ISSN 2395-1621

Securing Information of Pathology Lab using Two-Factor Data Security Mechanism in Cloud

[#1]Prashant Bastapure, [#2]Rohit Satpute, [#3]Prashant Sonawane,
[#4]Rohit Mankar, [#5]Chudaman Sukte

[1]prashant123bastapure@gmail.com,
[2]rohitsatpute1650@gmail.com,
[3]prashantsonawane1996@gmail.com,
[4]mankarr11@gmail.com,
[5]rajeshsukte@gmail.com

MAEER's MIT COLLEGE OF ENGINEERING,
KOTHRUD, PUNE

ABSTRACT

In this paper, we propose a two-factor data security protection mechanism for pathology laboratory system. Our system allows a pathologist (sender) to upload an encrypted information of patient on cloud storage server. The pathologist (receiver) needs to possess two things in order to decrypt the cipher text. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. There are two types of storages in the system. First one is private data storage and second is public data storage. We have to upload and download data on private storage with the help of security device and in public data storage we can download data using secret key via e-mail. This process is completely transparent to the third party (admin). The security and efficiency analysis show that our system is not only secure but also practical.

ARTICLE INFO

Article History

Received: 18th May 2018

Received in revised form :

18th May 2018

Accepted: 21st May 2018

Published online :

22nd May 2018

Keywords: two-factor, security, authentication, cloud storage.

I. INTRODUCTION

This Cloud computing is a pervasive technology and has been a platform in IT for several years. Cloud service providers [3] have developed and offered different service platforms to accommodate different needs of enterprise subscribers. However, there still exists the situation of enterprise customers' hesitation and reluctance to deploy their core applications using cloud service platforms. Cloud storage [1] is a model of networked storage system where data is stored in pools of storage which are generally hosted by third parties. There are many benefits to use cloud storage. The most notable is data accessibility. Data stored in the cloud can be accessed at any time from any place as long as there is network access. The perception of data security in cloud computing platform can be enhanced by data visibility. Storage maintenance tasks, such as purchasing additional storage capacity, can be offloaded to the responsibility of a service provider. Another advantage of cloud storage is data sharing between users. If pathologist wants to share a piece of data to another pathologist, it may be difficult for her to send it by email due to the size of data. Instead, pathologist uploads the file to a cloud storage system so that another pathologist can download it at any time.

In this paper, System Administrator add the legal user (Pathologist) which can use the existing system. The basic concept of this system is user can upload patient reports and laboratory tests data on cloud infrastructure. The authenticate user can also download the data on demand. It can also share public data to other different pathologies through cloud before share the patient information authentication is taken form the patient. Patient will decide whether data to be shared or not.

In this system, the authenticate user upload private data with the help of unique portable device and also can download with the help of only that device. It can share also publicly the data help of group sharing. In this system private data and public data is stored separately to improve security of the data. Despite its advantages, outsourcing data storage also increases the attack surface area at the same time. For example, when data is distributed, the more locations it is stored the higher risk it contains for unauthorized physical access to the data. By sharing storage

and networks with many other users it is also possible for other unauthorized users to access your data. This may be due to mistaken actions, faulty equipment, or sometimes because of criminal intent. A promising solution to offset the risk is to deploy encryption technology. Encryption can protect data as it is being transmitted to and from encrypted data to the cloud.

1.1 Our Contributions

In this paper, we propose a novel securing information mechanism for data stored in the cloud. Our mechanism provides the following nice features:

1) Private storage:
In private section pathologist can store their private data. This data can be accessed by only authorized pathologist. Also modification in this section can be done by authorized pathologist. The reason behind this to provide confidentiality and accessibility.

2) Public storage:
In public section pathologist can store the patient data. This data needs authorization of the patients while accessing the data on cloud storage.

II. RELATED WORK

We first review some solutions which may contain similar functionalities. We will further explain why they cannot fully achieve our goal.

In Two-Factor Data Security Protection Mechanism for Cloud Storage System based on Identity-based encryption [1]. Whenever the sender wants to send a message to the receiver it takes only receivers identity, no other information is defined, also there is no authentication from the receiver side whether to accept message or not. Therefore confidentiality of this system is less.

Hence we overcome their vulnerabilities and added new functionalities like storing detailed information about sender and receiver who upload or download the data on cloud server. Every time, while downloading the data it takes authentication from the data owner (patient), because of this confidentiality of our system maintained.

In OTP-Based Two-Factor Authentication Using Mobile Phones [2], the OTP is generated and provided through SMS functionality of mobile. But in our system OTP is generated on cloud server and that is provided through e-mail Services, which provides more security than short message service.

In Cloud Based Two Tier Security Scheme for Store, Share and Audit Our Data into Cloud [3] ,this system provides third party audit which controls the overall system functionality and accessibility of public storage. Then we propose a secure cloud based storage system that support public auditing and preserve private and that allow the third party auditors to perform simultaneously and efficiently audits for multiple users.

III. EXISTING SYSTEM

In the existing system different key used between sender and receiver required more time to get the transmission done as compare to symmetric key cryptography. Also asymmetric key cryptography utilizes more resources as compare to symmetric key cryptography.

AES is the most convenient mode of encryption for data transition, due to the elimination of key management existed in symmetric encryption. Due to same key is used for encryption and decryption receiver must have the sender key. He cannot decrypt it without sender permission.

As cloud computing becomes more mature and there will be more applications and storage services provided by the cloud, it is easy to foresee that the security for data protection in the cloud should be further enhanced They will become more sensitive and important, as if the e-banking analogy. Actually, we have noticed that the concept of two-factor encryption, which is one of the encryption trends for data protection1, has been spread into some real-world applications, for example, full disk encryption with Ubuntu system, AT&T two factor encryption for Smartphones2, electronic vaulting and druva - cloud-based data encryption3. However, these applications suffer from a potential risk about factor revocability that may limit their practicability.

IV. OVERVIEW

4.1 Our Intuition

There are three modules as follows:
1. Admin module
2. User module
3. Group module.
4. Patient module.

Admin module:

The system administrator adds the legal user(pathologist) which can use the existing system. It can also have authority to remove the users and accessibility of the group modules data. It provides centralized control of the existing system. With the help of the centralized control it improves the security of the patient repots.

User module:

The basic concept of this system is user can upload patient reports and laboratory tests data on cloud infrastructure. The authenticate user can also download the data on demand. It can also share public data to other different pathologies through cloud. While uploading of the data it can automatically encrypted with the help of device. In this system, the authenticate user upload private data with the help of unique portable device and also can download with the help of only that device.

Group module:

It can share also publicly the data help of group sharing. In this system private data and public data is stored separately to improve security of the data.

Patient module:

In this module, patient register by using their credentials. When a user wants to download data from public storage, first he sends a request to the respective patient. Patient will decide whether data to be shared or not.

V. DETAILS OF OUR PROPOSED MECHANISM

In our mechanism we used traditional Public Key Encryption. There are two way of encryption data, first allow a user to generate cipher text under a receiver's identity using advances encryption standard algorithm. In second type encryption cipher text is generated with the help of security device. The resulting cipher text can be decrypted by a valid receiver with secret key and security device.

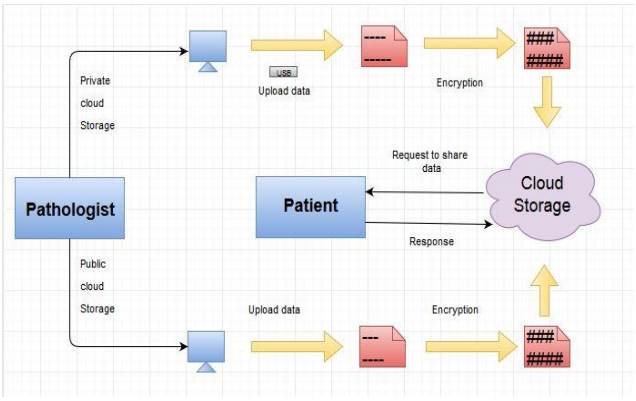

Figure.5.1 Upload Data on Cloud

In figure 5.1 shows the uploading of data by using two methods. First one is private data storage and another is public data storage. In private data storage we have to upload data by using security device. Firstly, pathologist login to system and whenever he wants to upload data on cloud first he has to attach security device in computer and upload data on cloud storage. When he uploads data it is in encrypted format by using AES algorithm. In public data storage, data is directly store on cloud storage without using security device and this data can be share all authorized pathologist in this system. In public data storage data is encrypted using AES encryption algorithm and store on cloud storage.

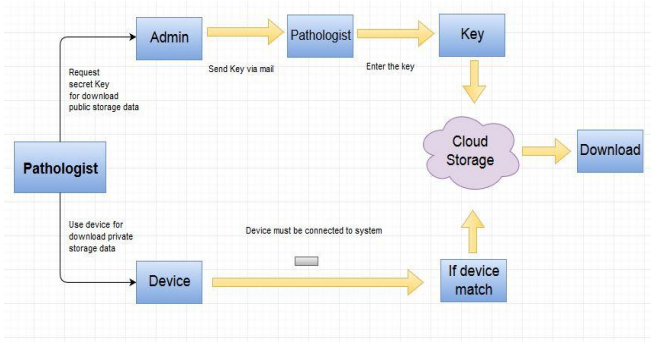

Figure.5.2 Download Data from Cloud

In figure 5.2 shows the two way of downloading the data first one is with the help of device download the private storage data. Pathologist login to system and whenever he wants to download the private data on cloud first sends a request to the respective patient. Patient [4] will decide whether data to be shared or not. And then attach security device in computer. Without the security device user is unable to download the private storage data. If user wants to download public storage data first he sends a request to the respective patient. Patient will decide whether data to be shared or not, and then he sends request to the admin for secret key then admin send the secret key on registered user email, by using the secret key user easily download the data.

VI. CONCLUSIONS

In this paper, we introduced a novel two-factor data security protection mechanism for pathology system, in which a data sender is allowed to encrypt the data with knowledge of the identity of a receiver only, while the receiver is required to use secret key and a security device to download the data. Our solution enhances the confidentiality of the data also we have provided two types storage facility first is private storage and public storage. So it is easy to maintain confidentiality of data. Hence receiver use security device for downloading the private storage data and using secret key download the public storage data Furthermore, we presented the security proof and efficiency analysis for our system.

REFERENCES

[1] Joseph K. Liu, Katia Liang, Willy Susilo, and Jianghua Liu: Factor Data Security Protection Mechanism for Cloud Storage System, IEEE Transactions on Computers (Volume: 65, Issue: 6, June 1 2016),30 July 2016.

[2] Mohamed Hamdy Eldefrawy, Khaled Alghathbar, Muhammad Khurram Khan: OTP-Based Two-Factor Authentication Using Mobile Phones, 2011 Eighth International Conference on Information Technology: New Generations

[3] Ms. Priya Kharmate, Prof. Ranjeetsingh Suryawanshi: Cloud Based Two Tier Security Scheme for Store, Share and Audit Our Data into Cloud ,2016 IEEE International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT)

[4] Harsha S. Gardiyawasam Pussewalage,Vladimir Oleshchuk: A Patient-Centric Attribute Based Access Control Scheme for Secure Sharing of Personal Health Records Using Cloud Computing 2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)

