ISSN No:-2456-2165

Enhancing the Security of Cloud-Enabled Healthcare Portal using Decoy Technique

Avinash A Panicker[1], Divya Shaji Thomas[1], Indu Cyriac[1], Akshara Sasidaran[2]
[1]UG Student, Dept. of CSE, SJCET, Palai, Kerala, India
[2]Assistant Professor, Dept. of CSE, SJCET, Palai, Kerala, India

Abstract:- With the development of cloud computing, IoT, Big data and so forth have accomplished new grounds of utilization along with enhancement. Medication care experts utilize Electronic Medical Records (EMR) which includes different sorts of medical reports of the patients from hospitals, X-rays, MRI and so forth. All this information is archived on the healthcare cloud, which offers types of assistance like backup and maintenance of the patients Personal Health Data (PHI). Two essential concerns medical services suppliers face while picking a cloud arrangement are lack of security and privacy. With numerous data breaches progressively reported in these years, there is a developing anxiousness among the patients about the loss of their health information. The objective is to deceive the attackers and thereby make data breach difficult for them and consequently develop a framework focusing on using cloud computing along with decoy technique is proposed. Likewise, if the user is identified as an attacker, he/she will be provided with a fake data generated using decoy technique instead of the original data. The valid users can connect with others by utilizing a key arrangement protocol. A video hiding module is also added as an additional feature.

Keywords:- *Electronic Medical Records (EMR), Personal Health Information (PHI), Cloud Computing, Decoy Technique.*

I. INTRODUCTION

Medical big data in healthcare refers to medical records such as lab reports, x-rays, ultrasounds, MRI reports, etc. These data are huge and complex, due to these factors it is difficult to store in traditional software and hardware facility. Therefore, a healthcare cloud system can be used to place this data. Healthcare cloud is a cloud computing facility that is used as the storage medium for different medical data. It helps in managing and tracking the patient's healthcare information, even if the patient moves across multiple cities. As the popularity of the healthcare cloud increases, the attack on the system also increases. The main issue is related to the security of those data stored in the system. Data and privacy protection, policy issues, and legal issues are the security issues. The aim of this paper is to provide a secured healthcare cloud. To achieve this, the proposed methodology is to secure the patient's Medical Big Data (MBD) by using the fog computing facility along with the decoy technique. This decoy technique enables in providing a second gallery known as Decoy Medical Big Data (DMBD) that appears as the Original Medical Big Data (OMBD) which serves as a honeypot to the attacker, thereby deceiving him.

II. SCOPE

Any web enabled device from any location can use data, software, code and services over the internet through an internet-based environment known as cloud computing. The development of IT industry has influenced the developments in remote healthcare system immensely. It has made the providing of health services even in the remotest areas easy. These systems provide a platform for sharing medical information systems, infrastructure and applications in a format with the ability to provide automatic subscription. All these systems together can create a platform for collaboration of medical systems, the infrastructure and the applications in the form to provide autonomous subscription.

III. OBJECTIVE

The aim of the project is to create a secure Healthcare Cloud. A way to secure the data more tightly and make it more difficult for the attackers to obtain. What is required is a system that can deceive the attacker. Data integrity and user profiling is also needing to be done for ensuring the genuineness of the user. System utilizes decoy data technique to provide twisted or fake data along fog computing over the cloud which serves as a honeypot to distract the attacker along fog computing over the cloud. This is facilitated by a tri-party protocol for key agreement according to cryptography placed between the user of the system and the cloud.

Therefore, the objectives of the project include:

- A platform that provides data on-demand for its user.
- Data security.
- Data integrity.
- A platform that verifies the authenticity of the user.
- Should be able to successfully deceive the attacker by providing fake data on an attack.
- Decoy data should be produced without manual assistance.
- Simple Interface and minimal involvement of the users.

IV. EXISTING SOLUTIONS

A. *Azure IoT for Healthcare*

Azure IoT is a platform by Microsoft aimed at improving patient experiences, sharing and unifying clinical tasks and enhancing healthcare manufacture and chain of supply utilizing IoT.

B. *Cloud Healthcare API*

The Cloud Healthcare API provides a managed solution for storing and accessing healthcare data, providing a critical bridge between existing care systems and applications hosted on Google Cloud.

C. *HealthSuite Digital Platform*

HealthSuite Digital Platform by Philips is aimed to interconnect the devices and data. It archives and share the aggregated clinical and consumer data. It emphasizes on the standards of collaborations to enable secure sharing of data. Remote monitoring is also offered by HealthSuite Digital Platform.

D. *Apple Health Record*

All the medical records associated with a patient from multiple points are amassed in Apple Health Record. The data produced by the patient such as from that of smart wearables are also displayed. The service provides an integrated and current medical data of the user. But all their services are limited exclusively for Apple users.

V. PROPOSED SYSTEM

The proposed system is focusing on the usage of decoy technique and profiling of the user. The process generates two separate sets of photos: Original Photo Set and Decoy Photo Set. The default access is to the decoy photo set. The data stored in the original photo set is only accessible to those users who undergo profiling and is identified as the valid users. The nature or the behaviour of the user is observed for the purpose of profiling and classification is done accordingly. The amount and type of the data downloaded the frequency of accessing, the incorrect security answers and login attempt etc. can be utilized for the profiling and classification of the user. A key generator generates the key for the purpose of encryption and decryption of the original data as well as the decoy data.

VI. SYSTEM STUDY

For the purpose of better understanding of the system, it is divided into several modules.

A. *Login*

Every user must be registered in order to have a login. Admins, doctors, and patients can log in using their username and password. After login, if the username and password are valid, the system directs to the homepage. If the credentials are invalid, access will be denied.

B. *Administrator*

Administrator can view and manage user permissions. Admin adds doctors and patients into the system and checks the integrity of the data.

C. *Documents*

The document module handles all the operations related to the documents. Users can view a dashboard of all the existing documents associated with the patient. Addition or removal of documents is done here. When new documents are inserted, their encryption is done in the document module.

D. *Profiling*

The important part of profiling a user is handled in this module. The classification of user as genuine or fraudulent is based on certain criteria. Apart from monitoring their actions and frequency, generation of One Time Password for enabling also takes place over here.

E. *Decoy Data*

It is the key feature in which a decoy data is used to deceive the attacker. Decoy data is produced from the provided documents without user intervention utilizing techniques in image processing.

F. *Video Hiding*

Video files related to the patients need to be stored. These are encrypted onto an image to further enhance the security of the user.

VII. TECHNOLOGIES USED

Technology used includes Cloud computing, Fog computing, PHP, Python, MySQL.

VIII. IMPLEMENTATION

The project aims to provide a secure healthcare portal. Encryption of the data using Blowfish, AES, hashing is used for achieving this. User profiling is done when a user tries to access files by using certain parameters. If access from an unauthorized person is identified, decoy data is provided, instead of the original data, which serves as a honeypot to deceive the attacker.

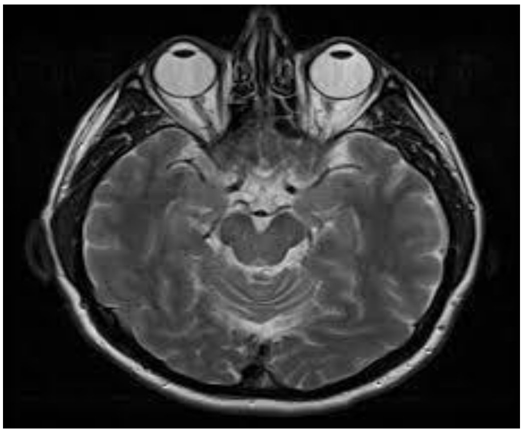

Figure 1. Original Image

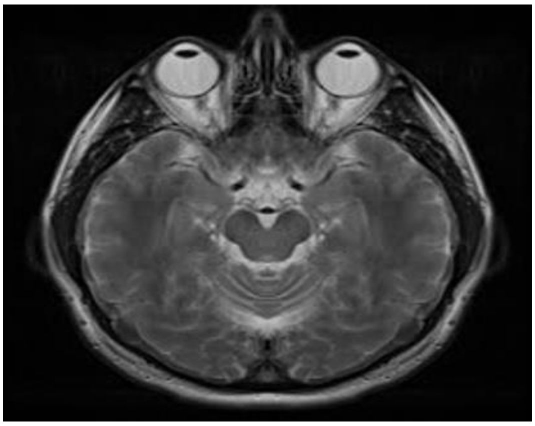

Figure 2. Decoy Image

IX. CONCLUSION

Medical data is termed as one of the most valuable forms of data. The data in cloud is more susceptible to attacks and theft attempts. For improving the security of the medical data, the proposed system emphasizes on safeguarding the user's Medical Big Data archived on the cloud utilizing the techniques of fog computing along with decoy data. This feat is achieved by producing two photo sets, Original Photo Set (OPS) and Decoy Photo Set (DPS). OPS is hidden and secured inside the Original Data Set. DPS is placed in the Decoy Data Set which acts as a honeypot for deceiving the attacker. Original Data Set is made available for only those users who have undergone user profiling successfully. The Decoy Data Set is kept as the default data access for all the users. The concept of hiding the Original Data Set and utilizing the Decoy Data Set to act as a safeguard, the vulnerability of the Original Data Set is reduced drastically. The tri-party agreement protocol for the key pairing cryptography between the user and the cloud for both the OPS and DPS facilitates this process. Therefore, the proposed system improves the security of medical data in the cloud.

REFERENCES

[1]. P. Khandge and S. B. Javheri," Implementation of Security in a Healthcare Cloud using Decoy Technique and Fog Computing Facility",2019 5th International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2019, pp. 1-4, doi:10.1109/ICCUBEA47591.2019.9129057.

[2]. Jaishree Jain, Dr. Ajit Singh," A Survey on Security Challenges of Healthcare Analysis Over Cloud", International Journal of Engineering Research & Technology (IJERT), Vol. 6 Issue 04, April-2017.

[3]. H. A. Al-Hamid and S. K. M. M. Rahman," Securing photos in the cloud using decoy photo gallery", 2017 International Conference on Wireless Communications, Signal Processing and Networking (Wisp NET), Chennai, 2017, pp. 816-822, doi: 10.1109/WiSPNET.2017.8299875.

[4]. H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren and A. 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," in IEEE Access, vol. 5, pp. 22313-22328,2017, doi: 10.1109/ACCESS.2017.2757844.