ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

Data Security Threats in Healthcare It Using Cloud

Prudhvi Madadi

PhD Student, Dept. of Human Capital Mgmt., Bellevue University, Omaha, NE, USA

ABSTRACT: In order to share the results of diagnostics and seek solutions to various health related issues healthcare providers are highly dependent on cloud services. Such data pertaining to healthcare is highly sensitive in nature and it should not be accessible by unauthorized individuals. Several studies in the recent past have highlighted the data security threats faced by healthcare information systems (HIS). The objective of this study is to analyze the security concerns in the context of HIS. This study also showcases the security challenges in healthcare cloud computing and highlighting related issues such as access control, identity management, authentication and authorization.

KEYWORDS: Data Security, Healthcare, Cloud Computing, Information Systems, Threats

I. INTRODUCTION

The term cloud computing can be described as a set of IT services which are provided to clients through a network. They are provided on a lease basis and can be balanced based on the service requirements of the client [1]. In the healthcare segment, cloud computing is viewed as a system which can be utilized as a platform to facilitate the sharing of applications, infrastructure and critical medical information [2]. The fundamental principle underlying the adoption and growth of cloud computing in healthcare is the sharing of the risk with the customer, which is the exact opposite of customer managed risk [3]. In addition to risk sharing a few other reasons for adoption of cloud computing by healthcare organizations include, security in communications, confidentiality of information related to healthcare, non-availability of any other alternative and its capability to counter frequent data breaches [4]. Likewise, developments in HIS produce impressive amounts of data to be managed.

Over the past couple of decades, technological innovations have immensely increased the popularity of cloud computing across industries. The cloud service has steadily engaged enrolled clients to get an access to the hardware and programming through a third segment over remote areas [5]. It has paved the way for a paradigmatic move in the manner the data is accessed and stored. As opposed to customary technology, cloud computing has numerous particular qualities, as the scope of advantages that belong to the cloud contributors are totally scattered, differing and altogether virtualized. Since, cloud computing represents a relatively novel computing representation at each dimension, similar to applications, network, hosts, and data, it resultantly raises the issue of the application safety to shift towards cloud computing [6]. In contrast with various other industries, healthcare services have been a bit moderate with regards to changing from customary techniques to cloud computing. However, the adoption of cloud computing in healthcare is largely hindered by the security concerns. Thinking about the requirement for integrating data and sharing the same among healthcare practitioners and associations, hospitals ought to have the option to make standard rules and recognize security challenges for improving security of data in cloud computing [7]

II. AIM OF THE STUDY

The study was conducted with the aim of exploring challenges in healthcare cloud computing, focusing primarily on security concerns.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

III. THE MAJOR SECURITY ISSUES IN CLOUD IN HEALTHCARE SERVICES

A. Privacy of Data

Data privacy is one of the major concerns for organizations, when it comes to the utilization of cloud computing services [8]. Data privacy is primarily violated by breach of data, which can be explained as the purposeful or accidental leak of secure or private data to an untrusted environment [9]. In the healthcare sector, data breach takes place when electronic health records, protected health information, business strategies, research data, financial data are leaked. Beyond monetary losses, healthcare data breaches can harm an organization's reputation and lead to litigation. With the expanding adoption of cloud and web services by therapeutic experts, analysts, and administrators, the healthcare organization has to adapt various measures to control and eliminate data breach [10]. In the year 2013, a similar case of data breach was reported by Genomic Health Inc. (provider of genomic based diagnostics cancer teats). The organization has a flagship line of gene expressions test for breast, prostate and colon cancer have been utilized to facilitate the treatment decisions of over 600,000 cancer patients globally. Knowing the sheer volume of data being processed Genome made using the cloud an inevitable choice. Like many organizations Genomics decision to move to cloud was faced with the issue of data privacy and they were continuously faced with challenge of keeping PHI on premises and further protect it in the cloud. Further protecting sensitive data across all applications coupled with monitoring usage and enforcing usage across unsanctioned applications was also a major hurdle. However they found a solution for these issues by adopting an active customized platform.

B. Cost of Ownership

It is quite difficult for any organization to adapt to the increased cost of ownership while introducing newer forms of technology, into their operation dynamics. Considered to be one of the significant risks, unexpected cost of ownership is also one of the most common occurrences for a healthcare organization when moving to the cloud [11]. The reason this happens is that healthcare set-ups will in general take a look at the cloud as far as just process and storage [12]. The IT staff involved in healthcare services often tries to match the expense of purchasing new tools and its installation to the expense of self-provisioning these equivalent assets in a different cloud condition [13]. This selective approach makes the healthcare organization dismiss the security, planning, compatibility and movement related to manual methods and costs involved [14].In the year 2014, the case of WebRTC (a browser-based technology) can be discussed in the context of the same. Enterprise organizations with restricted environments looking to adopt it will unavoidably experience issues pertaining to browser, plugin and network related aspects. What's more, the legacy devices and systems that have been utilized in the past to store content (e.g. patient health records and images) are found to be incompatible with WebRTC. To ensure the compatibility of WebRTC with traditional video conferencing solutions the healthcare concern would require software, hardware and patented protocols, which lead to increased expenditures.

C. Network Reliability

In a healthcare setup connected medical devices not only include smartphones but also the tablets clinicians' access to EHRs and administrative tools [15]. As the quantity of connected therapeutic tools keeps on increasing, the reliability of the network will dependably be the shared factor that supports activities related to digital communication practices [16]. In case of healthcare associations proceeding to increase associated medicinal tools and other IT devices to their computerized settings, network reliability is fundamental so as to enable suppliers to communicate with data all the more rapidly [17]. Building a reliable network is quite essential in order to match with the consistent and critical connections. Without proper considerations organizations often risk unreliable systems that have noteworthy negative downstream effects [18]. In the case of Marin General Hospital, in the year 2015 system administrators found that an assessment of the network assessment and site survey highlighted issues that were not quite evident. The majority of the remote site reviews included radio frequency. It was extremely troublesome get cent percent coverage: however a strong site overview, appropriate channel setup, and strong design were pivotal. The administrators at Marin investigated the creation of key tie-ups with their wireless vendors and ensured the involvement of the vendors engineering team that had a huge impact on the success and reliability of the network.

D. Cloud Storage Reliability

Cloud data storage is regularly set in a virtual environment and a virtual server is shared with customers and other providers of cloud services. Data is backed up to a cloud, through cloud storage gateways which connect with backup software using standard network protocols [19]. Directionally, the reliability of cloud storage is a key viewpoint to be considered while embracing cloud computing, particularly for the purposes of data warehousing and transfer [20]. So as to ensure security and protection cloud storage utilizes the present standard encryption models. Healthcare organizations do not need to stress on information being abused, even in a shared storage condition [21]. As opposed to the conventional tape backup, cloud storage is effectively scaled to oblige the clients' storage needs [22]. With regards to the same, the real-time circumstance of Netflix is very significant. In the year 2012 they encountered an eighteen hour blackout influencing most of its clients. It came about because of the failure of an Elastic Load Balancer (ELB) service in the US-East-1 cloud territory, where Netflix had the majority of its cloud storage processes. Taking key inputs from this blackout, Netflix moved to a more dynamic cross territorial design, where traffic load of the client is stored crosswise over three cloud regions. If there should be an occurrence of a blackout, traffic from the affected area can be diverted to the ones which are functional.

E. Service Levels

There has been a widespread adoption of cloud service solutions by healthcare set-ups over the years. However, service compliance and service level agreements have been under careful consideration [23]. In the healthcare sector the movement towards the creation of shared services has been quite affirmative. In the context of the same a healthcare parent organization primarily comprises of two entities: i) a provider of conventional healthcare services and ii) a cloud services provider catering to the needs of multiple healthcare organizations [24]. The CSCC guidelines in terms of the "Practical Guide to Cloud Service Agreements" [25] and "Public Cloud Service Agreements" [26] have provided the participating organizations a set of guidelines for service level operations. A similar case was reported by X Inc. USA (a developer of online games), in the year 2012. X Inc. wanted to use a cloud computing service to facilitate the core gaming process of their latest online game. They decided to adopt a cloud computing platform that supported automatic scaling and wanted a set of guarantees on the response time in order to retain the interested gamers. Subsequently, they were faced with the risk of non-adherence to the response time and were lost some of their gamers. They further decided to heavily penalize the cloud provider for such a violation.

F. Impact on healthcare industry and its services

There are numerous rigorous requirements of cloud computing for the healthcare sector taking into consideration the aspects of security, confidentiality, availability, traceability, reversibility, and long-term preservation of data [27]. While adhering to industry and government regulations, the providers of cloud facilities need to account for all the above mentioned aspects. Apart from the above mentioned aspects, the aspect of healthcare ethics also needs to be taken into account. [28]. A number of healthcare centers conduct clinical research which involves the analysis of huge amount of patient and healthcare data. Data breach occurring for such sensitive information is a clear violation of medical ethics. This can lead to a hampered brand image and drastic decrease in patient numbers. The stakeholders in the healthcare system need to carefully consider the ethics in healthcare when deciding to make a move towards cloud computing which encompass applications both clinical and nonclinical in nature. The clinical applications encompass EHRs, physician order entry and software for pharmacy and imagery needs [29]. Application nonclinical in nature include the aspects of, revenue cycle management, automatic patient billing, cost accounting, payroll administration, and management of claims [30].

IV. CONCLUSION

Over the years the adoption of cloud computing in the healthcare sector is expected to evolve and grow substantially. The heightened need for cloud computing is both from the technology and business angle. The ever increasing use of HIS and related devices, the need to analyze and store huge amounts of information related to healthcare to cater to both the population and personal health management has been primarily responsible for this increased demand for cloud computing. In addition to this are the ever more sophisticated and a plethora of healthcare cloud service offerings which are being extensively made available in the market. Providers of healthcare might face a lot of struggle in their attempt to reproduce the same as in-house applications. The application of technologies like: big data analytics, cognitive computing, mobile collaboration and information exchange is largely facilitated by cloud computing. This in turn is crucial in order to accelerate the delivery of advanced healthcare solutions. Hybrid cloud arrangements will be prevalent in order to support the requirements of the ever expanding healthcare market. This model provides the healthcare industry the flexibility to deploy workloads and data based on the analysis of business related risk or reward. The key factors determining the decisions of hybrid cloud deployment will be the security and privacy requirements and regulation compliance.

REFERENCES

[1] Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011) ‘Cloud Computing Security Issues and Challenges’, *International Journal of Computer Networks*, vol. 3, no. 5, pp. 247-255.

[2] Khana, F. A., Alia, A., Abbas, H., & Haldar, N. H. (2014) ‘A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks’, *Procedia Computer Science*, vol.34,no.1, pp. 511-517.

[3] Mehraeen, E., Ayatollahi, H., Ahmadi, M. (2016) ‘Health Information Security in Hospitals: the Application of Security Safeguards’, *ACTA INFORM MED*, vol. 24, no.1, pp. 47-50.

[4] Griebel, L., et al. (2015). A scoping review of cloud computing in healthcare. *BMC Medical Informatics and Decision Making, vol. 15, no.*7, 24-37.

[5] Chaudhry, U. Qidwai, M. H. Miraz, A. Ibrahim, and C. Valli, ‘‘Datasecurity among ISO/IEEE 11073 compliant healthcare devices throughstatistical fingerprinting,’’ presented at the 9th IEEE-GCC Conf. Exhib.(GCCCE), Manama, Bahrain, May 2017.

[6] G. Rosado, R. Gómez, D. Mellado, and E. Fernández-Medina,(2012) ‘Security analysis in the migration to cloud environments,’ *Future Internet*, vol. 4, no. 2, pp. 469–487.

[7] Chen, T. S., Liu, C. H., Chen, T. L., Chen, C. S., Bau, J. G., & Lin, T. C. (2012) ‘Secure Dynamic access control scheme of PHR in cloud computing’, *Journal of medical systems*, vol.36, no.6, pp. 4005-4020

[8] Habiba, U., Masood, R., Shibli, M. A., & Niazi, M. A. (2014) ‘Cloud identity management security issues & solutions: a taxonomy’, *Complex Adaptive Systems Modeling*, vol.2, no.5, pp. 1-37.

[9] Sultan, N. (2014). Making use of cloud computing for healthcare provision: opportunities and challenges. *International Journal of Information Management*, vol. 34, no.2, pp. 177-184.

[10] Safa, N. S., Sookhak, M., & Solms, R. V., (2015) ‘Information security conscious care behaviour formation in organizations’, *Computers & Security*, vol. 53, no. 3, pp. 65-78.

[11] Zapata, B. C., Fernández-Alemán, J. L., & Toval, A. (2014) ‘Security in Cloud Computing: a Mapping Study’, *Computer Science and Information Systems*, vol. 12, no.1, pp. 161-184.

[12] Sommer, T. (2013). Cloud computing in emerging biotech and pharmaceutical companies. *Communications of the IIMA*, vol.13, no.3, pp. 37-53

[13] Youssef, A. (2014) ‘A Framework for Secure Healthcare Systems Based on Big Data Analytics in Mobile Cloud’, *International Journal of Ambient Systems and Applications*, vol.2, no.2, pp. 1-11.

[14] Khana, F. A., Alia, A., Abbas, H., & Haldar, N. H. (2014) ‘A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks’, *Procedia Computer Science*, vol.34,no.1, pp. 511-517.

[15] C. Esposito, M. Ciampi, and G. De Pietro,(2014) ‘An Event-Based Notification Approach for the Delivery of Patient Medical Information,” *Information Systems*, vol. 39, no.4, pp. 22–44.

[16] Kuo, A. M. (2011). ‘Opportunities and Challenges of Cloud Computing to Improve Health Care Services’, *Journal of Medical Internet Research*, vol.13, no.3, pp. 58-71.

[17] Vidia, S., Vani, K., & Kavin, P. D. (2012) ‘Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing’, *International Journal of Engineering Research & Technology*, vol. 1, no.10, pp. 1-5.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 5, May 2019

[18] Takabi, J. B. D. Joshi, and G.-J. Ahn,(2010) ‘Security and privacy challenges in cloud computing environments’, *IEEE Security Privacy*, vol. 8, no. 6,pp. 24–31.

[19] J. Lloret, M. Garcia, J. Tomas, and J. J. Rodrigues, ``Architecture and protocol for intercloud communication," *Inf. Sci.*, vol. 258, pp. 434_451,Feb. 2014.

[20] Chen, T. S., Liu, C. H., Chen, T. L., Chen, C. S., Bau, J. G., & Lin, T. C. (2012) ‘Secure Dynamic access control scheme of PHR in cloud computing’, *Journal of medical systems*, vol.36, no.6, pp. 4005-4020.

[21] Johnstone, M. (2012). Cloud security: A case study in telemedicine. 1st *Australian e-Health Informatics and Security Conference*, December 3rd-5th, Perth, Western Australia.

[22] Gunamalai, C., & Sivasubramanian, S. (2015) ‘A novel method of security and privacy for personal medical record and DICOM images in cloud computing’, *Journal of Engineering and Applied Sciences,* vol. 10, no.10, pp.4635-4638.

[23] Balasubramaniam, S., & Kavitha, V. (2015). Hybrid Security Architecture for Personal Health Record Transactions in Cloud Computing’, *Advances in Information Sciences and Service Sciences,* vol. 7, no.1, pp.121-130.

[24] Jaswanthi, B., & NaliniSri, M. (2013) ‘Confidentiality and Privacy in Cloud Computing using Hybrid Execution Method’, *International Journal of Science and Modern Engineering,* vol. 1, no.5, pp. 84-89.

[25] Cloud Standards Customer Council 2015, Practical Guide to Cloud Service Level Agreements, Version 2.0. http://www.cloud-council.org/deliverables/practical-guide-to-cloud-service-agreements.htm

[26] Cloud Standards Customer Council 2016, Public Cloud Service Agreements: What to Expect and What to Negotiate, Version 2.0. http://www.cloud-council.org/deliverables/public-cloud-service-agreements-what-to-expect-and-what-to-negotiate.htm

[27] Floridi L. The ethics of information. Oxford: Oxford University Press; 2013.

[28] G. Singh, S. Sood, and A. Sharma,(2011) ‘CM-measurement facets for cloud performance," *Int. J. Comput. Appl.*, vol. 23, no. 3, pp. 37-42.

[29] B. Grobauer, T. Walloschek, and E. Stocker (2011), ‘Understanding cloud computing vulnerabilities,’ *IEEE Security Privacy*, vol. 9, no. 2, pp. 50-57.

[30] Bruin, B.D.& Florida, L (2017) ‘The ethics of Cloud computing’, *Sci. Eng. Ethics*, vol.23, no.4, 21–39.