International Journal of Mechanical Engineering and Technology (IJMET)
Volume 9, Issue 3, March 2018, pp. 71–78, Article ID: IJMET_09_03_008
Available online at http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=9&IType=3
ISSN Print: 0976-6340 and ISSN Online: 0976-6359

© **IAEME** Publication **Scopus** Indexed

SECURITY ANALYSIS IN MULTI-TENANT CLOUD COMPUTING HEALTHCARE SYSTEM

R. John Victor and Monisha Singh
Department of Computer Science,
Christ University, Bengaluru, Karnataka, India

ABSTRACT

Cloud Computing is an innovation in the field of Information Technology and in healthcare system because of the deployment models which services as profitability for the tenants. Cloud Computing is cost-effective, flexible and a delivery platform which provides business and services over internet. Multi-tenancy with its hardware sharing and high degree of configurability is utilized in cloud computing health care system even though many health care organizations are unwilling to adapt due to infrastructure and security shortcoming. In order to store the sensitive health care data cloud service providers should include promising security features where both the trusted and untrusted parties should be addressed in it. This paper addresses the security requirements and security issues in multi-tenant healthcare system, a frame is proposed for analyzing the security issues based on the available requirements and possible counter measures been suggested. The security concerns are analyzed by trust, confidentiality, integrity, audit and compliances and furthermore insight for the security is provided in multi cloud with possible security recommended for healthcare system.

Key words: Cloud Computing, Multi-tenancy, Health Care System, Security Analysis

Cite this Article: R. John Victor and Monisha Singh, Security Analysis in Multi-Tenant Cloud Computing Healthcare System, *International Journal of Mechanical Engineering and Technology* 9(3), 2018, pp. 71–78.
http://www.iaeme.com/IJMET/issues.asp?JType=IJMET&VType=9&IType=3

1. INTRODUCTION

Cloud Computing is the most popular technology available currently, with an instance to compute. As computing a utility customers utilize “pay-to-go” for computing, storage and application purpose [1]. It is a service model that offers tenants, term for consumers, provide a shared computing resources [2]. With the concept of pay-to-go it has the flexibility to upgrade and downgrade the resource making it popular model for organizations [1]. Cloud Computing is defined “Data center in which resources are shared by its virtualization technology, it provides elastic, on demand instant services and charge for the utilities”. Elasticity, on demand, Broad network access, Scalability, Pay-to-go and virtualization are the some of the characteristics of cloud computing model [1]. Cloud Computing is a new sculpt that is used for delivering and hosting information technology (IT) service. As many definitions been

given for cloud computing but the most standard one by the National Institute of standards and Technology (NIST) defines "Cloud computing is a model to facilitate on-demand network access shared based on computing resources configured like networks, servers, storage, applications and services rapidly improvised with minimal management and service interaction [3]. Cloud computing has a new architecture known as multi-tenancy. It has formal definition given by Bezemer "Multi-tenant application let tenant (customers) to share same hardware resources, providing with shared application and database instance allowing application to fit their needs as it runs in dedicated environment". Multi-tenancy has the ability to share hardware resources and offering high degree of configurability to software. It has the architecture in which multiple tenants use single database and application instance in a single environment and security breach can result in exposure of data to other tenants [2]. Multi-tenancy demanding to accomplish commercial growth in cloud computing which utilize resource sharing and virtualization. Multi-tenancy is different for different service models. Such as software as a service (SaaS), application is provided as facility by service provider in which tenants cannot observe or control essential infrastructure. In Infrastructure as a service (IaaS), where tenant is capable for provisioning, storing and networking resource can be controlled but cannot managed. Multi-tenancy arises when more than two virtual devices belong to different tenant share same physical resource. Multi-tenancy provides huge opportunity for the software developers even though expert sees vulnerability it is a major cloud computing features and will advances to confidentiality breach [1]. Though multi-tenancy helps achieving utilization in cloud, multi-tenancy challenges HIPAA compliance in health cloud by making it more vulnerable to cyber-attacks and data breaches. In this paper, we address the access control vulnerabilities introduced by multi-tenancy in cloud based health care information system. HIPAA compliance in health cloud emphasizes control mechanism to address HIPAA regulations. Health care entities are based on elements of HIPAA act [1]. Entities of health care are defined as health plans, health care providers and health care clearing houses, health care information's are transmitted electronically with connection transactions for health and human services.

2. RELATED WORK

In [2] Jason Flood has proposed a framework which actively detects security liabilities in a multi-tenant environment. While detecting the attacks it ensures that the information collected will be isolated in a legal forensic standard at all time. The main goal was to share malicious activity of user information with the authorities devoid of the data leakage of data of all the other tenants. In addition to it the author has described a methodology which would prevent the gap analysis phase of any cyber-attack.

In [3] the author proposed a security model for the requirements of health care system. Electronic health record sharing and integration we discussed, risk in the security and privacy issues are analysed for access and management a use case scenario is described for the corresponding security counter measures and techniques.

In [4] the author proposed a security analysis in order to identify the vulnerabilities and threats found in the cloud computing environment and counterfeit measures has been suggested for threats, an SPI model had been presented to categories the security issues for service model in Cloud Computing.

In [5] the author proposed a platform changing legacy application for multi-tenant model where the platform is converted to embedded system and single tenant to multi cloud, through tenant filter function data access is isolated, then the certification is combined with SaaS platform and performance test is done to migrated the system.

In [6] the author has proposed a Multi eHealth Cloud Service Framework MeCa) by adopting an approach which represents a set of evolving services and applications in their architecture that includes a new technology for smarter eHealth. Their research carries out a real testbed which was demonstrated that MeCa was a constraint optimized mobile eHealth application thereby saving consumption of energy in a Home-Assisted Living.

In [7] the author proposed a security model for the requirements of health care system. Electronic health record sharing and integration we discussed, risk in the security and privacy issues are analysed for access and management a use case scenario is described for the corresponding security counter measures and techniques.

In [8] the author proposed a software-defined framework of cloud security, for supporting the execution of security guidelines in a distributed cloud environment. It requires a security mechanism that is able to cope with their property of multi-tenancy and multi-cloud. This framework depends on the paradigm to construct and adjust mechanisms to circulated cloud constraints dynamically, and achieve the software logics to broadcast security policies which is to be considered in cloud resources. The framework was assessed via validation scenarios of use cases which comprises, cloud source state change, dynamic access control and cloud resource allocation/deallocation

In [9] the author proposed a virtualization framework that provides network communication design by supporting traffic matrices in virtual private clouds (VPCs) and eliminates the problem of load-balancing by using a design link algorithm. The configurations of bare metal data centre along with dynamic network environments were taken as inputs applying a global bound on all the links. The framework focuses on a fat tree architecture.

In [10] the author proposed an approach based on Secure Multi-Party Computation (SMC) protocols to warrant privacy issues in various collaborative systems. The proposed result is based on Paillier structure to ensure security of information that was achieved additive homomorphic property of this public key cryptosystem.

In [11] the author implements a Multi-Tenancy Architecture which is secure and more efficient. A performance evolution framework was developed in the multi-tenant architecture. Their research states that in the area of multitenancy in cloud, in spite of its significance, it is unexploited fully.

In [12] the author proposed an EMH (Elastic Multi-Hospital Management) model, which made use of cloud elasticity facility to deliver a framework that manages objects and physical spaces within multiple healthcare societies. Their solution offers a centralized management control centre which works with cloud elasticity to enlarge or reduce the number of virtual machines to support the variable incoming demands from the hospitals. The model in [4] is based on the RFID (Radio-frequency identification) sensor tracking with the client-server Service, in order to detect motion and objects. A prototype of the model was developed that provides a unique admin point and handles workload with cloud elasticity to report all the user requests within a short response time.

3. METHODOLOGY

System Model

The contact that the consumer and cloud has is the registration unit. It can be either an online form or a contract. The information should be allocated and gathered in order to verify and approve the information. This process is taken in consideration to avoid fraud possibility

resource allocation manager unit RAMU will allocate resource for the following customer request it is able to access the cloud database [3].

Threat Model

For securing the hypervisor an assumption is made that the multi tenancy is allowed by the cloud providers result in allowing resource over shared virtualization. It is designed regardless to exploit multi tenancy vulnerability [3].

Attack Model

Can be considered into Side channel attack, Brute forcing, Network probing. A side channel attack is based on information gain through the physical implementation of system. Brute forcing is the simplest strategies to build and attack and it is a most common used strategy. Network probing helps to find the physical topology where IPs and servers connected through networks [2].

Data Ontology

Core for most of the SaaS multi-tenant applications in which the intermediate data passed through different components, where the data is customized to include load balancing, encryption, schema and storage [7].

Conceptual Data Modeling

Constructed through ontology system it is used as a map of concepts and relationships, used to describe the application significance and similar to object oriented design it doesn't decide the actions and entities [10].

4. GENERAL SECURITY REQUIREMENTS FOR CLOUD COMPUTING HEALTHCARE SYSTEM

Availability

Availability promotes the accessibility and readability only to authorized personnel's only. Property availability can be made unobtainable to legitimate users on permanent and temporary basis. DoS attacks, natural disaster and equipment outage are the threats. It is hard to detect attack possibilities on the system or the services it affects the accessibility while it outsources the assets and data in healthcare organization to the service providers.

Confidentiality

Confidentiality denotes the authority and authorization to access the protected medical data. It ensures the users who are not permitted have entry to the data stored in cloud infrastructure. Confidentiality is related to authentication and tenant account to be protected from attackers.

Integrity

Information security is a data which portrays the resources and data which can be updated through official personnel's. It is related to software, hardware and data base of medical organizations. The conscientiousness of cloud service provider maintains the data integrity and its accuracy.

Privacy

For cloud computing tenant's privacy is considered to be important in both terms compliance with HIPAA standards and trust of healthcare organizations.

Trust

It demotes the property adequate convenience to its observers and works in its correct state to secure the threats. The system and the process is dependent to the service providers for its availability and utility of the service in cloud environment.

5. SECURITY ISSUES IN HEALT CARE SYSTEMS

Data Security

Referred as digital privacy measures to prevent unauthorized access. Protects from data corruption and it is an essential aspect for IT organization. Data security incudes Masking of data and erasure. It measures in encryption where all the digital data, software and hardware are encrypted which is unreadable for unauthorized access. It is important for health care records where patient record should be maintained and creating awareness to release data to medical faculties with care.

Data Breaches

Data breaches mostly involved in personal health information(PHI) in order to trade secrets. Common data breach concept attackers hacking the health records and using the patient's sensitive data and unauthorized hospital employee viewing patient's health information which is a constitutes data breach.

Network Security

Sharing of the patient data with several virtual machines. Data should be securely shared and improving the effectiveness, avoid disruption in service and enabling the continuous compliance, reducing liability in order to contain cost.

Authentication and Authorization

Patients records to be authenticated by the medical faculties with the organizational and through personal identification. Digital identities are increased to facilitate the transaction in various domain system. Authorization of the faculties permission in term to access the health records according to his/her rights information available in the organization. Authorization addresses the issue of responsibilities assigned to the medical faculties with the respective authorities in terms of addition, deletion, editing and uploading of records.

Backup

In health care organization backup of medical data likely encounters damaged target media which requires costly time consuming data services. Medical faculties error formatting of backup medium and overwriting od backup data. Deletion of data file due to replication of remote mirroring.

Web Application Security

There are critical web application vulnerabilities which is been listed such as the non-validated input, broken access control, broken authentication and session management, cross site scripting, buffer over flow, insecure storage, denial of services and insecure configuration management. Which is found in the health care organizations the major flaws result with human logics and interpretation.

6. PROPOSED FRAMEWORK FOR SECURITY ANALYSIS IN HEALTHCARE SYSTEM

In order to analyse the security utilities a criterion is classified into eight different security sub types to evaluate the issues in healthcare infrastructure.

Year	Cloud Security	Data Integrity	Service Availability	Privacy/ Security	Single Cloud	Multi Cloud	Cloud Storage
2011	Yes	Yes	-	Multi shares +Secret Sharing	-	-	-
2011	Yes	Yes	Yes	DepSky	-	Yes	Yes
2011	Yes	Yes	-	-	Yes	-	Yes
2010	Yes	-	-	RACS	-	Yes	Yes
2010	Yes	Yes	-	ICS	-	Yes	Yes
2010	Yes	-	-	SPORC	Yes	-	-
2010	Yes	-	-	-	-	-	-

Figure 1 Framework for security analysis in health care systems

Audit and Compliance

Medical data collection labels the analysis of data archival requirements for the needs of the information technology environment. Capturing, archiving, analysis, reporting and retrieving are the main processes in the subsystem which occurred during normal operation.

Access Control

Security bridging implies the access between the processes and the services within the environment via through entity identified through authentication and authorization.

Flow Control

The security policies bridged between the visibility and flow of information to ensure the information integrity bounded to the computing environment.

Credential Management and its Identity

For the creation and maintaining the permission identity for the objects regarded in order to explain access information and rights for networking to all other platforms and process sub system in a computing environment. It has an essential legal liability for managing and creation of objects incorporated with credentials.

Solution Integrity

It has the need for dependable and functional accuracy regarding the computational solution for the cloud environment.

Digital Signature

Unauthorized modification of data is prevented for all the possibilities of signature at attribute level.

Internal Replication

In order to prevent the data loss, Cloud providers should be able to provide backup and internal redundancy against document loss, to achieve availability of information for long term.

Secret Sharing Scheme

Data availability is increased by redundantly spreading multiple cloud providers. It prevents the cloud providers from spying on data which is key compromised in order to reduce the leakage of information in multi cloud, further to reduce the encryption errors or to comprise the decryption key to prevent from the cloud providers.

7. CONCLUSIONS

The use of cloud computing infrastructure reduces the structural cost of the medical organizations and the security is not measured significantly. Medical organization are worried about the unauthorized access of which will eventually lead to confidentiality and availability to the service will be in loss and data will misled to the cloud infrastructure. Multi cloud in health care framework is added with adequate enhanced security innovation which will lead to secure the medical data in terms of its requirement, the security issues address more than the current existing one in terms of single cloud, multi cloud with the enhanced framework will help to secure the vulnerabilities which will eventually led to data loss of medical images which reduces the trust in the cloud providers by the healthcare industry. The supplemented framework in multi-cloud will addresses the security risk in the healthcare infrastructure and provide proper assurance to it.

REFERENCES

[1] R. Zhang and L. Liu, “Security models and requirements for healthcare application clouds,” Proc. - 2010 IEEE 3rd Int. Conf. Cloud Comput. CLOUD 2010, pp. 268–275, 2010.

[2] J. Flood and A. Keane, “A proposed framework for the active detection of security vulnerabilities in multi-tenancy cloud systems,” Proc. - 3rd Int. Conf. Emerg. Intell. Data Web Technol. EIDWT 2012, pp. 231–235, 2012.

[3] H. Aljahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and J. Xu, “Multi-tenancy in cloud computing,” *Proc. - IEEE 8th Int. Symp. Serv. Oriented Syst. Eng. SOSE 2014*, pp. 344–351, 2014.

[4] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *J. Internet Serv. Appl.*, vol. 4, no. 1, p. 5, 2014.

[5] H. Ali, K. Khattak, H. Abbass, A. Naeem, K. Saleem, and W. Iqbal, "Security Concerns of Cloud-Based Healthcare Systems :," no. ReHIS, pp. 61–67, 2015.

[6] F. Ramalho, A. Neto, K. Santos, J. B. Filho, and N. Agoulmine, "A holistic approach to enable perceptive, instrumental and ubiquitous smart eHealth," LANOMS 2015 - 8th Lat. Am. Netw. Oper. Manag. Symp., pp. 56–61, 2015.

[7] M. Anwar and A. Imran, "Access Control for Multi-tenancy in Cloud-Based Health Information Systems," *Proc. - 2nd IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2015 - IEEE Int. Symp. Smart Cloud, IEEE SSC 2015*, pp. 104–110, 2016.

[8] E. Benkhelifa, D. A. Fernando, and A. Alangari, "Customised performance benchmarking for novel multi-tenancy architecture," Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. AICCSA, 2017.

[9] M. Compastie, R. Badonnel, O. Festor, R. He, and M. Kassi-Lahlou, "A software-defined security strategy for supporting autonomic security enforcement in distributed cloud," Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, pp. 464–467, 2017.

[10] J. Duan and Y. Yang, "A Load Balancing and Multi-Tenancy Oriented Data Center Virtualization Framework," IEEE Trans. Parallel Distrib. Syst., vol. 28, no. 8, pp. 2131–2144, 2017.

[11] M. Marwan, A. Kartit, and H. Ouahmane, "Applying secure multi-party computation to improve collaboration in healthcare cloud," Proc. - 2016 3rd Int. Conf. Syst. Collab. SysCo 2016, 2017.

[12] C. J. Guo, W. Sun, Y. Huang, Z. H. Wang, and B. Gao, "A Framework for Native Multi-Tenancy Application Development and Management A Native Multi-tenancy Enablement Framework Challenges of the Native Multi-tenancy Pattern," ECommerce Technol. 4th IEEE Int. Conf. Enterp. Comput. ECommerce Eser. 2017 CECEEE 2007 9th IEEE Int. Conf., pp. 551--558, 2017.

[13] M. Almorsy, J. Grundy, and A. S. Ibrahim, "SMURF: Supporting multi-tenancy using re-aspects framework," Proc. - 2012 IEEE 17th Int. Conf. Eng. Complex Comput. Syst. ICECCS 2012, pp. 361–370, 2017.

[14] J. Flood and A. Keane, "A proposed framework for the active detection of security vulnerabilities in multi-tenancy cloud systems," Proc. - 3rd Int. Conf. Emerg. Intell. Data Web Technol. EIDWT 2012, pp. 231–235, 2017.

[15] R. D. R. Righi, G. Rostirolla, C. A. Da Costa, M. Goulart, and E. Rocha, "Elastic Management of Physical Spaces and Objects in Multi-Hospital Environments," Proc. - 2016 IEEE Int. Conf. Internet Things; IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016, pp. 33–38, 2017.

[16] Gangu Dharmaraju, J. Divya Lalitha Sri and P. Satya Sruthi, A Cloud Computing Resolution in Medical Care Institutions for Patient's Data Collection. International Journal of Computer Engineering and Technology, 7(6), 2016, pp. 83–90

[17] Dr. V. Goutham and M. Tejaswini, A Denial of Service Strategy To Orchestrate Stealthy Attack Patterns In C loud Computing , International Journal of Computer Engineering and Technology, 7(3), 2016, pp. 179 – 1 8 6

[18] T. Rajesh and Dr. S. Mohan Kumar, Medical Diagnosis Cad System Using Latest Technologies, Sensors and Cloud Computing. International Journal of Computer Engineering & Technology, 8(1), 2017, pp. 43–50.

[19] Naga Raju Hari Manikyam and Dr. S. Mohan Kumar, Methods and Techniques To Deal with Big Data Analytics and Challenges In Cloud Computing Environment. International Journal of Civil Engineering and Technology, 8(4), 2017, pp. 669-678.