Cloud based Information Security and Privacy in Healthcare

Divya Raval
PG Student,Dept of IT
V.E.S Institute of Technology
Mumbai, India

Smita Jangale
Associate Professor, Dept. of IT
V.E.S Institute of Technology
Mumbai,India

ABSTRACT
Cloud computing is emerging as a promising prototype for computing and is drawing the attention from both academia and industry. The cloud-computing model is transferring the computing infrastructure to third-party service providers that manage the hardware and software resources with important cost reductions. It is emerging as a new computing example in the medical field apart from other business domains. Wide number of health firms has started shifting electronic health information to the cloud environment. Initiating cloud services in health sector will not only simplify the exchange of electronic medical records between the hospitals and clinics, but also enables the cloud to act as a medical record storage center. Besides, moving to cloud environment eases the healthcare organizations from the monotonous tasks of infrastructure management and also reduces development and maintenance costs. The medical data stored in cloud makes the treatment systematic by retrieving patient's medical history from the database before going for the treatment and get to know about the health issues of the patient.

General Terms
Health Care, Health Information Technology (HIT), Electronic Health Record (EHR), Cloud Computing, HIPAA Compliance.

Keywords
Attribute Based Encryption (ABE), DDoS, Personal Health Record (PHR).

1. INTRODUCTION
Hospitals are organizations which generally process a lot of information daily. Think for instance of the medical information of patients: a normal hospital is visited by thousands of patients each year and for each patient, the hospital needs to store contact information, insurance information, appointments with medical specialists, and a medical data: medical reports, radiography pictures, laboratory reaction and more. All this information is processed by various persons inside a hospital organization. Medical professionals need to access medical information for effective treatment of a patient; administrative departments need to be aware of which medical operations have been performed to be given reimbursement etc. The amount of information that hospitals process and the inherent features of this information make it important that hospitals handle this. Information with care. Medical information is sensitive information, and hospitals should ensure that this information processes cautiously.

Cloud computing refers to on-demand, self-service Internet infrastructure that enables the user to access computing resources anytime from anywhere. It's a new model for providing computing resources, but not a new technology. Examples of frequently used non-health care an application comprises of Microsoft, Hotmail and Google Docs, while few effective known applications in health care include Microsoft HealthVault and Google Health (recently discontinued [6]). Although, in contrast with typical computing, this model provides three new advantages: large computing resources available on demand, withdrawal of an up-front devotion by users, and payment for use on a short-term basis as needed. Various articles, meetings, and blogs have described its applications in industry, business, transportation, education, and national security.

Health care, as with any other service action, requires continuous and systematic innovation in order to remain cost effective, efficient, and timely, and to provide satisfactory services. Several managers and professionals predict that cloud computing can enhance health care services, benefit health care research, and change the face of information technology (IT) [6].

The benefits of pay as use, automatic updating, and no need of establishing own infrastructure and efficient maintenance of databases makes cloud computing widely used in healthcare organizations. Instead of managing as well as maintaining of composite Health Information Technology (HIT) systems, it is shifting its burden by getting services from the Cloud service providers [1]. According to the [1] "it is expected that about 80% of the today's organizations will be moved on cloud till 2020". In spite of these important advantage organizations using cloud computing services are facing a lot of challenges and risks. The main problem is extensive security necessities by the healthcare cloud services providers. Privacy is also one of the major concerns of cloud computing in e-Health.

2. RELATED WORK
Every single data or information is of the chief responsibility for the organizations especially in healthcare as it needs to be accessible and secure from unauthorized access. The patient's data was stored on manual files and kept them in safes below physical locks in the near past. Data was secured by considering physical security. After the development in computer field, organizations moved from traditional manual systems to computer based data storage systems. These Computer based information system saved data on hard drives; tape drives and backup were very often taken for recovery of data in case of emergency. Data was secure and systematic as well as effective to manage and retrieve by using these automated healthcare information systems. This model shift forced health organizations to rely totally on computer based information systems [1].

Ming Li (2013), reports a new idea of patient centric structure and process for data access control to PHRs stored in semi-trusted servers. Attribute-Based Encryption (ABE) method was used to encrypt every patient's PHR file. It exploits

multi-authority ABE for the privacy of patient's by vital improvements of access policies. Revoking of access policy is not possible at all the instants and the attributes which were known to the user leads to privacy concern.

In Attribute-based encryption [2], the data owner has to first describe the attributes based on which the encryption needs to be performed. The number of users in the system doesn't matters. Each attribute has public key, secret key, and a random polynomial, so different users cannot merge their attributes to recover the data, and different users cannot takeaway collusion attacks. Only the user who holds the authorized attributes can meet the expectations of the access policy to decrypt the data.

Practically all key generation schemes used by authority are prevailing. Since these schemes contain the authority that just meets the need of private cloud environments, the authority should be removed in the future.

In Existing attribute-based encryption the main issues such as key management ,scalability, effective policy updates, and efficient on-demand cancellation are non-trivial to solve, and remain largely open up-to-date.

Current Market Dynamics: In contrast with other industries, the healthcare industry has significantly underutilized technology. To improve operational efficiency. Most healthcare systems still depend on paper medical records. Information that is digitized is generally not transferable, preventing information sharing between the different healthcare providers. The application of technology to ease the collaboration and to correlate the care between patients and physicians, and amongst the medical community is limited. Around the world, healthcare improvement has mandated that it is time for healthcare information technology (HIT) to be updated and cloud computing is at the center of this change. The healthcare industry is moving toward an information-centric care distribution model, empower in part by open standards that support cooperation, collaborative workflow and information sharing. Cloud computing provide an infrastructure that enable hospitals, medical practices, insurance companies, and research provision to get better computing resources at lower initial capital investments. Furthermore, cloud environments will lower the barriers for innovation and modernization of HIT systems and applications. Cloud computing provides the key technology requirements of the healthcare industry:

- Permits on-demand access to computing and large storage facilities which are not provided in traditional IT environments.
- Assists big data sets for electronic health records (EHR), radiology images and genomic data offloading, an inconvenient task, from hospital IT departments.
- Eases the sharing of EHRs among authorized physicians and hospitals in various geographic areas, providing more convenient access to life-saving information and decreasing the need for duplicate testing.
- Enhances the ability to analyze and track information (with the proper information Governance) so that data on treatments, costs, performance, and success studies. Can be analyzed and acted upon. Healthcare data has strict requirements for security, confidentiality, availability to authorized users, traceability of access, reversibility of data, and long-term maintenance. Hence, cloud vendors need to account for all these while adapting to government and industry regulations. Problems in making IT systems practical have delayed cloud computing growth in the health care industry. When taking into account a move to cloud computing, healthcare actors (medical practices, hospitals, research facilities, etc.) need to carefully review the type of application moving to the cloud (clinical and nonclinical applications). Clinical applications comprises of EHRs, physician order entry and software for imaging and pharmacy use. Nonclinical applications comprise of revenue cycle management, automatic patient billing, cost accounting, payroll management, and claims Management.

3. INFORMATION SECURITY IN HEALTHCARE

Information security is the preservation of information and information systems from unauthorized access, use, disclosure, interference, modification or destruction. Information security is achieved by ensuring the confidentiality, integrity, and accessibility of information. In health care, and for the purposes of this guide, confidentiality, integrity, and availability mean the following:

Confidentiality–the attribute that electronic health information is not made available or disclosed to unauthorized persons or processes.

Integrity – the attribute that electronic health information have not been altered or destroyed in an unauthorized manner.

Availability – the attribute that electronic health information is accessible and useable upon demand by an authorized person.

In advanced healthcare environments, there is a strong need for an infrastructure which reduces time consuming efforts and expensive operations to obtain a patient's complete medical record and uniformly integrates this heterogeneous collection of medical data to distribute it to the healthcare professionals. Electronic health records have been widely acquired to enable healthcare providers, insurance companies and patients to create, manage and access healthcare information at any situation. All the healthcare industries need to handle more requests with the available resources. The main objective of all the healthcare organization is to grow the number of people getting access to healthcare services [3]. Therefore day by day the amount of data that need to be stored, managed and updated is increasing exponentially. The healthcare industries desire more computation ability so that the quality of the service increases. Cloud computing enhances patient care by providing faster, better, secure and ubiquitous services at a lower cost and which meets the requirements of the healthcare sector. As a result, healthcare providers are more willing to shift their systems to clouds that can eliminate the geographical distance barriers among providers and patients [3]. With cloud computing, different doctors can access a patient's health records even if they're miles apart. These physicians need not have a direct communication to request for a transfer of health records. They can just access them through clouds.

4. GENERAL REQUIREMENTS FOR HEALTHCARE CLOUD SECURITY

General Requirements of cloud security depend on privacy, Trust, integrity, availability, confidentiality as shown in figure:

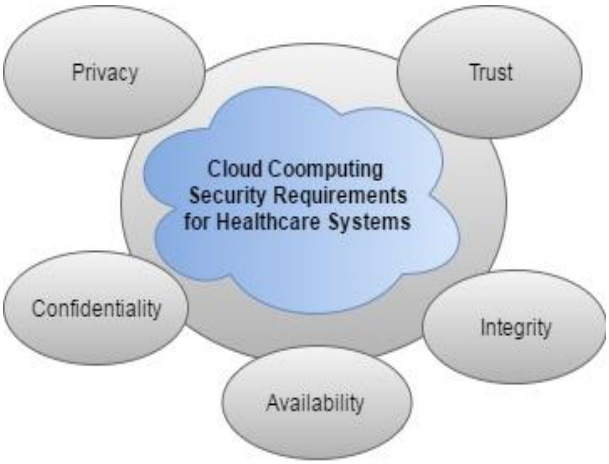

Fig 1: General Requirements of Cloud Security

4.1 Confidentiality

The idea of confidentiality denotes to those persons who are authorized to have access to system and protected medical data through permissions. The attribute of confidentiality ensures that not permitted users cannot have entry to the secured medical data of healthcare organizations stored in cloud infrastructure. The risk of compromise of medical data is at high level suitable to the participation of multiple parties, devices and applications drawn in for the manipulation of medical data due to an increase in number of access points to the medical data of patients stored on cloud infrastructure[4]. It plays an important part in maintaining and managing control over healthcare organizations medical data that is being stored across different remote cloud database locations. The property of confidentiality can be achieved by using the encryption techniques and algorithms, which include public key pairs, symmetric key, and length of the key and management of the key in the scenario of symmetric cipher. These encryption techniques will depend upon the service provider and also on the awareness and knowledge of the healthcare organization side so that they can encrypt their medical data before uploading it on the cloud. Confidentiality of medical data is related to authentication of user in cloud computing. User's account must be protected from attacker to attain confidentiality; authentication is the process, which brings assurance among users whilst they are presented to an information system for the authorization process. If mechanism lacks strong authentication procedure than it is viable to attack and user's account can be breached easily.

4.2 Integrity

Major feature of information security is integrity of data. It portrays that data or resources can be tailored or updated only by the official personnel's. Integrity is related with software, hardware device and data of healthcare organizations. The mechanisms that safeguard integrity accounts the modification that has taken place in data of healthcare organizations [4]. Users of cloud services should not only care about the confidentiality of data but also the integrity of data. Encryption ensure that confidentiality is maintained but it does not support with this concept that whether the medical data has been transformed or not, whilst it is present in the cloud infrastructure. So, it is the conscientiousness of cloud service provider to make sure that medical data integrity is maintained and is accurate. Atomicity, Consistency, Isolation, Durability (ACID), these features of cloud must be forced from corner to corner all the computing resources of cloud computing delivery models. This includes the protection of medical data on cloud infrastructure through both cryptography and through physical monitoring.

4.3 Availability

Availability denotes to that property which is being accessed and readily available to authorized personnel's only. The property of availability can be attacked and made unavailable to legitimate users on temporarily or permanent basis and in the same way loss can also be in terms of partial or complete. DoS attacks, natural disaster: earthquakes, floods, equipment outages these are all threats to availability. It is little hard to detect the possibilities regarding attacks on the accessibility of system or service. The threats that are directly affecting the accessibility can be either a network based assault such as DDoS [4]. There is a possibility that attack can also occur from the malicious insider while outsourcing the assets and healthcare organizations data to cloud service providers.

4.4 Privacy

It is that property which associates to the control of disclosure of personal information to unauthorized persons. Privacy is considered to be an important occupant of cloud computing infrastructure in both the terms such as compliance with the HIPPA standard and the trust of the healthcare organizations end. Privacy is a pivotal point in all challenges, which include the requirement to secure the information regarding identity, components of policy during the integration process and histories of performances. The healthcare organizations must be provided with an acceptable level of translucency in their operations and assurance of privacy by the cloud service providers.

4.5 Trust

Trust denotes that attribute which provides appropriate convincing to its observers that a system or process is working in its right state and is secure from threats. Healthcare system is dependent on cloud service provider for the availability and utilization of services in cloud computing environment [4]. In order to get services from provider the healthcare organization has to store its confidential and critical medical records on the cloud service supplier's side. Trust is applied through efficient and effective security policies, if cloud service providers want to build trust in their healthcare organizations they need to follow strict security policies that the medical data of user will not be provided to unauthorized parties and it should be protected from the malicious insiders.

5. BENEFITS OF CLOUD COMPUTING IN HEALTHCARE

There are immense benefits and advantages upon implementation of cloud computing in healthcare industry some of which may include**:**

5.1 Mobility of records

In many cases a person's health information can be needed by two or more health institutions in that case by implementation of cloud technology a person's health information can be easily synchronized and shared at the same time. Hence this improves physician's ability to provide a better health care to the patients [5].Thus by implementation of cloud technologies a patients information is readily available.

5.2 Speed:

By making use of cloud based technology and services always enable faster and accurate access to all the important information for the healthcare services providers and the history of their patients.

5.3 Security and Privacy

By utilizing cloud computing is mainly used for storage of medical records online. With the recent HIPAA update, cloud healthcare service providers are now responsible for HIPAA compliance as healthcare entities they serve. Thus this comprises of encryption of data and secure backup of this data which contains the health information of a person, then verifying if the data can be easily retrieved, and finally security can be improved by using permission based and secured database.

5.4 Reduction of costs

By acquiring these cloud techniques in healthcare- patients, physicians, other medical organizations experience cost reduction to a great extent. Since there is no need for these healthcare institutions and doctors to invest huge amounts in hardware infrastructure and their maintenance as these problems are already handled and taken care by the cloud computing providers [5]. According to a recent report by Healthcare Financial Management, says depending on the size and extend of the healthcare organizations the reduction is achieved by utilization of EHR's can amount up to $37 million over the next five year period.

6. CHALLENGES OF E-HEALTH CLOUD

No doubt, e-Health Cloud provides a lot of benefits in the industry of health care, but unfortunately it receive a number of problems in HIT as well as in cloud computing. Processing and storing of sensitive medical data of patients is a major challenge [4]. The following section describes the issues and challenges of e-Heath Cloud and their proposed solutions.

6.1 Data/Service Reliability

Cloud service providers need to provide excellent reliability of services over the cloud especially in healthcare industry [4]. Healthcare need data in the right form as well as cloud services. Illegitimate changes in data and errors in data are not adequate. So cloud must provide data and services without any error.

6.2 Data Management

E-health cloud needs to assign storage of millions of patient's data. Medical specialist accesses this sensitive data from different location at the same time [1]. There are different views of data like HD graphics, 3D and audio and video data. In order to manage this data systematically and provide it when desired, fault tolerant systems/services need to be assured.

6.3 Flexibility

According to the need of different healthcare providers, e-Health Cloud Service provider should be capable to serve accordingly [1]. The services provided by cloud should also be very flexible so that services can be configured according to user requirements. Additionally, adding new services as need should be accommodated.

6.4 Availability

The most important requirement for any healthcare providers is the consistent availability of the services from e-Health Cloud. Healthcare providers cannot continue their functions without availability of services and patient's sensitive data. This is why these services should be consistently available without any disturbances. The main reasons for failure of Cloud services may include network failure, software and hardware failure, or security attacks and natural disasters. E-Health Cloud should be proactive and ensure continuity of service in effective and efficient way. If backend up gradation is required then services for the healthcare should not be interrupted.

6.5 Security

Could Service providers store data, of patients from different healthcare organizations? There is need of strong access control and authorization mechanism to secure this huge and sensitive data. The security standards should be implemented so that sensitive data can only be accessible to right organization. E-healthcare service providers can only be shifted on cloud if they are guaranteed of their desired security [1]. So, policies and standard as organizations wants should be properly implemented by the cloud services provider.

6.6 Privacy

Many healthcare organizations are hesitant to shift to cloud computing services due to privacy concerns. For e-Healthcare systems, Privacy is one of the major alarms because of sensitivity of patient's data [1]. Due to sensitivity of patient records cloud is facing serious privacy issues. Recently United States of America (USA) Intelligence agencies recorded the sensitive information of German chancellor. Now organizations are worried about privacy issues.

7. PROPOSED SYSTEM

Cloud based health system solution is based on the concept of "Cloud Computing" a distributed computing system where a blend of virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered. This system provides an environment where patient's records are stored and it will be referenced by the doctors to improve the efficiency of the treatment. This handles the medical history of each individual of the country and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database. The details of the patients will be stored and an identification number will be generated when their data are stored into the database for the first time after the implementation of the system. Whenever they go for a treatment, their medical data will be stored into the database using their identification number. For security reasons, any person who wants to view their data will be allowed only to read the data. They will not be given access to update the database. For hospitals to update the database they require the license number along with the identification number of the person whose record has to be

stored.

Advantages of Proposed System:

- Achieving data confidentiality and identity privacy with high efficiency.
- Efficiently realizing access control of patient's personal health information.
- Resist various kinds of malicious attacks and far out performs previous schemes in terms of storage, computational and communication overhead.

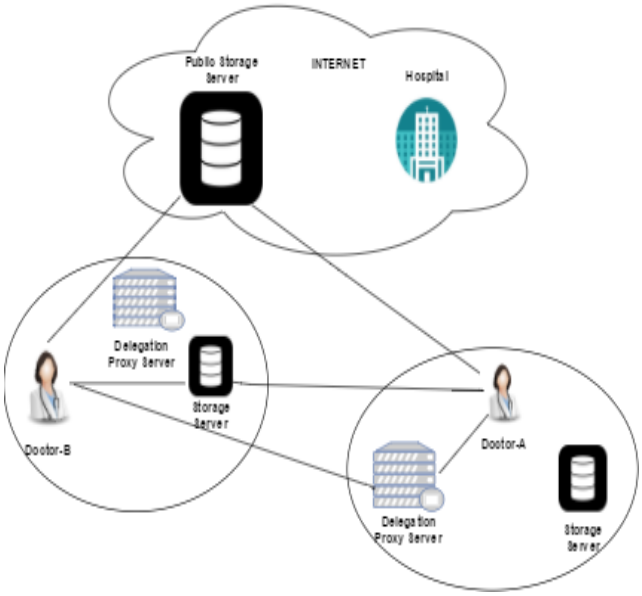

Fig 2. Proposed System diagram

8. CONCLUSION

The current shift of adopting cloud computing in the medical field can enhance and solve several collective Information concern in healthcare organizations as well as cost optimizations. Standardized cloud-based applications will bring obvious benefits to patients, physicians, insurance companies, pharmacies, imagining centers, etc. when sharing information across medical organizations providing better results. Challenges such as security concerns and interoperability will rise owing to the cloud-computing model. Therefore, the adoption of the cloud is progressing slowly. Through the implementation of best application in the design, deployment and use of it will hopefully generate a future growth of the cloud-based systems adoption, despite all of the obstacles.

9. REFERENCES

[1] Abdul Manan, I.A. (2014).”Opportunities and Threats of cloud computing in Healthcare”.*International Journal of Computer Applications,Volume10-No2*, 0975-887

[2] Aruna Devi. S, M. (Mar-2014). “Enhancing Security Feautures in Cloud Computing for Healthcare using Cipher and InterCloud”. *International Journal of Research in Engineering and Technology* , 200-203.

[3] G. Rathi, A. M. (2015). “Healthcare Data Security in Cloud Computing”. *International Journal of InnovativeResearch in Computer*, 1807-1815.

[4] Haider Ali Khan Khattak, H.A. (n.d). ”Security Concerns of Cloud Based Healthcare System”.

[5] G.Nikhita Reddy, G.R. (n.d).”Study of Cloud Computing in Healthcare Industry”.

[6] Alex Mu-Hsing Kuo, PhD. (2011)” Opportunities and Challenges of Cloud Computing to improve health care Services”. *Journal of Medical Internet Research*,