kept in big data storage in the cloud. Apart from these there are several security issues in the cloud for example, a data theft attack is one of the security breaches of healthcare data in the cloud. In this paper, we focus mainly to secure the private data in the cloud using fog computing. We have also proposed a protocol called tri-party one round authenticated key agreement, which is based on bilinear pairing cryptography. This generates a key which provides a secure communication among the participants. Thus the private data in cloud is stored and accessed securely by implementing a decoy technique.*

Index Terms*- key management; Fog computing; Medical big data; security and privacy; pairing-based cryptography; decoy technique*

I. INTRODUCTION

An increasing number of devices such as sensors, smart phones, wearable or portable are being used to provide healthcare services in hospitals and at home. Big data comes in different forms such as text, images, audio, etc. healthcare big data refers to a set of electronic medical health data that are large and complex. Due to complexity and huge volume, it is difficult to manage those datasets using certain software or hardware. Medical big data(MBD) in healthcare industry contains information such as patient data in electronic patient records(EPRs); clinical data; machine generated/sensor data such as monitoring vital signs; and non-patient information such as emergency care data, news feeds, and articles in medical journals. In the e-health research, telemedicine is one of the emerging fields. In this service, EMRs including MBD, images and multimedia medical data are transmitted on the insecure internet connections as they are required by the remote doctors[4].
The infrastructure of the healthcare cloud would make it easier to obtain all the information together for a patient. While the patient moves from one hospital to other. Thus, by this the patient information can be managed and tracked easily. In the healthcare cloud all the service providers and stakeholders communicate with each other through cloud servers, as illustrated in fig1.



When compared to cloud computing, healthcare cloud has several different issues related to security such as legal and policy issues, data protection, privacy protection[2]. In privacy issues we concentrate on three things that are trust, uncertainty and compliance. There is another issue related to the customer is lack of transparency, which means the customer does not know whether his/her data are physically stored or what happens to it. To this end, a proper policy is required to define the relations between consumers, utilities and third parties in the cloud and to make sure that it is secure.

II. BACKGROUND AND PRELIMINARIES

In this section we analyze few technical backgrounds that will help us in better understanding of the various concepts.

A. Cloud Computing

cloud computing is everywhere. It gets its name as a metaphor for the internet. Internet is represented in network datagrams as a cloud[3]. Cloud is present at remote location and it provide services over public and private networks. It offers online data storage, infrastructure and application.

Cloud computing provides different services such as software as a service (SaaS), platform as a service (PaaS) .SaaS is a model in which an application is hosted as a service to customers who access it via the internet. PaaS is another application delivery model, which supplies all the resources required to build applications and services completely from the internet, without having to download or install software.

Mobile cloud computing infrastructure can be used for healthcare applications. The traditional infrastructure involves a set of cloud resources, which can be accessed remotely by the users via through the internet.

B. Fog Computing

Fog computing is nothing but the extension of the cloud computing. It facilitates the operation of compute, storage, and networking services between the end devices. Fog computing is also known as fogging or edge computing[5]. Fog computing can be used to hide the true data of the user by creating a decoy information and placing it beside the original data in the cloud. This computing can be used to create decoys with minimal intervention, where it is used to protect the real, sensitive data by providing a “fog” of information.

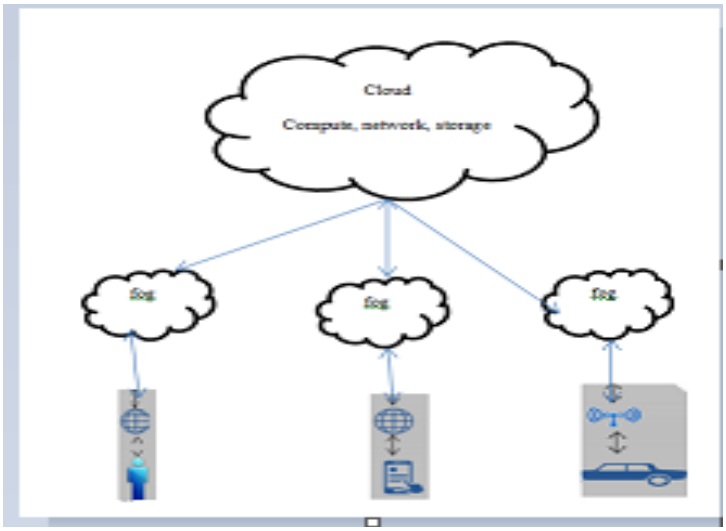


Figure2:fog computing architecture

C. BigData

The transpire technology that today is on demand is “Big data” which emphasis both in science and industry. Big data is a collection of datasets which contains enormous amount of data ranging in zettabytes. Data intensive technologies are becoming a new technology trend in science, industry and business. Big data is linked with almost all the human activities digital services to research point of view. Big data plays a vital role in research field and researchers are very urge to find more and dig more about it. By defining the security framework of big data the work proposed by the authors could be extended and allow secure mechanism for processing, storage, and transfer of big data.

Big data encounters a lot of issues namely management issues, storing issues, processing issues and most important one is security issues. By providing authentication, access control and authorization to the data one can ensure data

security in cloud computing. One of the major advantage of big data is data analytics in which the individual is allowed to access the content or look and feel the real time websites.

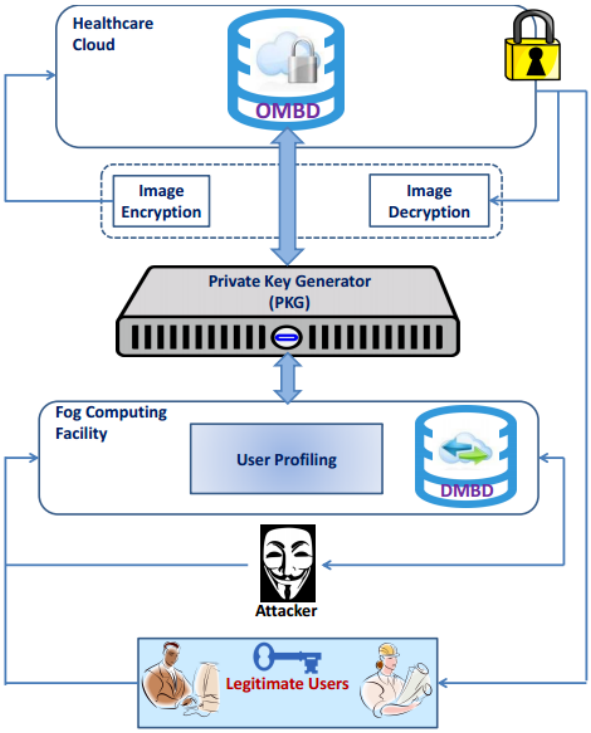
D. BigData Security and Privacy Issues In Healthcare

Patil and seshadri has focused the work on big data healthcare security and privacy. The reactive to proactive paradigm shift in healthcare made an alarming sign to protect the data. The patients identity and diagnosis report etc must be kept safe.

Forbes magazine reported that target corporation sent a baby coupons to a teenage girl. This created the security feel in healthcare field to maintain the personal space of the patient.

E. Decoy Data Technology

It is the duplicate or garbage data that is provided to the user when the user is detected as an intruder. Decoy data files are the one which is not useful to the authorized users but acts as a trap to unauthorized users. The attackers will believe that the data obtained are the original one. Whenever the cloud service notices the abnormal access, the decoy files which contains duplicate data are returned by the cloud and delivered as it appears as a original data. To achieve this, decoy should have certain features. The decoy should seem trustworthy and authentic. And decoy should attract the attacker to make him/her open the file. The decoy should be distinguishable that real user must be able to identify the real data and decoy data.



III. METHODOLOGY

A. DMBD ALGORITHM

In this section, whenever we use “gallery/photo gallery” it means multimedia MBD(medical big data) and the gallery contains medical big data. We have two types of medical big data that is stored in cloud to secure data that is OMBD(original medical big data) and DMBD(decoy medical big data).

DMBD is used as a trap gallery and it is used to protect OMBD by distracting the attacker[3]. To protect the original data DMBD is placed in the fog computing as honey pot which is located in the cloud. Therefore, for each newly uploaded MBD in the OMBD, a decoy will be placed in the DMBD.

B. USER PROFILING ALGORITHM

User profiling is used to determine whether the user is legitimate or not based on certain features such as amount of downloaded data, user-search behaviour, etc. Depending on how the user deals with the cloud data and based on the parameters he/her will be evaluated whether he is authorized user or not.

Based on the following characteristics the system will determine the behaviour of the person

1.login time
2.session time
3.upload count
4.download count
5.how many files are read and how often.

C. PHOTO ENCRYPTION ALGORITHM

It is a technique used to secure a photo by changing it to an ununderstandable one. It contains several levels of security with different properties. here we are using blowfish algorithm. It is a symmetric key cryptography where the key does not change such as automatic file encryption. This algorithm is chosed because of the following reasons:

1. It has longer key length which makes it more secure.
2. It can encrypt any photo format or size.

D. PHOTO DECRYPTION ALGORITHM

It is the reverse process of photo decryption algorithm. The process will obtain the original data. In this the inputs will be cipher photo and the key and finally it obtain the plain photo.

E. ORIGINAL MBD ALGORITHM

The OMBD contains the real users photo for which the whole system was built to secure original data. This gallery is situated in cloud. Each time when the user needs to access it, user needs to pass the security challenge initially. And when the user needs uploads the photo into the gallery , the original photo will be encrypted using a decoy in the DMBD.

F. BLOWFISH ALGORITHM

From the competitive analysis on different symmetric encryption algorithms such as DES, AES and Blowfish. The comparision between these algorithms are based on criteria given below:

1.Block size: larger the block size, it is more secure. The block size used for all algorithms is 64 bits except for AES, which contains 128 bits. Hence AES is more secure but it costs more to implement.
2. Key length:The longest key length means less number of successful attacks. Blowfish is more secure since its key length range from 32 bits to 448 bits.
3.Encryption/decryption time: The algorithm which consumes shortest time is blowfish. And it is secure.
4.power consumption:Power consumption is more in 3DES and blowfish consumes less power compared to others.
5.Confidentiality:Blowfish has the highest confidentiality while the DES is low.

Thus by above comparision we can say that blowfish gives better performance. and it is the best candidate to use in the proposed system.

IV. CONCLUSION

Apart from securing the cloud data, this paper focuses on securing users multimedia data and medical big data in the cloud using fog computing. To this end two galleries are generated. Where original medical big data is kept secretly in the hidden gallery. DMBD is used as a honeypot and it is kept in fog. The user by default accesses DMBD instead of accessing OMBD. After certain security challenges the authorized user will be allowed to access the original medical big data. While the unauthorized user will get the decoy file which contains duplicate data. Thus the original multimedia big data become more secure by setting the default value to DMBD.

V. 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.
[2] Frost & Sullivan: Drowning in Big Data? Reducing Information Technology Complexities and Costs for Healthcare Organizations.http://www.emc.com/collateral/analyst-reports/frost-sullivan-reducing-information-technology-complexities-ar.pdf
[3] M. Chen, S. Mao, Y. Liu, "Big Data: A Survey", Mobile Networks and Applications, Vol. 19, No. 2, pp. 171-209, April 2014.
[4] M. S. Hossain, and G. Muhammad, "Healthcare Big Data Voice Pathology Assessment Framework," IEEE Access, vol. 4, no. 1, pp. 7806-7815, December 2016.
[5] 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.
[6] M. Chen, P. Zhou, G. Fortino, "Emotion Communication System", IEEE Access, Vol. 5, pp. 326-337, 2017.

