International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

Medical Big Data Protection using Fog Computing and Decoy Technique

Medha. M.R[1], Ms.Krishnachalitha.K.C[2]

[1]*Msc Computer Science, St.Joseph's college (Autonomous), Irinjalakkuda, Thrissur, Kerala*
[2]*Assistant Professor, Dept of Computer Science, St.Joseph's college (Autonomous), Irinjalakkuda, Thrissur, Kerala*

Abstract - *Nowadays in hospitalities the doctors use medical data in the form of Electronic which is known as Electronic Medical Records (EMR) .It contains multimedia big data such as X-rays, ultrasounds, MRI reports etc. This medical data is kept on the healthcare cloud for the efficient storage and accessing. As the popularity of healthcare clouding increases security issues related to this also increases. The most serious issue is data theft attacks. In this paper the main focus has been given to provide security for the medical data stored in the healthcare cloud system using fog computing facility and decoy technique.*

Key Words: **cloud computing, fog computing, decoy file, MBD, OMBD, DMBD**

1. INTRODUCTION

Medical big data in healthcare refers to the medical records such as lab reports, x-rays, ultrasounds; MRI reports etc. these data is huge and complex due to these factors it is difficult to store in traditional software and hardware facility. Hence we use a healthcare cloud system to place those data. Healthcare cloud is a cloud computing facility which is used as the storage medium for different medical data. It provides the benefits of both software and hardware through the provision of services over the Internet. As the popularity of healthcare cloud increases the attacks on the system is also increases the main issue is related to security of those data stored in the system. The security issues are legal issues, policy issues, data and privacy protection etc. because of these problems cloud has less security mechanism. The aim of this paper is to provide hundred percentage of security to the big data called Medical Big Data (MBD) in the healthcare cloud. For this a technique called Decoy is used with Fog computing facility. This technique provides a second gallery known as Decoy Medical Big Data (DMBD) that appears as the Original Medical Big Data (OMBD) to the attacker. In this methodology when the attacker catches the system the decoy files are retrieved and also it uses a double security technique by encrypting the original file when an attacker is realize that they deals with a decoy file then they need to figure out the original data from the secured one hence this methodology provides a 100% security to the data. The advantage is that there is no need to worry if the user is an attacker because only the decoy file is retrieved and original file is hidden it only gets to the legitimate user after successful verification. At the end we use a compression algorithm to manage memory efficiently to store these data.

2. TECHNICAL BACKGROUNDS

Cloud computing

Cloud computing is defined by the NIST (2009) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1], [2].The service models provided by cloud computing is categorized into three: (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 [3]. 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 [4].Several features are available in cloud computing, for example: on-demand broad network access, self-service, measured service, resource pooling, and rapid elasticity. Self-service means that the customers can manage and request their own resources. On the Internet or in private networks, the services offered are known as broad network access. In pooled Resources, the customer draws from a pool of computing resources, usually in a remote data center. The services can be scaled larger or smaller, and customers are billed according to the measured use of a service [18].

Fog computing

Fog computing is a method that provides different services such as storing, processing and communication closer to end user. Fog computing extends the cloud to the edge of the network. Fog computing also can be defined as the decoy generator and locate them beside real data to

protect the original data. It provides different services similar to decoys thus it can be considered as an alternative for 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 honey pots, 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; for example, when the user creates a new document, he/she can create a fake document that will appear as a mirror document but contains bogus information. Such manual creation of decoys is obviously very tiring for the user, especially if we are talking about a large organization with multiple users and files. For this reason, fog computing is used to create decoys with minimal user intervention [5], [6], [7].

Decoy file

The basic idea behind this technique is to limit the damage Caused by stolen data by decreasing the value of the stolen Information. To achieve this, the decoy should have certain Features. First, it 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. Thus, the decoy should seem authentic and trustworthy. Second, the decoy should be enticing enough to attract the attention of the attacker and make him/her open the File. Third, the decoy should be conspicuous, which is closely Related to being enticing. Whereas enticing is related to how Curious an attacker is about a decoy, conspicuousness has to do with how easy a decoy is to access. Therefore, the decoy should be easily located by search queries. Fourth, the decoy should be differentiable so that the real user can distinguish between the real and the decoy file. Balancing differentiability for authentic users with believability for attackers is one of the critical aspects of any decoy deployment system. Fifth, the decoy should be non-interfering so that the real user will not accidentally misuse the bogus information contained in the decoy. Finally, the decoy should be detectable; this feature refers to the ability of decoys to alert their owners once they have been accessed [8], [9], [10].

3. ALGORITHMS

In our system we use different algorithms for security of data stored in the healthcare cloud system. Previously said that when a attacker tries to access the data only the decoy files are retrieved and the original file is hidden it can be only accessible by the legitimate users after a set of verification tasks.

DMBD Algorithm

DMBD is like a trap gallery which is placed inside the fog computing like a honey pot to provide protection to the original data. The user directly accesses this DMBD the original data is retrieved only to the legitimate user after verifications. User profiling and decoy file systems are two anomaly detection systems provided by fog computing. For each uploaded data the corresponding Decoy data is created instantly.

User Profiling

User profiling algorithm is used to check whether a user is legitimate or not. It is performed on the basis of certain parameters. These parameters include behavior of search, amount of data downloaded, nature of operations, division of tasks and IP address. There are three different types of algorithms Explicit, Implicit and Hybrid. The Explicit algorithm is gathering from user profile and it contains high quality information but the difficulty is that it needs a lot of effort to update the profile. To overcome this problem Implicit is used it needs minimal effort from humans because it automatically update the user profile. Here we use Hybrid which is the combination of both explicit and implicit because here we need a large amount of interactions between the user and content.

Key Exchange algorithm

In this system there is a need to communicate the OMBD agent and DMBD in different situations. For example, when a user uploads medical data the OMBD agent need to inform about this updating to the DMBD to create a decoy file for the MBD this communication between these parties should be secured.

Mutual Authentication Protocol

This one is need to make secure communication between the parties those who communicate in this system. The parties can be defined as any user who uses, access, process on healthcare data.

Photo Encryption algorithm

This is used to encrypt photos to an understandable one. There are different types of photo encrypting algorithms are available here we use Blowfish algorithm. It is a symmetric key cryptography and the key length is large it make the algorithm most secured. It can encrypt any file format of photo with any size. The inputs would be the original photo and the encryption key. After that, based on the Blowfish algorithm length, the photo will be divided. The beginning of the array will be directly after the photo header since the header would not be encrypted. The array elements will be stored in rows, left to right ordered,

with every photo scan line represented by one row, and the photo rows will be encrypted from top to bottom [11].

Photo Decryption algorithm

This algorithm is used to provide the reverse of the encrypted photo. This process gives the original form of the photo. Here the same encryption key is used but the sub keys might be different.

Original MBD algorithm

This contains the original data and it is placed in the cloud system. The data is first upload to this system then using key exchange algorithm the corresponding decoy file is generated on fog system. The data in the cloud is encrypted to provide a double security for the OMBD.

LZW algorithm

LZW stands for Lempel Ziv Welch and which is used to compress the huge and complex data for effective memory utilization. There are two types of compression one is without losing any data and the other is with loss of data. LZW is a lossless compression algorithm that is there is no loss of data when compressing the huge data.

3. PROPOSED SYSTEM

The system is mainly focused on providing protection for the Medical Big Data in healthcare cloud using Decoy technique with fog computing facility. Here a decoy file called Decoy gallery or illusion gallery is created using decoy technique. This gallery is placed in the fog system which is closer to the end user and the user whether legitimate or attacker is access this data first. On the other hand the original medical data kept inside cloud with encrypted form. To confirm whether the user is legitimate or not using user profiling algorithm the legitimate user is entered only to the original data only after this verification. There is nothing to worry if any hacker gets access to the decoy file they get only the imaginary form of the original data and the hacker believe that they got the original one. The parties who came to use this system need to verify their authentication using Authentication protocol. At the end we use a compression algorithm to manage memory efficiently to store these data. Lempel Ziv Welch (LZW) is used as compression algorithm which is used to compress the huge and complex data for effective memory utilization. There are two types of compression one is without losing any data and the other is with loss of data. LZW is a lossless compression algorithm that is there is no loss of data when compressing the huge data.

4. CONCLUSION

We have already familiar with different methods or techniques to make secure different types of data. Here we focus on providing security for the records of patients in Hospitals. For this we use Decoy technique with fog computing facility. Here two galleries are created one is OMBD which is kept in the cloud and other is DMBD which is kept inside the fog. The user is first access DMBD and the OMBD is get only after verifying the user is original one. This technique provides more security to the data.

REFERENCES

1) I. Foster, Yong Zhao, I. Raicu, and Shiyong Lu. Cloud Computing and Grid Computing 360-Degree Compared. Grid Computing Environments Workshop, Austin, 2008.
2) P. T. Grance. (October 2009) The NIST Definition of Cloud Computing. Available online:http://csrc.nist.gov/groups/SNS/cloud-computing
3) Flavio Lombardi and Roberto Di Pietro. Secure Virtualization for Cloud Computing. Journal of Network and Computer Applications 2010, Volume 6, pp. 1-10.
4) Zawoad and R. Hasan. (Feb 2013) Cloud forensics: a meta-study of challenges, approaches, and open problems. Available online: http://arxiv.org/abs/1302.6312
5) Jonathan Voris, Jermyn Jill, Angelos Keromytis, and Salvatore Stolfo. Bait and Snitch: Defending Computer Systems with Decoys. Columbia University Academic Commons, 2013.
6) 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.
7) Bhaludra Raveendranadh Singh, S. Sunanda, Moligi Sangeetha Y. LakshmiKanth. A Secure Framework for Mollifying Attacks in Cloud.International Journal of Computer Trends and Technology 2014, Volume16, pp. 204-207.
8) Siddhesh P Karekar and Sachin M Vaidya. Perspective of Decoy Technique using Mobile Fog Computing with Effect to Wireless Environment. International Journal of Scientific Engineering and Technology Research 2015, Volume 4, pp. 2620 - 2626.
9) Majid Hajibaba and Saeid Gorgin. A Review on Modern Distributed Computing Paradigm: Cloud Computing, Jungle Computing and Fog Computing. Journal of Computing and Information Technology 2014, Volume 2, pp. 69-84.
10) Flavio Bonomi, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. Fog Computing and its Role in the Internet of Things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, 2012.
11) Pia Singh, Image Encryption and Decryption Using Blowfish Algorithm in MATLAB. International

Journal of Scientific & Engineering Research 2013,
Volume 4, pp. 150-154.