SSSSSS

by mithula nithmali

Submission date: 12-Aug-2020 03:07PM (UTC+0530)
Submission ID: 1366423753
File name: ssd_Assignment.docx (23.56K)
Word count: 2915
Character count: 16994

Abstract

Cloud computing is a modern way of providing knowledge and services. Most administrators and analysts agree it can enhance health care programs, support health care studies, and transform the face of information technology for the health. Large global companies are now investing millions of dollars in infrastructure, facilities, software and applications to promote the use and utilization of cloud computing by customers, organizations, and businesses. How cloud computing can affect the healthcare sector remains to be seen as it is very complex, dynamic and specific, and poses many challenges such as securing health information for members. However, Health care data are very critical documents and must not be given access to unauthorized persons to protect the information security of patients. The data centralization in the cloud poses many questions regarding protection and privacy for people and health care providers. This data centralization creates a one-stop honey pot for attackers to steal data and intercept data in motion and transfers data ownership to cloud service providers. In this paper, we briefly described about the cloud computing, common health security issues, recent ehealth security studies and possible approaches for ehealth security.

Keywords: HER-Electronic Health Records

Introduction

With the evolution of Information Technology, more fields replaced their traditional work with the newest technologies. As the result of that healthcare get combined with cloud computing. It is the best solution to provide IT as a Service.*Cloud computing will help healthcare organizations concentrate their resources on healthcare programs and strengthen patient care [1]. Cloud computing benefits from the enormous budget necessary to move all IT infrastructures to provide integrated services to many organizations [1].

Healthcare industry faces many obstacles and growing pressure to minimize the costs of delivering healthcare services, implement modern electronic healthcare systems, and exchange data with other healthcare and government entities easily and securely [1].Government and healthcare agencies have increasingly urged healthcare facilities to improve various e-Health technologies[1]. In general cloud providers store data in multiple data centers and geographic area locations. This issue may cause for both advantage and disadvantage. Because data storage on the cloud will be redundant and different data centers will help recover from disaster. This may vulnerable to thefts and loss of data, store data in different locations would be more vulnerable to theft and loss. There are many security threats associated with cloud use, such as failure to distinguish virtual accounts, identity theft, misuse of privileges and poor encryption [2].

Healthcare data is very sensitive documents and should not be made available to unauthorized parties to protect the confidentiality and privacy of patient information. Transformation of healthcare services to e health clouds vulnerable to various types of attacks, and clouds are accessible in shared environment so it vulnerable to loss of data and theft. And the centralization of cloud data poses many issues regarding protection and privacy of each individual and healthcare providers. Data centralization offers one step honey pot for attackers to steal and intercept data in motion, and transfers data ownership to cloud service providers [2].* This paper talk about Common Health security Issues and available e-health security solutions.

Cloud Computing

What is cloud computing?

According to the NITS definitions Cloud computing is a model for enabling convenient on –demand network access to a shared pool of configurable computing resources such as servers, file storages data and applications that can be rapidly provisioned and release with minimal management effort or service provider interaction [4].

Cloud Deployment Models

Public Cloud provides resources as a service to enables consumers to develop and deploy multiple services in the cloud to general public or industrial organization and available through and automated services or network with low financial investment on infrastructure compared to the capital expenditure requirement with normally associated with other deployment models.
Private Cloud managed and run only by particular organization has to pay more attention and cost for the security requirements of the particular organization. Aim of this private cloud is to provide security and keeping control of user data **Hybrid Cloud** is a composition of private and public cloud types. Have to consider about use of multiple cloud and this will ensure to the security manager about the labelling and classification of the data are assigned to correct cloud type and also there is a risk of merging different types of clouds. **Community Cloud** supports to a specific community such as organization or several organizations who has mutual interests and requirements managed by any of organization in the community or third party service provider.

Cloud service delivery models

IaaS (Infrastructure as a Service) A model refers to the hardware infrastructure provided by Cloud Service Provider hosts servers, processing, storage, memory and various virtualized computing resources with the ability to deploy and run software which can include Operating systems and Application and make them available through the Internet. **PaaS (Platform as a Service)** A model which provide on application development platforms and tools on its own infrastructure and makes them available through network with the capability to deploy on the cloud infrastructure created by client or acquire application creating.
SaaS (Software as a Service) A model which provides application with capability to use the application running on cloud infrastructure through internet and incorporates by cloud service provider.

Key features of Cloud Computing

On – Demand self Service Services in the cloud can accessed and handled without any human intervention by customers through the cloud service providers.
Broad Network Access Computing services, application and data of customers available and accessible via the standard mechanisms using protocols.
Resource Pooling provides concurrent cloud services to multiple clients by pooling in a multi – tenant environment.
Rapid Elasticity According to the customer perspective, no limitation in resource provisioning.

E-health cloud benefits

Data availability for healthcare stakeholders [2]

Decreases data storage costs – no need of buying hardware and softwares.

Enhance patient care – continuous interaction of the patient with different stakeholders.

Enhance Medical Researches: centralized data repository provides opportunity to support medical researches and disease controls

E-health cloud limitations

Security and privacy - open and shared environment of e health cloud cause of vulnerability to loss of data and thefts.

Availability and reliability - Verification of identities that meet similar safety standards and define specific data protection and information security needs.

E-health cloud is vulnerable to different types of security attacks like Denial – of services attacks, authentications attacks etc.

Limited control: Centralization of limits the control over data ownership

Interoperability Issue: risk of managing data within shareable environment. Therefore standards are required to achieve proper communication, coordination and collaboration across the platforms of health care providers.

4. Common e health security issues

Today, Healthcare focuses on obtaining medical records anytime, wherever. Usage of healthcare cloud computing framework allows for collaboration and aggregation of medical information. The clod computing model does offer some advantages but also raises risks to privacy and protection of health data. The cloud service providers must address cloud security issues to increase the level of trust between patients and healthcare providers [1]. Throughout this segment, we address important safety criteria for eHealth systems and discuss privacy concerns that impede the broad-based adoption of cloud computing by healthcare providers.

The International Medical informatics Association (IMIA) studied data privacy and security problems in networked health-care systems [2]. The research paper, "A secure framework for sharing electronic health records over clouds" proposed a platform allowing for safe cloud-based sharing of HER among various healthcare providers .It provides EHRs with confidentiality, integrity, authenticity, availability of EHRs [3].

R. Gajanayake, R. Iannella, T. Sahama developed a special privacy policy and secured oriented access management design just for e-Health. Their architecture was obtained by integrating 3 distinct safety models such as Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC). The biggest downside of this system is its potential to be effective only as an individual security model in order to satisfy the criteria of health electronic records [4].

Security and privacy issues in the eHealth environment are not just about adhering to the security paradigm of confidentiality, integrity and availability (CIA). In [5], P. Metri and G. Sarote argue that cloud data protection risks involve spoofing identity by an attacker pretending to be a real user, stomping on data involving noxious adjustments and material modifications, repudiation of users denying their signature legitimacy after performing a data operation, and leakage of information by access to unauthorized users.

F. Rezaeibagha and Y. Mu built up a completely unique access-control system to deal with the the difficulties of security and privacy in Electronic Health Record. The system embraced hybrid clouds and also some cryptographic building blocks were implemented with access control policy transformation to tackle various EHR users with different access rights and permissions in different cloud environments to make the model effective[6]. The biggest downside with this system is its failure to provide user space to extend. This does not offer space for scalability, since there is a small number of users.

5. Recent ehealth security studies.

There is a huge amount of research undertaken to tackle protection and privacy concerns in eHealth. We review recent works in this section.

The research paper, "Data security and privacy challenges in adopting solutions for IOT," (2016) describe many failures in healthcare safety related to non-repudiation, the CIA model and what it means for healthcare industry stakeholders. They also address several established organizational approaches and risk reduction methodologies, and distinguish what the industry should do to reduce security risks and threats to privacy [8].

Kennedy Edemacu, Beakcheol Jang and Jong Wook (2020) Kim introduced a new descriptive, productive and collusion-resistant access control scheme with immediate attribute for secure sharing of wellbeing information in community health frameworks. The proposed method also accomplishes forward and in reverse security. However, when implementing in the real world, two impediments could impact their proposed access control schema. First, with the amount of attributes involved, ciphertext and key sizes increase linearly. This can be bedetrimental in environments where there is a high number of attributes, but the system does have minimal capacity and resources on network and second, Depending on the scale of the data currently being covered for protection. At the point when their access control scheme is sent in reality, there could be a slight increment in computational proficiency [12].

K. Shah and V. Prasad (2017) list numerous encryption methods as well as addressing security and privacy issues in the cloud of health care by introducing a new system with cloud-based privacy-aware role-based access control (CPRBAC) model. The purpose of this is to decrease overhead computing complexity and communication. Nonetheless, there doesn't include comprehensive research examination of the approach's efficacy and its mitigation of attacks on security and privacy [9].

B. Dhivya, S. P. S. Ibrahim, and R. Kirubakaran describe a system that enables safe cloud-based sharing of EHRs among various health care providers. The article also reveals that the suggested solution is immune to man-in-the-middle attacks and replay attacks. In any case, they didn't examine the scalability of the methodology as well as its sensitivity to other serious security threats, including data integrity and availability, and also overhead computing [10].

M. Marwan, A. Kartit, and H. Ouahmane propose (2017) a new approach based on Shamir's Hidden Sharing Scheme (SSS) and multicloud definition to boost cloud storage capacity to support security criteria to prevent data loss, unauthorized access and privacy leakage. The suggested strategy splits the confidential data into several small shares, therefore no information on medical records is revealed. In addition to the mutli-cloud architecture, data is spread through different cloud storage networks. Therefore confidentiality of the data is secured. But the argument is no aspects of optimum number of shares and no standard review of collected health care data are discussed in the article [11].

Availability of Security issue solutions

Because of the risks involved such as unauthorized use or access to private and confidential health data, many healthcare providers use cloud technologies with caution. To alleviate protection and privacy issues, cloud service providers have to follow certain guidelines and recommendations. There are some standards used by different countries to ensure cloud privacy and security.

US Standards

Health Insurance Portability and Accountability Act (HIPAA)

The purpose is to preserve the privacy of sensitive information about patients. HHS provide HIPAA security rules and privacy rules, to protect the privacy and security of data. Main goal of the HIPAA privacy rules is to provide set of standards and guidelines to protect patient's medical and HIPAA security rules provide security to each patient health records with the allowing technological bodies which support healthcare services and produces high - quality services for patients and healthcare providers. [2]

Health Information Technology for Economic and Clinical Health (HITECH)

Through providing benefits and awarding grants, the HITECH promotes healthcare providers, and enhance public interest in HER through ensuring adequate privacy and security controls. Lack of financial resources, technical expertise and secure infrastructures motivated the HITECH act regulations [2].

General Data Protection Regulation (GDPR)

GDPR is the European Union which regulates the protection of EU citizen's individual data. It is a newest data protection regulation established since 2018. Cloud service Providers should demonstrate compliance by keeping all data processing activities logged in. They will take suitable personal and organizational measures and should apply the appropriate personal and organizational measures. According to the new regulations, companies will ask consumers for clear consent, customers do have the right to opt out, and businesses will keep a record of all consumer consent. Data security by design means service providers should design their processes to respect the privacy of users, should comply with the laws on safety, and they will track what personal data they carry, where it originated, with whom they share it, and where they store consumer data. Furthermore, data must be used for the purpose that it was gathered. Under the new legislation the rights of data subjects are extended. The new legislation grants customers the right to be forgotten, and data must be deleted permanently if necessary. For all Member States, reporting of breaches is mandatory; the new act requires a organization to report data breaches to the regulator and consumer within 72 hours or face serious penalties. Organizations will also have measures in place to recover when they do arise from security breaches. "Commonly use and machine readable" format. They do have the option to pass on their data to another provider [2].

ISO/IEC 27000 –Series

The ISO/IEC 27000 published by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC). And it for standards reserved for address information security concerns and provides best practices on information security.

Conclusion

Cloud computing is a modern computing paradigm that aims to give end-users more versatility, less cost and more productivity in IT services. This offers future opportunities to increase implementation of EHR, health care facilities and research. However, as mentioned above, there are still many obstacles to promoting the new healthcare models. Security is one of the key issues hindering the fast cloud computing adoption in the healthcare sector. The qualities and advantages of distributed computing far surpass its risks and dangers. Without a significant interest in framework and labor, security guidelines are progressively hard to meet. In this paper, we discussed about small

introduction about cloud computing, common e-health security issues, recent work in e-health security and available e health security solutions.

From the discussion in this chapter, one can easily understand healthcare security issues, healthcare responsibility, and how we can secure our information in the healthcare cloud.

References

1)S. Allen, “Cloud Computing and Health Care Security,” Cloud Computing Journal, 2011.

2) US Department of Health & Human Services (HHS), Health Information Privacy, US Department of Health & Human Services (HHS), Washington, DC, USA, 2005.

3) A. Ibrahim, B. Mahmood, and M. Singhal, “A secure framework for sharing electronic health records over clouds,” in *IEEE International Conference on Serious Games and Applications for Health (SeGAH)*, pp. 1–8, Kyoto, Japan, May 2016.

4) R. Gajanayake, R. Iannella, T. Sahama Privacy oriented access control for electronic health records e-J Health Inf, 8 (2) (2016), pp. 175-186

5) P. Metri and G. Sarote, “Privacy issues and challenges in cloud computing,” *International Journal of Advanced Engineering and Technology*, vol. 5, no. 1, pp. 5-6, 2011.

6) F. Rezaeibagha, Y. Mu,Distributed clinical data sharing via dynamic access-control policy transformation,Int J Med Inf (2016), pp. 25-31

7)

8) S. Supriya and S. Padaki, “Data security and privacy challenges in adopting solutions for IOT,” in Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE green Computing and communications (GreenCom) and IEEE cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 410–415, Chengdu, China, 2016.

9) K. Shah and V. Prasad, “Security for healthcare data on cloud,” International Journal on Computer Science and Engineering (IJCSE), vol. 9, no. 5, 2017.

10) B. Dhivya, S. P. S. Ibrahim, and R. Kirubakaran, “Hybrid cryptographic access control for cloud based electronic health records systems,” International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 2, no. 2, 2017.

11) M. Marwan, A. Kartit, and H. Ouahmane, “Protecting medical data in cloud storage using fault-tolerance mechanism,” in Proceedings of the 2017 International Conference on Smart Digital Environment, pp. 214–219, Rabat, Morocco, July 2017.

12) Kennedy Edemacu, Beakcheol Jang, Jong Wook Kim,"Collaborative Ehealth Privacy and Security: An Access Control with Attribute Revocation based on OBDD Access Structure",IEEE Journal of Biomedical and Health Informatics, April 29,2020 a

SSSSSS

ORIGINALITY REPORT

30%	22%	26%	25%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.hindawi.com Internet Source	9%
2	Submitted to De Montfort University Student Paper	2%
3	www.ripublication.com Internet Source	2%
4	Submitted to Sheffield Hallam University Student Paper	2%
5	Nureni Ayofe Azeez, Charles Van der Vyver. "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis", Egyptian Informatics Journal, 2019 Publication	1%
6	Kennedy Edemacu, Beakcheol Jang, Jong Wook Kim. "Collaborative eHealth Privacy and Security: An Access Control with Attribute Revocation based on OBDD Access Structure", IEEE Journal of Biomedical and Health Informatics, 2020 Publication	1%

7	Yazan Al-Issa, Mohammad Ashraf Ottom, Ahmed Tamrawi. "eHealth Cloud Security Challenges: A Survey", Journal of Healthcare Engineering, 2019 Publication	1%
8	link.springer.com Internet Source	1%
9	Submitted to Laureate Higher Education Group Student Paper	1%
10	Submitted to University of Petra Student Paper	1%
11	secappdev.org Internet Source	1%
12	thinkmind.org Internet Source	1%
13	www.coursehero.com Internet Source	1%
14	Submitted to Webster University Student Paper	1%
15	Submitted to Northcentral Student Paper	<1%
16	Craig A. Stewart, Richard Knepper, Matthew R. Link, Marlon Pierce, Eric Wernert, Nancy Wilkins-Diehr. "chapter 645 Cyberinfrastructure,	<1%

Science Gateways, Campus Bridging, and Cloud Computing", IGI Global, 2015
Publication

17	digitalcommons.ilr.cornell.edu Internet Source	<1%
18	Nureni Ayofe Azeez, Charles Van der Vyver. "Chapter 5 Security Challenges and Suggested Solutions for e-Health Information in Modern Society", Springer Science and Business Media LLC, 2020 Publication	<1%
19	Submitted to California InterContinental University Student Paper	<1%
20	mitiq.mit.edu Internet Source	<1%
21	"Smart Infrastructure and Applications", Springer Science and Business Media LLC, 2020 Publication	<1%
22	Mbarek Marwan, Ali Kartit, Hassan Ouahmane. "Secure cloud-based medical image storage using secret share scheme", 2016 5th International Conference on Multimedia Computing and Systems (ICMCS), 2016 Publication	<1%
23	Submitted to University of Wales Institute,	

	Cardiff Student Paper	<1%
24	Submitted to City University of Hong Kong Student Paper	<1%
25	"Health Information Science", Springer Science and Business Media LLC, 2015 Publication	<1%
26	Submitted to College of Europe Student Paper	<1%
27	Kennedy Edemacu, Beakcheol Jang, Jong Wook Kim. "Efficient and Expressive Access Control With Revocation for Privacy of PHR Based on OBDD Access Structure", IEEE Access, 2020 Publication	<1%
28	www.slideshare.net Internet Source	<1%
29	appa-net.org Internet Source	<1%
30	Hao Jin, Yan Luo, Peilong Li, Jomol Mathew. "A Review of Secure and Privacy-Preserving Medical Data Sharing", IEEE Access, 2019 Publication	<1%
31	Assad Abbas, Samee U. Khan. "A Review on the State-of-the-Art Privacy-Preserving	<1%

Approaches in the e-Health Clouds", IEEE Journal of Biomedical and Health Informatics, 2014
Publication

32 Shekha Chenthara, Khandakar Ahmed, Hua Wang, Frank Whittaker. "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing", IEEE Access, 2019 <1%
Publication

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		