Security Issues involved in sharing of Healthcare Information's Through Cloud Storage

P.Subhasri [*1], Dr.A.Padampriya [2],
[1] Research Scholar, [2] Associate Professor,
[1,2] Department of Computer Science, Alagappa University – Karaikudi,
[1] swarnasubha91@gmail.com
[2] mailtopadhu@yahoo.co.in

Abstract— **The evolution of cloud computing in healthcare management systems provides better storage and sharing of medical records through the network. In healthcare systems, cloud not only facilitates the exchange of electronic medical records but it also enables to share the contents in a secured way. The storage of HIS (Healthcare Information Systems) in cloud provides greater flexibility but at the same time it has security issues. By storing the information in cloud the availability and accessibility is easily achieved. This paper aims to describe the security issues involved in storing Healthcare information cloud.**

Keyword - Healthcare Information Systems, Cloud computing Services, Cloud security challenges, Authentication.

I. INTRODUCTION

With the increase in advancement of healthcare sector, the medical record of patient also increases. The enormous growth of medical records pose a very big challenge for healthcare experts as they have to manage, share and process the contents without any loss. Medical records sharing system enables the records to be shared among the stakeholders [1]. The need for sharing is for quick and easy access. Cloud computing is a promising solution to share the healthcare information over the internet. It is an on-demand network access to share a pool of configurable computing resources with minimum managing effort and good service provider interaction [1]. Cloud computing will helps the users in handling the healthcare information efficiently, expanding the storage capacity and providing secured access to the information by access control mechanisms.

The main advantages of sharing medical contents [7] through cloud computing is, i). To improve the quality of care provided, ensuring the patient gets well faster as a secured way. ii). To increase the safety of the contents with its access control policies. iii). To reduce the cost for patients because this eliminates the need for repeat tests and scan. In this paper the various challenges involved in sharing healthcare information through cloud platform is described. The issue associated with sharing of information especially medical images through cloud, the existing solutions and its limitations are also discussed in this paper.

The paper is organized as follows. Section 1 provides a general introduction of storing and sharing the medical contents using cloud. Section 2 presents a brief study of the cloud computing services, security issues and background work. Section 3 elaborates the benefits and challenges of information sharing and analyses the cloud security issues. The contributions are concluded in section 4.

II. CLOUD COMPUTING SERVICES

The main objective of cloud computing is to share the data from provider to end users through the internet. Cloud computing provides various types of services to share healthcare information rather than a unit of product [3]. These services provide easy and flexible sharing of medical records. The basic types of services [3] as discussed as follows,

Web-based cloud services: This can be use on web service functionality, rather than using fully developed applications. It includes an application programming interchange for Google maps, and also the payroll or credit card processing.

Saas (software as a service): This services provides a given application to multiple tenants, typically using the browser saas solutions are common in sales, HR and ERP.

Paas (Platform as a service): This service is the different type of saas. The user runs their own application but they do it on the cloud provider's infrastructure.

Utility cloud services: There are virtual storage and server options that organizations can access on demand, even allowing the creation of a virtual data centre.

Managed services: In this type of services, a cloud provider utilizes an application. Anti-spam services or even application monitoring services is one of the managed services.

Service commerce: This service of cloud solutions are a mix of SaaS and managed services. It includes expense tracking, travel ordering or even virtual assistant services.

2.1 Cloud Computing Security Issues

The cloud service provider for cloud makes sure that their customer/user does not face any security problems similar to data loss and data theft. There are three types of issues [3] may raise while discussing about the security of the cloud.

Data issues

Whenever a data is stored on a cloud, anyone from anywhere at any time can access it. So, data stealing and modification is a serious issue in cloud computing environment. Data protection in cloud computing is the main factor to reduce the data security issues in the cloud. When data protection is needed, encryption methodologies can be used to store the data on the cloud in a secured manner.

Privacy issues

When the data stored in a cloud, the malicious users may upload infected applications to affect the entire processing. In such case authentication is the best solution to preserve the privacy of data.

Security issues

Cloud computing security can be done on two levels. One is provider level and another one is user level. The provider level composed the security of the shared data and the user level satisfies the trust during the processing from the cloud. The cloud is good only when there is a good security provided by the service provider to the user. So the security mechanism of the stored data is much more important.

2.2 Background Study

Rabi Prasad Padhy et al. in 2012 [5] have proposed a cloud based model for developing the healthcare systems. In this paper, the authors implemented cloud computing system in healthcare is not to compete with each other but serves to facilitate and improve the quality of patient care. They present a cloud based rural healthcare information system model to store medical records of their patients on cloud.

Chia-Chi Teng et al. in 2012 [2] developed a framework for medical imaging applications to securely communicate the medical image with cloud computing. The author provides a framework which is cloud-based image storage and management service using a standard DICOM protocol. The design and implementation of this system demonstrated the feasibility of using the cloud computing infrastructure to provide an image repository and processing platform for some mobile devices.

Chenghao He et al. in 2010 [1] has proposed a solution to simplify the network module that are connected within the hospitals by the use of cloud computing. This paper is based on the concept of information sharing and high-end processing is available in the cloud. The author describes a cloud based HIS management system which contains the framework of all hospital data that can be acquired from the cloud.

III.CLOUD BASED HELATHCARE INFORMATION SYSTEMS

Online medical contents sharing system allows physicians to built a better network for storing that medical information's [2]. Cloud computing provides massive storage applications with highly managed remote services, so it has gathered a specific attention from information technology vendors. Generally cloud platform is an exchange stand which is used by all healthcare organizations and can be used as a storage centre for the purpose of storing medical records. In HIS (Healthcare Information System) reliability and security are the main concerns.

3.1 Benefits of Sharing Medical Information on Cloud Platform

Ease of Access

When compared to traditional server-based medical records storage system with cloud computing, cloud based storage system provides much faster and very easier to access. Because all the medical contents are accessed from the cloud computing based centralized system, user can access the information's from anywhere with internet connection [6].

Cost

Sharing of medical records on cloud platform is cost effective. Some of the studies showed that the use of cloud technology can decrease the cost by minimizing the hardware, software and on-site IT costs.

Increases Productivity and Efficiency

In cloud technology there is no need to upgrade individual technology, because the storage regulations compliance, backup systems and disaster recovery are managed in centralized mode. The users and healthcare professionals save the time by accessing this information from the cloud.

Creating a More Connected, Patient-Centric System

With the help of the cloud storage, the healthcare professionals can quickly access and share the medical information about a patient across one hospital sector to other. Storing the medical records in one centralized repository in cloud has good advantage instead of storing the medical information in multiple PACS at different locations.

3.2 Challenges in Sharing Medical Information on Cloud Platform

Some of the challenges and issues in sharing of medical information on the cloud platform are discussed as follows,

Distributed Denial of Service Attacks

The main security threat in sharing medical information system is Distributed Denial of Service Attacks [7]. The hacker exploits its weakness in cloud methods and easily accessible tools to launch these attacks.

Solution: The cloud Administrator provides a strong password protection mechanism to access the stored medical contents against Distributed Denial of Service Attacks.

Confidential Data Leakage

The top security issue in cloud is confidential data leakage [4]. The service provider of the cloud have to take steps to protect the confidentiality of the stored information, otherwise the hackers may be mishandle the stored data.

Solution: Authentication based Access control mechanism is the better solution against this confidential data leakage issue. Because when the access control mechanism is processed, then only the cloud service providers know who are using the stored data.

Security issues in Sharing of Information in Cloud

The main data security issues are raised in sharing the medical information in cloud is privacy, confidentiality, integrity and availability. It refers to technological tools used to protect identifiable health care data from unauthorized access [4].

Solution: Cryptographic solutions are the main methods to store the ciphered content on cloud, because the authorised person only knows the mechanism to decipher the content.

3.3 Analysis of Cloud Security issues

The following four types of cloud security issues are analysed and its solutions are listed in the following table,

TABLE I. Cloud Security Issues with solutions

Issues	Description	Solutions
Data Security	Normally involves the protection of data from Confidentiality, Integrity and Availability aspects.	Cryptographic techniques are implemented to secure the data.
Network Security	Involves the security of network from attacks such as spoofing, Denial of service, Man in the middle attack.	Password based Authentication mechanism is the best way to secure the stored content against attacks.
Virtualization Security	Hypervisor is the main target of hackers. Allocation and de-allocation of memory.	Access control based authentication is the better way to prevent the attacks.
Audit and Compliance	Problem of the verification of authorization and authentication records.	Privileged users monitoring is accessed by the cloud administrator with the help of registration concerns.

3.4 Features to be incorporated

- To provide a complete analysis and get the perfect solution to maintain the integrity, confidentiality and authentication on the storage medical details on cloud.
- To provide a simple and user friendly interface to the commonly required functionality.
- To present a standard consistent model for common cryptography tasks.
- To define trust boundaries between Cloud Providers (CP) and consumers to clearly establish and promulgate boundaries of responsibility for providing security.

IV. CONCLUSION

Cloud computing technology includes a set of important policy issues like privacy, security, anonymity, reliability, telecommunications capacity and among others. But the important aspect between them is security and how the cloud providers assure it. The storage of HIS (Healthcare Information Systems) on cloud provides the quality and security of the patient details. This paper analyses the security issues on cloud and provides the solutions for that security issues. And also this paper concludes that the sharing of healthcare information's on the cloud platform is easy, quite efficient and more flexible to use.

REFERENCES

[1] Chenghao He et al., "A cloud computing solution for Hospital Information System", http://ieeexplore.ieee.org/document/5658278.
[2] Chia-Chi Teng et al., "Mobile Ultrasound with DICOM and Cloud Connectivity", Proceedings of the IEEE-EMBS International Conference on Biomedical and Health Informatics (BHI 2012) Hong Kong and Shenzhen, China, 2-7 Jan 2012, pp. 667-670.
[3] Cloud computing principles, systems and applications NICK Antonopoulos http://mgitech.wordpress.com.
[4] Dr.A.Padmapriya and P.Subhasri, "Cloud Computing: Security Challenges & Encryption Practices", in International Journal of Advanced Research in C4omputer Science and Software Engineering (IJARCSSE) in March 2013 Volume 3, Issue 3, ISSN: 2277 128X, pp. 255- 259.
[5] Rabi Prasad Padhy et al., "Design and Implementation of a Cloud based Rural Healthcare Information System Model", UNIASCIT, Vol 2 [1], 2012, ISSN 2250-0987, pp. 149-157.
[6] P.Subhasri and Dr.A.Padmapriya, "Multilevel Encryption for Ensuring Public Cloud", Accepted in International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) in July 2013, Volume 3, Issue 6, ISSN: 2277 128X. pp. 527-532.
[7] The ultimate guide to implementing a medical image sharing portal, http://www.dicomgrid.com/, last accessed on 15/10/2016.