Cloud Based Medical Image Exchange-Security Challenges

Shini.S.G\(^a\), Dr.Tony Thomas\(^b\), Chithraranjan.K\(^a\)

\(^a\)Sree Chithra Thirunal College of Engineering
\(^b\)Indian Institute of Technology and Management-Kerala
Thiruvananthapuram, Kerala, India

Abstract

Cloud-based medical image sharing platforms are increasingly becoming more prevalent in medicine. Ultimately online medical image transfer systems allow physicians to build better and deeper referral networks, which in turn mean increased volumes and a more open platform for collaboration. Cloud computing has gathered specific attention from information technology vendors in providing massive storage applications and highly managed remote services. Cloud platform can form an exchange platform that all healthcare organizations use and can serve as storage center of medical records. Reliability and security are the main concerns about cloud computing. Adopting cloud computing can result in both positive and negative effects on data security. This paper presents a study about the security issues involved in data storage and sharing through cloud. It highlights the different types of security problems and how their existence can affect the cloud users.

© 2012 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of Noorul Islam Centre for Higher Education

Keywords: Cloud Computing; Cloud Based Medical Image Exchange; Security; Privacy.

1. Introduction

Enormous increase in medical images presents a big challenge for healthcare providers as they have to manage, share and process this data while reducing costs. The explosive growth in amount of medical imaging data are due to certain factors such as increasing age of patient population, new medical imaging technologies such as 3D imaging, PET/MR scans, increase in size of data studies etc. Many of medical organizations do not have much IT resources or storage for managing the increasing volume of data. Cost and security are main evaluating factors for managing data storage and access.

Medical record sharing [1] enables medical records to be shared across all healthcare establishments, starting with public hospitals and polyclinics and progressively to healthcare establishments in the private and charity sectors. With quick and accurate access to essential
medical information, medical staff involved in treatment can customize treatment to better meet patient’s unique needs, wherever he is. The main advantages are

1. Improves the quality of care provided, ensuring that patient gets well faster.
2. Increases the safety. For example, ready access to information about patient’s drug allergies and current medications enables doctors to prescribe medication accurately and reduce unnecessary side effects.
3. Reduces the cost for patients as doctors can now view the results of any recent blood tests, x-rays, CT Scans etc; an investigation online, thereby reducing the need to repeat the tests.

In the past, film was the medium used to share medical images with multiple health care services [2]. But it was expensive, clumpy and inefficient. Then compact disc (CD) is appeared [3]. The main advantages of CD are low cost, portability and high storage. CDs have a different viewer which differ in many ways and are often are not intuitive to new users or to occasional users to use them. Further, Discs can become defective and unreadable. Then emerged technologies like peer-to-peer (P2P) [4] systems and cloud computing [5] that are capable of enabling sharing of medical records across autonomously managed heterogeneous healthcare information systems.

In this paper we describe the various mechanisms for medical image storing and sharing of medical images through cloud platform. The issues associated with the sharing of medical images through the cloud, the existing solutions, their limitations and future direction for then described. The rest of the paper is organized as follows. In section 2 we describe the cloud based medical image storage and sharing mechanisms and associated security issues. In section 3 we discuss the existing technologies and related works and analyses them. In section 4 we discuss the future direction for research. The conclusion is in section 5.

2. Cloud Based Medical Image Exchange

Cloud Based Medical Image Exchange provide on demand medical imaging information technology (IT) services from remote or remotely managed third-party platforms over a network. Medical imaging is the process used to create images of the human body (or parts and function thereof) for medical procedures seeking to reveal, diagnose or examine disease. Medical images are the main means of the healthcare diagnostic procedures. Medical images come from a board spectrum of imaging technologies such as computed axial tomography (CT), magnetic resonance imaging (MRI), digital mammography and positron emission tomography (PET), and they generate a large amount of image data and important medical information.

The MRI, Ultrasound scan and CT images are mainly stored in digital formats which are related with the patient data and information. One of the main digital format used for medical imaging is DICOM (Digital Imaging and Communication in Medicine).It is a standard for handling, storing, printing and transmitting information in medical imaging.DICOM files can be exchange between two entities that are capable of receiving image and patient data in DICOM format. A DICOM file consists of two parts, a file header and a data set part, as shown in Fig.1.The File header contains identification information while Data Set part contains the actual medical image. The header consists of a 128 byte File Preamble, followed by a 4 byte DICOM prefix. A Data Set represents an instance of a real world Information Object. A Data Set is constructed of Data Elements. Data Elements contain the encoded Values of Attributes of that object. The Transfer Syntax used to encode the Data Set shall be the one identified by the Transfer Syntax UID of the DICOM File Meta Information.
Cloud services enable storing, archiving, sharing and accessing images which allows the healthcare organizations to manage data more efficiently and cost effectively [1]. Cloud based medical image sharing is a very cost-effective solution because it doesn’t require monetary investment in a lot of hardware. After confirming the identities of each provider, cloud medical image sharing can proceed over a virtual private network (VPN). As part of this connection, the provider receiving the image uses a password sent via email to log into the cloud server and see the studies. A secure cloud-based medical imaging exchange can speed access to pertinent current and historical imaging studies. It securely connects referral hospitals, physicians, and specialists online, enabling organizations to leverage their existing RIS and PACS systems. Hospitals that deploy a medical image exchange can view and share images and reports with their referral partners in real time, without relying on physical media such as CDs.

The sharing and exchanging of medical images through cloud can be of two paradigms [6]. The first method is to provide a set of services in the cloud that move medical images between sites on demand. The second method includes archiving the medical data in cloud so that original source sends images into cloud only once. Through the cloud, medical image sharing will help patient safety and satisfaction by cutting down on the number of duplicate tests, potentially saving money and protecting people from unnecessary side effects of repeated tests. The benefits of putting medical images in a cloud include:

a) **Data Portability:** With online patient health records, it is easier to access and share data between the patients and doctors and between the specialists.

b) **Increased and Flexible Storage Capacity:** With cloud-based EMR, doctors and other healthcare professionals do not have to administer/upgrade their own hardware. Additional data storage is available as needed.

c) **Data Migration:** The main benefit of cloud technology is that data need to be migrated only once. Then the data can be accessed and utilized with any PACS. It is necessary for an organization
to work with a vendor that can migrate data efficiently, since it is time and resource intensive criteria.

d) Patient-Centric Connected System: Consolidating and storing medical image information in single centralized repository in the cloud instead of multiple PACS in different sites means health care providers can quickly access and share images across various departments and organizations. The schematic diagram for sharing of medical images through cloud is shown in Fig 2.

Fig 2: Sharing medical image through cloud

Cloud based services adopt a principle for medical image sharing called server-side rendering or remote rendering[7], meaning all of the image rendering, processing, etc. being directed by the user is actually being executed on the server in the cloud. The result of this rendering, an HTML page, is all that is actually downloaded to the user’s PC. The actual image data itself is not downloaded to the user’s PC. The actual image data itself does not leave the secure server in the cloud. This technology solves the problem of moving large data sets from the PACS archive to a diagnostic or clinical workstation for them to be rendered. This solution totally avoids the data incompatibility problems encountered when an organization attempts to actually import digital image data from an ‘outside’ PACS into their local PACS. Instead of importing ‘outside’ study data into the local PACS, so the images can be accessed and viewed by the physicians using the local PACS web viewer. The cloud solution depends on its own embedded display application to access and display the image data.

2.1 Limitations

Although cloud sharing makes image transfer faster, often streamlining and improving patient care, the biggest stumbling block to widespread use is still fear and unease about the technology. Some of the limitations of storing and sharing of medical images through cloud are mentioned here. The first hurdle for many facilities and practices is having the proper high-speed bandwidth needed to quickly transfer images. Primary storage, deduplication and compression will minimizes bandwidth consumption dramatically while also increase performance. Image latency has become a critical issue for the user community under cloud due to low bandwidth. User acceptance of image rendering and analysis applications is often driven by performance criteria. It is unclear that remote rendering will provide sufficiently low display latency for all medical imaging applications when the server must be accessed over the internet. Latency [8] is controlled by the lowest bandwidth pathway in the communication exchange. High bandwidth networking in a remote data center
cannot overcome the limitations of relatively low bandwidth, shared communication links. Medical images stored in cloud should be available to the doctors at time they queried. Delay in accessing may cause dangers to patient’s life during situation like surgery. There can sometimes be a temporary or permanent, partial or complete disruption to the cloud service, also known as downtime. Primary causes of downtime include internet bandwidth, equipment and software malfunction, natural disasters.

2.2. Security issues in Cloud based Medical Image Exchange

Security has been the primary focus in cloud based medical image sharing and movements have been made across multiple fronts to protect the information. Security [9] refers to physical, technological or administrative safe guards or tools used to protect identifiable health data from unauthorized access or disclosure. The main data security components are privacy, confidentiality, integrity and availability. Security and privacy requirements extend to all aspects of the storage environment, including data protection and disaster recovery—representing another burden on already stressed health care organizations. Securing medical images can be more challenging compared to other aspects of electronic protected health information as they are often transmitted between providers if a patient moves or seeks additional care from another entity. Privacy is about the protection and careful use of the personal information of patients. Confidentiality is the assurance that sensitive information is not disclosed. For example medical image data should not be accessed by unauthorised parties. Integrity checking mechanisms prevents unauthorised modification of data. For example received medical images have not been modified during the transmission. Availability, refers to the notion that data and services are available for use when needed. The main threats in image storage and sharing in cloud are given below.

2.2.1. Distributed Denial of Service attacks (DDoS)

One of the main security threats to cloud based medical image sharing is DDoS [10] attacks. This attack is a threat to the availability of cloud infrastructure and its resources. Hackers are exploiting weakness in cloud defence methods, utilizing cheap, easily accessible tools to launch these attacks. The data centers and cloud operators are not well prepared to defend against them. Firewalls and IPSs are essential solutions for a layered defence strategy, but they are designed to solve security problems that are fundamentally different from dedicated DDoS attacks. Existing solutions mainly concentrate mitigating these attacks by keeping a small attack surface, monitor traffic regularly, block whatever traffic makes up an attack as soon as possible and block access to ports that only need to be accessed from specific locations, on As this attack become more threatening, data center operators and cloud service providers must find new ways to identify and avoid DDoS attacks.

2.2.2. Confidential Data Leakage

Confidentiality of medical images stored in cloud is a top security issue. Cloud providers have taken steps to protect confidentiality of their content in their legacy data centers because of high costs from disclosures, penalties resulting from breaches, and loss of reputation. Confidentiality of data cannot be maintained and protected easily because of lack of visibility, sharing of information and attacks of malicious insiders.

Cloud environments pose different obstacles for protecting confidentiality of medical data. In infrastructure as-a-service (IaaS) environments, customers have the ability to create corporate infrastructure in the cloud. Encryption, access control and monitoring can reduce the threat of
information disclosure. However, modern content security monitoring and filtering solutions may be difficult or impossible to deploy due to architectural or other limitations in this cloud environment. In platform-as-a-service (PaaS) environments, customers can quickly spin-up new Web, database and email servers, but will find they have even fewer ways to do any monitoring or protection of content than in an IaaS environment. Customers with confidential content are at the greatest mercy of vendors in SaaS environments. With few exceptions, there is no way for a customer to ensure security of content at a SaaS provider. He must be completely trusted and trustworthy (and bound by a strong contract) to maintain security on behalf of the customers.

Encrypting a medical image file before it’s sent to cloud can secure the confidentiality of images[11]. The existing security techniques can scramble the image file such a way that it can only be accessed with a password. However, encrypted images can only be accessed by the user – regardless of where the file is stored. The stored images could be protected by using encryption. A cloud provider can protect data in transit by encrypting it in the pipe between the provider and the service consumers system.

2.2.3. Access Control

Abuse usage of cloud power by cyber criminals is the main threat to security of contents in cloud. Existing systems has a low barrier to entry, which makes it easy for hackers to launch security attacks on cloud computing resources. For some companies, the nature of the cloud allows any person with a valid credit card to register and use cloud services. Spammers, malicious code authors and other criminals can use these platforms to launch denial of- service attacks, host botnet command and control servers, perform password and key cracking and other malware and infect legitimate tenants in the cloud systems. Existing solutions are outsourcing the access control structures to the “cloud”, introduces immediate privacy concerns. A good solution should ensure that the access control structures are not leaked to the cloud provider, while still allowing the remote sites to use them to verify access rights and help in enforcing access decisions [11].

2.2.4. Data ownership:

In general, the owner is defined as the creator of the information. Establishing the ownership of the information is necessary for protection against unauthorized access or misuse of patient’s medical information. The ‘owner’ can refer to the person responsible for the information or the organization creating and storing the information. The term of ‘owner’ may refer to ‘creator’, ‘author’ and ‘manager’ of the information. The embedding of the ownership seal in the images is achieved through means of watermarking and encryption techniques

2.2.5. Zero tolerance:

Due to encryption or watermarking, spots will appear in medical images retrieved from cloud. This may lead to wrong interpretations like presence of tumours; outgrowth etc. On the basis of these details doctors may give fault diagnosis. For preventing this zero tolerant images is needed in which watermarking techniques should be performed carefully. It requires extreme care when embedding additional data within medical images because this information must not affect the image quality.
3. Related Works

Cloud computing [5] is a type of parallel and distributed systems that have a large pool of easily usable and accessible virtualized resource. These resources can be dynamically adjusted for different application requirements. Cloud provide services such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) [12]. Cloud is available at Private, Public, Community and Hybrid levels [13]. The advantages of cloud computing include low cost, high storage, openness and graceful failure, convenience in control and environment sustainability. At present there exist many Cloud services providers like Hadoop, Amazon Compute Cloud EC2, Microsoft Azure and Google AppEngine[14][15][16][17].

In [18], the authors proposed a system called MIFAS (Medical Image File Accessing System) to solve the problems in exchanging, storing and sharing of medical images. They utilized Hadoop platform and coallocation mechanism to establish cloud environment for MIFAS. MIFAS could easily enable users to retrieve, share and store medical images among different hospitals. The system’s workflow is like this: user first inputs username and password for authentication; users then input search condition to find patient’s information; user could then view patient’s medical images. The author compares PACS [19] with MIFAS on the basis of image retrieval time, proximal failure problem, synchronization and concurrency. They proved that MIFAS is better and is scalable, cost effective and easy to manage.

In [20], the authors designed and implemented a medical image archive service using DICOM [21] standard as a cloud computing based solution under Microsoft Windows Azure platform and tools. The prototype consists of 1) a DICOM server which handles standard DICOM store/query/retrieve requests; 2) a DICOM image indexer that parses the metadata and store the information in a SQL Azure database; 3) a web user interface implemented in ASP.NET and Microsoft Silverlight technologies that allow users to search and view archived DICOM images based on any combination of DICOM tags. This system can lower the storage and management and to increase disaster recoverability.

In [19], the author presents a module of PACS Cloud architecture to grant interoperability with DICOM devices. PACS Cloud Gateway is a component of PACS Cloud, which focuses mainly on the translation from DICOM commands to non-DICOM and vice-versa. This Gateway focuses on full compatibility with DICOM standard. It has important services like DICOM storage and DICOM query/retrieve, capable of storing, querying and retrieving data from repository. PACS cloud must grant access to archive server at anytime. The proposed PACS cloud architecture is designed such as to separate sensitive data elements manipulation from demanding computational operations. In this system data are in the cloud, but the provider cannot do anything with it because they are all encrypted and the keys live in Master index, where cloud provider doesn’t have access. Main advantages of the system are scalability and reliability of data.

4. Future Research Directions

Cloud based medical image exchange has unique attributes that raise many security and privacy challenges in areas such as data security, recovery, and privacy, as well as legal issues in areas such as regulatory compliance and auditing. The main research areas are:- When clients store their medical data on the server without themselves possessing a copy of it, how the integrity of the medical data can be ensured if the server is not fully trustworthy? Will encryption solve the data confidentiality problem of sensitive data? How will encryption affect dynamic data operations such as query, insertion, modification, and deletion? Medical data in the cloud is typically in a shared environment alongside data from other clients. How the data segregation should be done, while data are stored, transmitted, and processed? Data anonymization and privacy preserving techniques will increasingly assume greater importance in cloud based medical image exchange and more mainstream research are required in this area.
5. Conclusion

Medical Imaging and Cloud computing could become the most data and computing intensive activities in future. Cloud is an emerging approach for various medical imaging applications. In this paper we discussed about cloud based medical imaging mechanism and analyzed the various security issues associated with this approach. We examined the current solutions and discussed their limitations. Finally we discussed the future directions for research.

References

[1] Zhuo-Rong Li, En-Chi Chang, Kuo-Hsuan Huang, Feipei Lai, "A Secure Electronic Medical Record Sharing Mechanism in the Cloud Computing Platform," IEEE 15th International Symposium on Consumer Electronics 2011, pp. 450-457.

[2] Mendelson DS,Bak PRG,Menschil E and Siegel E,"Image Exchange: IHE and evaluation of image sharing",J Radiographics,2008,pp.1817-1833.

[3] Sodickson A,Praseth JLedbetter S,"Outside imaging in emergency department transfer patients:CD import reduces rates of subsequent imaging utilization",J radiology,2011,pp.408-413.

[4] Sivatsa, M. Gedik, B. Ling Liu, "Large Scaling Unstructured Peer-to-Peer Networks with Heterogeneity-Aware Topology and Routing",IEEE Transactions on Parallel and Distributed Systems ,2006,pp.1277-1293.

[5] Luis M. Vaquero, Luis Rodero-Merino, Juan Caceres, "A Break in the Clouds: Towards a Cloud Definition," in ACM SIGCOMM Computer Communication Review, January 2009, Volume 39, Number 1.

[6] Steve G.Langer,"Challenges for Data Storage in Medical Imaging Research",Journal of Digital Imaging,2010,pp.203-207.

[7] James Philbin,Fred Prior and Paul Nagy,"Will the Next generation of PACS be sitting on a Cloud?",Journal of Digital Imaging,2010,pp.301-305.

[8] Jiang Bian, Remzi Seker and Umit Topaloglu, "A Secure Distributed File System for Medical Image Archiving", IEEE International Conference on Social Computing 2010, pages 961-967.

[9] COHN, S. P., "Privacy and confidentiality in the nationwide health information network", online at http://www.ncvhs.hhs.gov/060622lt.ht.,2006

[10] Bakshi, A and Yogesh, B,"Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine", ICCSN ’10. Second International Conference on Communication Software and Networks, 2010, pp.260-264.

[11] Shucheng Yu,Cong Wang,Kui Ren and Wenjing Lou,"Achieving secure, scalable, and fine-grained data access control in Cloud Computing",INFOCOM 2010.

[12] Gerald Briscoe,Alexandros Marinos,"Digital Ecosystems in Clouds: Towards Community Cloud Computing",Department of Media and Communication London School of Economics and political science.

[13] Rajkumar Buyya, Chee Shin Yeo, SriKumar Venugopal,"Market Oriented Cloud computing environments and the Cloudsim Toolkit: Challenges and opportunities", 2009.

[14] Amazon Elastic Compute Cloud(EC2),http://www.amazon.com/ec2.

[15] Apache Hadoop project,http://hadoop.apache.org/hdfs.

[16] Microsoft Windows Azure,http://www.microsoft.com/azure.

[17] Google App Engine,http://appengine.google.com.

[18] Chao-Tung Yang,Lung-Teng Chen,Wei-Li Chou,"Implementation of a Medical Image file Accessing System on Cloud Computing"IEEE international Conference on Computational Science and Engineering 2010, pages 321-326.

[19] Luis A,Bastiao Silva,Carlos Costa,Augusto Silva and Jose Luis Oliveira,"A PACS Gateway to the Cloud", IEEE International Symposium on Electronics and Telematics Engineering 2011, pages 335-340.

[20] Teng C, Mitchell J, Walker C, Swan A, Davila C, Howard D,Needham T," A medical image archive solution in the cloud. "In:Software Engineering and Service Sciences (ICSESS) – IEEE International Conference Beijing: 431-434.

[21] DICOM, http://medical.nema.org/.