IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 12, December 2015.
www.ijiset.com
ISSN 2348 – 7968

Data Security in Health Cloud Infrastructure

Repu Daman[1], Manish M Tripathi[2]

[1] *School of Telemedicine & Biomedical Informatics(STBMI),*
Sanjay Gandhi Post Graduate Institute of Medical Sciences (SGPGIMS), Lucknow
repudaman@yahoo.com profile: www.repudaman.com

[2]*Dept. of Computer Science& Engineering, Kursi Road, Integral University, Lucknow*
Lucknow, UP, India
mmt@iu.ac.in

Abstract

The healthcare industry is looking to reap the benefits of emerging technologies such as mobile computing and cloud computing. It has a large volume of information like Patient Health Records (PHR) that needs to be collected, stored and retrieved again whenever needed. These PHR when equipped digitally become Electronic Health Records (EHRs). This large amount of data collected as EHRs has to be stored, processed and updated frequently and has to be available whenever and wherever necessary. Cloud provides the necessary infrastructure now-a-days at low cost with better quality. Migration towards Cloud computing thus lowers the cost of storing, processing and updating with improved quality in healthcare. Security of data in the cloud is of concern today for EHR which consists images of patients and history. The EHRs include the patient's scan images, x-rays etc. which are the patient's private data. Most of the patient data is personal in nature and is in multiple formats. In this paper Cloud Computing Infrastructure, Key Factors for Security in public cloud, Security Control, Cloud Safety & Assessment Model is discussed.

Keywords: *Telehealthcare, cloud computing infrastructure, security in healthcare*

1. Introduction

Cloud computing has been defined by US National Institute of Standards and Technology (NIST) as a model for enabling convenient on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Cloud Computing is a model where in on-demand access to the resources are provided to the users as they plug into the cloud provided that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user application. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

The essential characteristics of cloud computing are:

- **On-demand self-service:** A consumer can provision computing capabilities, such as server time and network storage, as needed.
- **Broad network access:** Broad range of network accessibilities by various client platforms.
- **Resource pooling:** The provider's computing capabilities are pooled to serve multiple consumers using a multi-tenant model. Resources are dynamically assigned and reassigned according to consumer demand.
- **Rapid elasticity:** Capabilities can be rapid, elastically provisioned, and in some cases automatic; the consumer capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

The healthcare industry is under constant pressure to streamline the sharing and availability of information, while at the same time maintaining ever-more rigorous controls over patient privacy and of course, reducing costs at the same time. Cloud computing thus offers significant opportunities, perhaps even more significant than in many other industries. The ability to quickly access computing and storage resources when needed without the requirement for a large technical staff is the perfect solution for many hospitals, health clinics and doctor's offices. It should provide them with an incredible opportunity to improve services to their customers, the patients, to share information more easily than ever before and improve operational efficiency at the same time. The challenge at least for now is the critical element of maintaining patient privacy. The risks of exposing sensitive patient data, especially in public cloud infrastructures, continue to act as a drag on the rate of cloud adoption.

2. Cloud Transformation Models

Cloud computing deployment models are classified into four types

ISSN 2348 – 7968

A. *Public Cloud*

The public cloud offer applications, storage and other services to the general public by a service provider based on "pay-as-you-go" model. A public cloud is constructed with a view to offer unlimited storage space and increased bandwidth via Internet to all businesses. Public clouds are owned, hosted and operated by third party service providers to cater all kind of requirements from small, medium and big businesses. Public clouds include Amazon Elastic Cloud Computer, Google App Engine, Blue Cloud by IBM and Azure Services platform by Windows.

B. *Community Cloud*

The cloud infrastructure is shared between the organizations with similar interests and requirements whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud but more than a private cloud, so only some of the cost savings potential of cloud computing are realized. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. For example, all the government agencies or member of a similar group or community can share the same cloud.

C. *Hybrid Cloud*

Hybrid clouds combine the advantages of private and public clouds, offer flexibility, control and security of multiple deployment models. IT organizations use hybrid clouds to employ cloud bursting for scaling across clouds. Hybrid cloud has a feature of optimal utilization, Data-Centre consolidation, Risk transfer and availability.

D. *Private Cloud*

Private cloud is a cloud infrastructure build exclusively for a one organization, deployed within certain boundaries like firewall settings whether managed internally or by a third party and hosted internally or externally. Users are charged on the basis of per Gigabyte (Gb) usage along with bandwidth transfer fees. Data stored in the private cloud can only be shared amongst users of an organization and third party sharing depends upon trust they build with them. Popular examples of private cloud include Amazon Virtual Private Cloud (Amazon VPC), Eucalyptus Cloud Platform, IBM SmartCloud Foundation and Microsoft Private. Private cloud is further classified as on-premises and externally hosted private cloud. Private cloud has enhanced security measures, dedicated resources and customization feature. Private cloud is considered a better option than other cloud deployment models as data security risk of private cloud is less as compared to public cloud. Technology of the private cloud is older than the public cloud i.e less elastic in nature.

3. Cloud Service Models

Cloud service models can be offered as Software as a Service (SaaS), Platform as a Service (PaaS) & Infrastructure as a Service (IaaS)

A. *Software as a Service (SaaS)*

Software as a Service (SaaS) is the form of providing the cloud service consumer with the capability to use the cloud service provider's application software running on a cloud infrastructure. These applications are configured to suite the consumers preferences and are accessible from various client devices through the Internet (e.g., web-based email, electronic health records).

B. *Platform as a Service (PaaS)*

Platform as a Service (PaaS) is another service model that is found in the cloud where the service consumer is provided with the capability to deploy onto the cloud infrastructure applications created using programming and support tools by the service provider (e.g., centralised analysis of MRI scans or X-rays built for example on Microsoft Azure).

C. *Infrastructure as a Service (IaaS)*

Infrastructure as a Service (IaaS) refers to the capability provided to the service consumer to provision processing, storage, networks and other fundamental computing resources, as well as being able to deploy and run arbitrary software. These can include operating systems and applications (e.g., networks for transmission of diagnostic tests or the inputs from personal monitoring devices).

Traditional IT Infrastructure is just like car. One can manage all the infrastructure resources like Applications, Data, Runtime, Middleware, Operating System, Virtualization, Data Center, Server, Storage and Networking. Infrastructure as a service (IaaS) is like a rental car. User can only manage Applications, Data, Runtime, Middleware, Operating System part. Rest is managed by the cloud vendor. (SaaS) is like in public transit. Nothing is managed by the user all are controlled and managed by cloud vendor. Platform as a Service (PaaS) is like a taxi where only Application and Data part can be managed by the user and is managed by the Cloud Vendor.

4. Cloud computing in Healthcare Environment

Management of Data, Data Access & Retrieval and Sharing of data are three of important component for cloud computing in Healthcare Environment. Healthcare

ISSN 2348 – 7968

environment uses a cloud collaboration platform to manage electronic health records (EHRs) and electronic medical records (EMRs). Cloud platform takes advantage of advanced information and communication technology (ICT) to provide seamless service that includes mobile availability and integrated video. Cloud infrastructure thus focuses on state-wide or countrywide telemedicine and public healthcare management. The telemedicine solution promotes collaboration between hospitals, improving resource utilization and medical services and promotes collaboration between medical and health organizations, improving rural and urban healthcare services and management capabilities. It promotes collaboration between doctors and the public and ensuring equal, convenient, and efficient health service for everyone. Overall it features convenience, high-quality service experience, high performance, high stability, cost-effectiveness and high security.

5. Healthcare data requirement

Healthcare data has stringent requirements in terms of Security, Confidentiality and Availability to authorized users, Traceability of access, Reversibility of data and Long-term preservation. Cloud vendors need to account for all these while conforming to government and industry regulations. Interoperable have delayed cloud computing growth in the Health care industry.

A. Identification of Actors & Applications

Healthcare Actors plays important role in deploying cloud infrastructure in healthcare environment. Healthcare actors include Medical Doctors & Paramedical Staff Members, Medical Practices, Hospital and Research Facilities. There is a need to consider carefully type of application moving to cloud. Applications used in a hospital are clinical and nonclinical in nature. Clinical Applications includes EHR, Physician Order Entry, Software for Imaging and Pharmacy whereas Non Clinical Applications include Revenue Cycle Management, Automatic Patient Billing, Cost Billing, Payroll Management, Hospital Security & Surveillance etc. Healthcare actors must also consider the cloud service model (IaaS, PaaS, or SaaS) that best addresses their business requirements. SaaS, with its pay-per-use business model is the most attractive economic option, especially for Small physician practices, since the need for full-time IT personnel is eliminated along with capital expenses associated with system hardware, operating systems and software. PaaS is a viable option for larger healthcare institutions that have the resources to develop their own cloud based solutions. For healthcare institutions seeking a more scalable infrastructure, IaaS offers a cost-effective turn-key solution that provides scalability with security, flexibility, defined service level agreements, built-in backup and data protection.

B. Security Challenges

- Data maintained in a cloud may contain personal, private or confidential information such as healthcare related information that requires the proper safeguards to prevent disclosure, compromise or misuse.
- Data jurisdiction, Security, Privacy and compliance are impacting adoption by healthcare organizations

C. Cloud-based Privacy and IT Security Solutions

The cloud computing industry is beginning to offer critical IT security services and infrastructures. These services are intended to improve the robustness of traditional enterprise IT security solutions or supplement the level of IT security with other cloud services. Privacy and IT security features can be offered as SaaS, PaaS or IaaS.

D. IT Security Platform as a Service (PaaS) Opportunities

Web Services Security (WS-Security) is a proposed IT industry standard that addresses security when data is exchanged as part of a web service. WS-Security is one of a series of specifications from an industry group that includes IBM, Microsoft and Verisign. Related specifications include the Business Process Execution Language (BPEL), WS-Coordination and WS-Transaction. The protocol specifies how integrity, privacy and confidentiality can be enforced on messages and allows the communication of various security token formats, such as Secure Access Markup Language (SAML), Kerberos and X.509 Digital Certificates. Its main focus is the use of XML Signature and XML Encryption to provide end-to-end security. The WS-Security protocol provides a model for many levels of security needed for web services. WS-Security specifies enhancements to Simple Object Access Protocol (SOAP) messaging aimed at protecting the integrity and confidentiality of a message and authenticating the sender. WS-Security also specifies how to associate a security token with a message, without specifying what kind of token is to be used. It does describe how to encode X.509 certificates and Kerberos tickets. WS-Security is intended to be extensible so that new security mechanisms can be used in the future. These security tokens allow for single sign-on capability that allows for the verification of end user credentials across multiple applications in addition to interoperable authorization permissions. WS-Security requires the implementation of various hardware and software components as a platform for development of web services and sites.

ISSN 2348 – 7968

E. IT Security Infrastructure as a Service (IaaS) Opportunities

IaaS has the security features of a series of firewalls, anti-virus functionality or virtual private network (VPN) access for a community cloud network. This offers the potential of reducing software acquisition and management costs for integrating HIS or EMR applications to a regional e-health hub. The cloud-based privacy and security services is primarily for greenfield deployments which requires increased and uniform levels of privacy protection and IT security at reduced deployment costs.

F. IT Privacy and Security Software as a Service (SaaS) Opportunities

One of the principal privacy challenges in health care is the management and enforcement of patient information wishes, commonly known as informational consent. Many EMR and HIS solutions do not offer this capability and would require potentially costly retrofits to support this legislative requirement. By offering this software capability as a service in a community or private cloud, EMRs and HIS solutions operating in a cloud context could leverage this feature at reduced costs and implementation timeframes. This would also have the benefit of ensuring a uniform implementation, interoperability

G. Medical ethics and the cloud

Cloud computing is evolving faster than regulation and is an increasing need to apply some ethical values in its service offerings, most especially in the health sector in order to protect patient's safety and privacy. Sensitive health-related data in most cases hold the key to life and death where such data are compromised, they may cause irreparable loses to the data subjects such as employment and insurance opportunities. The pertinent question to ask in this respect is whether ethics should be a considerable factor before deploying e-health application in the cloud.

- How will it be guaranteed for example, that the cloud service provide will keep medical records for a period of time required by law if goes bankrupt?
- Will it be easy to transfer these data to a different provider in view of the lack of interoperability that exits in the services?

6. Literature Review

Several major public cloud computing environments exist, such as Microsoft Azure, Rackspace, Amazon's EC2 service and Verizon. These providers allow customers to run an operating system of their choice and maintain full control of their operating system and network environment. Providers can be classified as infrastructure as a service (Iaas), Platform as a service (Paas). System administrators do not have direct control over the operating system or network. Maintaining Security and Privacy requires Authorised Access, Confidentiality, Patient's Consent, Relevance, Information Ownership, Information Consistency and Audits & Archiving

A. Network Issues

- DDoS Attacks – Distributed Denial of Service mitigating techniques as included in Amazon Web Services (AWS) platform to avoid this kind of attack.
- MITM Attacks – Man in the Middle attacks are avoided because all the endpoints of AWS are secured by Secure Socket Layer (SSL), which provides server authentication.
- IP Spoofing – Traffic Platform is controlled by Firewall Infrastructure. Stored data cannot send spoofed network data.
- Port Scanning – Unauthorized port scans by customers are violation of the provider's user policy.

B. Amazon Virtual Private Cloud from Security Perspective

- Private subnets in Amazon's Environment with nonroutable Internet protocol (IP) addresses
- Option to assign public IP addresses to servers
- Ability to assign public IP addresses to servers
- Ability to create a virtual private network (VPN) connection to Amazon to incorporate servers into the wide area network of an organisation
- Combination of public IP addresses and VPN to create multitiered services
- Inbound and outbound stateful packet inspection firewalls rules for each server group
- Ability to setup a host-based firewall (if supported in the operating system)
- Network access control lists (ACL) to control incoming and outgoing traffic at the subnet level
- Multiple network interfaces for each server to build sophisticated network architectures

7. Key Factors, Security Control, Cloud Safety & Assessment Model

A. Keys factors to be considered before moving to Cloud infrastructure

Key factors considered before moving to cloud are

- **Consider a cloud risk assessment**. Health Insurance and Portability & Accountability Act

ISSN 2348 – 7968

(HIPPA) should be familiar with the need to conduct a risk assessment and special care should be taken to understand a risk assessment

- **Consider using a "private" or "hybrid" cloud solution.** Many organizations decide to take a phased approach when moving to the cloud rather than move all their data to a public cloud provider. Opt for private clouds or hybrid clouds. Private clouds which aren't shared with other customers or hybrid clouds that allow them to keep some data under their control while leveraging a cloud provider for less sensitive functions.
- **Understand exactly what are not getting.** Considerable variation exists among cloud providers in terms of the security functions they perform and those that remain the customer's responsibility. Unless your provider states otherwise, assume that any particular requirement, such as encryption or data backup, remains your responsibility.
- **Ensure cloud vendor complies with HIPAA and other regulations.** Cloud vendor must complies with HIPPA and other regulations and be particularly wary of cloud providers who insist they are not business associates under the new rules.
- **Know where your data is today – and where it will be tomorrow**. Consider not only where cloud provider is hosting data but also what happens to it when service expires including how to meet HIPAA/HITECH data-retention and data-destruction requirements.
- **Consider cloud security "donut hole."** Cloud providers only attest to the security of its physical infrastructure excluding the shared virtualization systems that support the cloud service. This can leave the so-called "donut hole" between the host's coverage and the point where the healthcare organization handles its security and seek a host who closes this gap.
- **Determine what the cloud provider will and won't sign.** Considering HIPAA compliance, will the vendor attest to what protections the healthcare provider has in place and its responsibilities? If not, can it provide a third-party audit report attesting the healthcare provider possesses such security protections? In medical services and healthcare, cloud computing needs to maintain compliance with some acts for data security and privacy protection like Health Insurance Portability and Accountability Act of 1996 (HIPPA), HITECH & GLBA.

B. Key Security Control for Healthcare Cloud Infrastructure

Key Security Control that Healthcare Cloud Infrastructure should have

- **Role-based access**- Many different types of employees needs access to the EHR system for different reasons. In order to keep data safe, providers should make sure they can configure a system so that people only have access to information they need for their jobs. Biometric methods for example, fingerprint recognition and palm vein scanning can enhance authentication and information security.
- **Data encryption** - Information should be encrypted not just while it's stored on the cloud provider's servers, but also as it's being transmitted to avoid interception.
- **Digital signature** - This is one method providers can use to verify that the electronic records are authentic when they're transmitted back and forth between the hospital and the EHR vendor. A digital signature can be used to verify that the sender is legitimate and that the information wasn't tampered with while it was in transit.
- **Hiring and training** - Lot of security threats come from inside an organization, it's important that a cloud provider conducts thorough background checks for all employees with access to systems and provides security training to avoid breaches due to employee negligence.
- **System monitoring** - Technical controls keep unauthorized people from accessing electronic records, they aren't perfect. That's why it's important that a cloud-based EHR is monitored in order to create a log of all the people who have accessed the system.

To keep the system secure and avoid getting stuck in case of a security incident following points needs to be considered:

- Audits and testing — In addition to the initial audit before signing on for a service, hospitals should be able to conduct regular audits and security tests.
- Notification of changes — Cloud customers should be notified of any time software will be changed or upgraded, with an explanation of what that means for security and service availability.
- Mandatory security precautions — Since software may change often, organizations may want the contract to specify which security controls must always be in place.

ISSN 2348 – 7968

- Compensation - Cloud providers should have an incentive to protect data. That means the contract should include significant penalties if the vendor's actions result in a security incident.

C. *Healthcare Cloud Solution Security Parameters & Cloud Safety*

Cloud Solution should include

- Embedded encryption that secures data backup and archive data in-flight or stored within the cloud;
- Integrated alerting, reporting and data verification functionality to help ensure that data has safely reached the cloud without the risk associated with manual scripting or standalone gateway appliances;
- Native REST/HTTP integration to deliver seamless data and information management across on-site and cloud-based storage architectures; and
- Integrated features such as de-duplication and compression to enable efficient movement of backup and archive data across a network for long-term cloud storage.

Healthcare is warming up to cloud services, and that means extra vigilance. Minimum step taken to keep data safe are as mentioned below.

- **Control over cloud services:** Hospitals are using various types of cloud services by downloading cloud-based apps for file sharing, storage, collaboration, and other functions. Organization can standardize these apps, educate employees about their availability. By doing these available services that are in demand, necessary controls can be placed to comply with your regulatory, security, and compliance needs.
- **Service Level Agreement:** Ensure an attorney scrutinizes cloud services contract and service level agreement (SLA) so it meets organization's requirements and includes penalties in the case of failure. Because many states now have their own data security, breach, and personal health information protection laws in place, determine where your data will be housed and how this location could affect your organization's legal responsibilities.
- **Strengthening the Network:** Without a strong, reliable network, a healthcare organization's cloud initiative is on rocky ground and employees will soon figure out workarounds such as unsecured public Wifi. As more healthcare providers add cloud services, telehealth, video, connected devices, and other network-hungry technologies to their networks, it's crucial that infrastructures support these additions. Atlantic Health System, for example, upgraded its network when the organization added virtual desktop infrastructure, secure text messaging and Roaming communication technology for nurses.
- **Inventory PHI:** Protected health information (PHI) has to be carefully safeguarded. Organizations must, therefore, consider who has access to this data, both internally and at cloud service providers; whether it's centrally stored or scattered throughout an organization; and how it's protecting the data. A cloud company that specializes in technology, networks, servers and security solutions could well provide a much more secure environment than a two-person practice. Healthcare organizations might need to ensure their cloud partners are HIPAA certified, depending on usage or data stored or accessed. A large payer or health system could, on the other hand, prefer to use its larger, more sophisticated internal IT resources to defend PHI and related equipment.

D. *Assessment model*

- The risk assessment is based upon the model of ENISA (2009). They also made an assessment about cloud computing security. Some risks overlap with the ENISA research and show to have the same score. Because of the different risks identified the results show to be different. However, the identified risks that are somewhat the same as identified by ENISA show similar results. In this assessment we use different scales and I made the assessment based upon the found literature. The risks are anchored. They are compared with each other and thus assessed by me.

First we will list the most important risks that we want to assess. These gathered risks are partly a result found with this research. The risks are as in table 1:

Risk1: Changing Policies Risk2: Privacy laws Risk3: Poor security by cloud provider Risk4: Different countries different laws Risk5: Grey areas with new technology Risk6: XML signature attacks	Risk7: Cloud access tools failures Risk8:Flooding attacks Risk9:Denial of service Risk10:Lock in effect Risk11:Third party access to your data Risk12:Bad IP references Risk13:Cloud bankrupt Risk14:Downtime

Table1: Important risks in Cloud computing

ISSN 2348 – 7968

Chance of risk actually occurring is scaled from 1 to 7 also 1 being the lowest. The higher the value, the higher the risk is. In words we can describe the numeric values as 1. Very low, 2. Low, 3. Low/medium, 4. Medium, 5. Medium/high, 6. High & 7 as Very High

8. Conclusion

- SaaS based electronic medical record (EMR) solutions are a natural fit for small physician practices to which most physicians belong because of their affordability, ease of use, and small requirement for ongoing technical support.
- Cloud computing-based health applications such as Microsoft HealthVault and Google Health can help create a new market of consumer-oriented healthcare applications, enabling better consumer lifestyle choices and more active consumer participation in choosing a course of treatment for serious health problems.
- Private and or e-health community-based clouds have the potential to offer data custodians and information managers more control over governance, security mechanisms and infrastructures, thereby potentially reducing risk.
- Private or dedicated health care community cloud offerings can provide the opportunity for collaboration in determining the appropriate levels of data safeguards and processes necessary to manage risk. Public cloud offerings typically provide less control over choice and operations of IT security and privacy mechanisms
- Concerns about privacy are not a valid reason to avoid cloud computing:
  - ✓ Each of the deployment models (private, community, public or hybrid) can be leveraged as appropriate to the privacy needs of the application and the community.
  - ✓ Regardless of the deployment model, there must be mature, transparent and well managed mechanisms to ensure secure implementations that appropriately meet the privacy and disclosure requirements of each jurisdiction in the country

References

[1] Repu Daman and Manish M Tripathi; Encryption Tools for Secured Health Data in Public Cloud; International Journal of Innovative Science, Engineering & Technology;Vol II Issue 11,2015, pp-843-848
[2] How to maintain security in cloud Hamami, Oren Health Management Technology; Jun 2013; 34, 6; ProQuest
[3] Making the cloud work for healthcare Webb, Geoff Health Management Technology; Feb 2012; 33, 2; ProQuest
[4] Biomedical Cloud Computing With Amazon Web Services Vincent A. Fusaro1*, Prasad Patil, Erik Gafni, Dennis P. Wall, Peter J. Tonellato; August 2011, Volume 7, Issue 8; PLOS Computational Biology
[5] Storing and using Health Data in Virtual Private Cloud; Journal of Medical Internet Research;
[6] Opportunities and Challenges of Cloud Computing to Improve Health Care Services; Alex Mu-Hsing Kuo; J Med Internet Res. 2011 Jul-Sep; 13(3): e67. J Med Internet Res. 2011 Jul-Sep; 13(3): e67.
[7] Medical Applications and Healthcare Based on Cloud Computing; Lidong Wang, Cheryl Ann Alexander; Vol.2, No.4, August 2014, pp. 217~225 International Journal of Cloud Computing and Services Science (IJ-CLOSER)
[8] How to maintain security in the cloud, Hamami, Oren, Health Management Technology; Jun 2013; 34, 6; ProQuest

Repu Daman is currently working as Telemedicine Network Manager at National Resource Center (NRC), School of Telemedicine & Biomedical Informatics (STBMI), Sanjay Gandhi Post Graduate Institute of Medical Sciences (SGPGIMS), Lucknow. India. He was associated with various telemedicine projects and networks funded by Central Govt, State Govt. in India & International projects at North Korea and Maldive under World Health Organisation (WHO) and IHDP-World Bank.

Manish Madho Tripathi is currently working as an Associate Professor at Dept of Computer Sciences & Engineering, Integral Univesity, Kursi Road, Lucknow