Emerging Security Concerns for Implementing Cloud Computing in Healthcare Sector

Mervat Adib Bamiah , Sarfraz Nawaz Brohi , Suriayati Chuprat
Universiti Teknologi Malaysia, Malaysia
abmervat3@live.utm.my, nbsarfraz2@live.utm.my, suria@ic.utm.my

***Abstract* — Cloud computing has significant features such as scalability, on-demand self service, availability, reliability that benefit healthcare organizations to improve its quality of service in cost-effective manner. By using cloud services in healthcare it became possible to reach large population of people in isolated geographical areas that will assist in saving their lives since cloud enables the usage of latest technologies through its various service delivery and deployment models via the internet on pay-per-use billing pattern. However, cloud computing has a dark side when it comes to security and privacy considerations. Healthcare organizations are reluctant to trust cloud computing due to the fear of losing their sensitive data, as it resides on the cloud side with no transparency of its location or the Cloud Service Provider (CSP) mechanisms used to secure their data, which have created a barrier against adopting this agile promising paradigm. This paper represents the significance of implementing cloud computing for healthcare and the security concerns that must be addressed in order to adopt and benefit from cloud computing services in healthcare sector.**

Keywords- Healthcare; Cloud Computing, Challenges

I. INTRODUCTION

Cloud computing evolved as a new IT paradigm to provide an agile method to deliver services in smart way. It is a business model that has inherited the benefit of other technologies such as distributed, pervasive, ubiquitous, utility computing and virtualization to offer cost effective and scalable IT services. Cloud computing in healthcare will support existing electronic healthcare and the future trend of implementing smart healthcare systems. The urgent need for pervasive and ubiquitous access to healthcare data is pulled by the market and users' need for advanced and accurate diagnosis and disease treatment procedure for modern medical practices. Canada Health Council has released its second healthcare report in 2011 [1] that described existing healthcare challenges such as the need to integrate healthcare services over providers, services and illnesses. For example, patients with chronic illness are frequently being moved between inpatient and outpatient environment that require collaboration amongst physicians, pharmacists and other healthcare professionals [2]. Another challenge is the need for performance measurement of healthcare service delivery by benchmarking it for best practices. Moreover connectivity is also an additional challenge to handle a heterogeneous healthcare IT infrastructure and various smart devices since successful healthcare interoperability will depend upon healthcare ability to connect people, processes, data, policies and procedures. Limited access to patient-related information during decision making and the ineffective communication among patient care team members may also result in the occurrence of severe medical errors [3]. These challenges have raised the necessity for an agile IT solution such as cloud computing which is a dynamic, flexible and virtualized technology that can benefit healthcare sector to carryout tasks in efficient and cost-effective manner [4]. In healthcare sector, technology contribute in providing high quality of medical services. IT solutions such as electronic healthcare brought significant benefits in solving issues of human errors and providing an agile way of accessing and processing large volume of patient's information as well as saving papers and storage space. The amount of data available in healthcare sector is growing rapidly as paper records moved online and the range of data types makes the process quite complex. Everything from written prescriptions by medical professionals to real-time individual healthcare information readings must be integrated and analyzed for decision making. Certain healthcare information changes very slowly, while some high-volume streaming information is handled in real-time. The increasing number of population and the accelerating innovations of smart electronic devices (Smart phones, robots, sensors, chips etc) have facilitated the dynamic nature of healthcare delivery. However, it requires an IT infrastructure such as cloud computing which supports significant interoperability among the various components to ensure timely, efficient and patient centric care [1].

II. IMPLEMENTATION OF CLOUD IN HEALTHCARE

Various research's have been conducted on cloud computing as an IT solution to improve healthcare services, for-example [6 - 9] have proposed a cloud based system to automate the process of collecting patients' vital data via a network of sensors connected to electronic medical devices and to deliver the data to the cloud storage, real time processing as well as distribution. Another work done in this area is from [10] who described a cloud

computing protocol management system which provides multimedia sensor signal processing and Security as a Service (SCaaS) to mobile devices. This system has relieved mobile devices from executing heavier multimedia and security algorithms when delivering mobile healthcare services that will improve the utilization of the ubiquitous mobile device and expand it to rural communities. [11] reported a pervasive cloud project called Dhatri, which leveraged cloud computing and wireless technologies to enable doctors to access patient health information at anytime from anywhere. [12] described a cloud computing prototype emergency medical system for the Greek National Health Service that integrates the emergency system with personal health record (PHR) systems to facilitate the physicians with easy and immediate access to patient data ubiquitously and pervasively in cost effective way. Furthermore [13 -14] discussed the power of cloud computing paradigm in reducing Electronic Health Record (EHR) start-up expenses. Gartner stated that cloud service revenues are to reach 148.8 billion USD by 2014, with large percentage from the healthcare cloud sector [5]. Some of the world high reputable organizations have also invested in the cloud medical records services such as Microsoft's HealthVault, Oracle's Exalogic Elastic Cloud, and Amazon Web Services (AWS), for processing personal health information online. Several European organizations contracted Trustworthy Clouds which are patient home centric health care service to remotely monitor, diagnose, and assist patients in their own habitat. The complete process will be stored on the cloud and will be accessible healthcare related parties [15].

III. CLOUD COMPUTING IMPLEMENTATION CHALLENGES

Several significant challenges should be considered before adopting cloud computing regarding to its dynamic multi-tenant virtualized nature that are described as follows [16] :

A. Abuse and Nefarious Use of Cloud Technology

Cloud service providers facilitate the users with various types of services including unlimited bandwidth and storage capacity. Some of them offers free limited trial periods that gives an opportunity for hackers to access the cloud immorally, their impact includes decoding and cracking of passwords, launching potential attack points and executing malicious commands. Spammers, malicious code authors and other cybercriminals can conduct their activities with relative impunity, as cloud providers are targeted for their weak registration systems and limited fraud detection capabilities [20].

B. Insecure Interfaces and APIs

Cloud users are using software interfaces and APIs to access and manage the cloud services. These APIs need to be secured since they play an integral part during provisioning, management, orchestration and monitoring of the processes running in a cloud environment. The security and availability of cloud services is dependent upon the security of these APIs so they should include features of authentication, access control, encryption and activity monitoring. APIs must be designed to protect against both accidental and malicious attempts to avoid threats. If cloud service provider relies on weak set of APIs, variety of security issues will be raised related to confidentiality, integrity, availability and accountability such as malicious or unidentified access, API dependencies, limited monitoring/logging capabilities, inflexible access controls, anonymous access, reusable tokens/passwords and improper authorizations [17].

C. Malicious Insider

Insider attacks can be performed by malicious employees at both provider's and user's site. Malicious insider can steal the confidential data of cloud users. A malicious insider can easily obtain passwords, cryptographic keys and files. These attacks may involve various types of fraud, damage or theft of information and misuse of IT resources. The threat of malicious attacks has increased due to lack of transparency in cloud provider's processes and procedures [18]. It means that a provider may not reveal how employees are granted access and how this access is monitored or how reports as well as policy compliances are analyzed. Additionally, users have little visibility about the hiring practices of their provider that could open the door for an adversary, hackers or other cloud intruders to steal confidential information or to take control over the cloud. The level of access granted could enable attackers to collect confidential data or to gain complete control over the cloud services with little or no risk of detection. Malicious insider attacks can damage the financial value as well as brand reputation of an organization.

D. Virtualized Technology Issues

Due to the cloud virtualization, cloud providers are residing the user's applications on virtual machines (VMs) within a shared infrastructure. The VMs are virtualized based on the physical hardware of cloud provider. In order to maintain the security of users, providers are isolating the VMs from each other so if any of them is malicious, it will not affect the other VMs under the same provider. The VMs are managed by hypervisor in order to provide virtual memory as well as CPU scheduling policies to VMs. As the hypervisor is main source of managing a virtualized cloud platform, hackers are targeting it to access the VMs and the physical hardware, because hypervisor resides between VMs and hardware [16], [19] so attack on hypervisor can damage the VMs and hardware. Strong isolation should be employed to ensure that VMs are not able to impact or access the operations of other users running under the same cloud service provider. Several vendors such as Xen and KVM are providing strong security mechanisms of securing the cloud hypervisors, but still it is identified that sometimes security of VMs is compromised.

E. Data Loss or Leakage

Data loss can occur due to operational failures, unreliable data storage and inconsistent use of encryption keys. Operational failure refers to deletion or alteration of records without a backup of the original content that can take place intentionally or unintentionally. Unreliable data storage refers to saving of data on unreliable media that will be unrecoverable if data is lost [20]. The inconsistent use of encryption keys will result into loss and unauthorized accesses of data by illegal users that will lead to the destruction of sensitive and confidential information. Example of data loss is Twitter hacks. The online accounts of Twitter accessed by hackers and their numerous sensitive corporate documents were stolen. These documents were housed in Google's online web office service Google Docs. Although Google was not the one to be blamed for security break-in as the security of documents from twitter was not efficient enough. Instead, the entire company data was only one password crack away from discovery [21]. Loss of core intellectual property can have competitive and financial implications beside the compliance violations and legal consequences.

F. Account Hacking

Account or service hijacking refers to unauthorized access gained by attackers to control the users' accounts, such as phishing, fraud and exploitation of software vulnerabilities. For example if an attacker gains access to users' credentials, they can spy on their activities/transactions, manipulate their data, return falsified information and redirect them to illegitimate sites [22]. Users' account or service instances may become a new base for the attackers who can leverage the cloud service providers' reputation by launching subsequent attacks. With stolen credentials, attackers can often access critical areas of deployed cloud computing services, allowing them to compromise the confidentiality, integrity and availability of those services. Authentication and authorization through the use of roles and password protecting is a common way to maintain access control when using web-browsers to access cloud computing systems.

G. Data Governance and Regulatory Compliance

Clients are responsible of their data and applications even if it resides on third party storage such as cloud [23]. There should be shared data security terms included in Service Level Agreement (SLA) initiated between CSP and clients, based on the sensitivity of their data. Cloud computing should be under well-developed information security governance processes, as part of the client's overall corporate governance obligations with due care in terms of scalability, availability, measurability, sustainability and cost effectiveness. Since cloud physical storages are widely distributed across multiple jurisdictions that have different laws regarding to data security, privacy, usage and intellectual property. CSPs are responsible for incorporating the corresponding regulatory compliance with government and legal country specific policies when deploying client's data and applications [24]. CSPs should satisfy privacy rules by using up-to-date security techniques such as encrypting clients' data and documents on the fly and on the cloud by using strong techniques (e.g. 256 bit AES algorithms) and using firewalls to restrict the traffic to each cloud instance by source IP address. In addition to allowing the access to clients data through Secure Socket Layer (SSL) encrypted endpoints. Furthermore, providing a disaster recovery mechanism that starts quickly in case of a server failure and developing an authorization model to provide discretionary, role-based and context-aware authorizations to prevent any unauthorized access [25].

H. Service Level Agreements (SLAs)

SLAs refer to a legal contract that describes the minimum performance criteria CSPs promises to meet while delivering the required service(s) to their client(s). It defines the responsibilities of the related parties and sets out the remedial action plus any consequences that will take effect if performance falls below the promised standard [26]. Lack of trust by clients will create a barrier against adopting cloud computing paradigm. This lack of clients trust may occur as a result of SLAs not offering a commitment to allow cloud users to audit their data. The loss of data governance causes concerns when user's sensitive data and mission-critical applications move to a cloud computing environment where providers cannot guarantee the effectiveness of their security and privacy controls [27]. In this process clients must understand their security requirements, what control and federation patterns are necessary to meet those requirements in order to protect their rights and themselves against critical business security threats besides holding CSPs responsible for service failure and their confidential data loss.

I. Multi-Tenancy

In cloud environment, multi-tenancy means clients are sharing the same infrastructure and databases in order to take advantage of cost and performance that come with economies of scale. Tenants can share the IT resources which may encounter threats of data loss, misuse, or privacy violation. Ensuring security by means of integrity, access and availability of data, as well as confidentiality and non-repudiation is a must in cloud computing environment where the clients' data is under the control of CSP in multi – tenant shared environment [28]. Security must be considered in all aspects of cloud infrastructure

IV. Conclusion and Future Work

Moving healthcare services to the cloud means that sensitive patient data from hospitals also move to the cloud which can pose severe security and privacy issues. In this paper we presented the challenges that should be considered and overcome for healthcare to trust this promising paradigm. In our future work proposed solution for trusted cloud computing that will be presented with the usage of trusted platform technologies.

REFERENCES

[1] C. Kuziemsky, et al., "3rd Annual Workshop on Interoperability and Smart Interactions in Healthcare (ISIH)," In Proceedings of the 2011 Conference of the Center for Advanced Studies on Collaborative Research (CASCON '11). IBM Corp. pp. 351-352.

[2] C. Doukas, et al., " Mobile healthcare information management utilizing Cloud Computing and Android OS," In Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE. Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE. pp. 1037-1040.

[3] Healthy Living Now, 2012. Health. Available at: http://www.healthylivingnow.org/health.html [Accessed September 5, 2012].

[4] M. Deng, et al., "A Home Healthcare System in the Cloud Addressing Security and Privacy Challenges," In Cloud Computing (CLOUD), 2011 IEEE International Conference on., 2011 IEEE International Conference on. pp. 549-556

[5] P. Mell and T. Grance, "The NIST definition of cloud computing," ACM 2010, 53(6):50.

[6] X. Wang and Y. Tan, "Application of cloud computing in the health information system," In Computer Application and System Modeling (ICCASM), 2010 International Conference on. Computer Application and System Modeling (ICCASM), 2010. pp. V1-179-V1-182

[7] D.B. Hoang and L. Chen, "Mobile Cloud for Assistive Healthcare (MoCAsH)," In Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific. Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific. pp. 325-332

[8] C. Rolim, et al., "A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions," In eHealth, Telemedicine, and Social Medicine, 2010. ETELEMED '10. Second International Conference on. 2010. pp. 95-99.

[9] MT. Nkosi, and F. Mekuria, "Cloud Computing for Enhanced Mobile Health Applications," In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on. Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on. pp. 629-633.

[10] G. Rao, et al, "Dhatri - A Pervasive Cloud initiative for primary healthcare services. In Intelligence in Next Generation Networks (ICIN)," 2010 14th International Conference on. Intelligence in Next Generation Networks (ICIN), 2010 14th International Conference on. pp. 1-6.

[11] V. Koufi, et al., "Ubiquitous access to cloud emergency medical services. In Information Technology and Applications in Biomedicine (ITAB)," 2010 10th IEEE International Conference on. pp. 1-4.

[12] E. Schweitzer, "Reconciliation of the cloud computing model with US federal electronic health record regulations," Journal of the American Medical Informatics Association,2011, JAm Med Inform Assoc amiajnl-2011-000162 [Online] Available at: http://jamia.bmj.com/content/early/2011/07/04/amiajnl-2011-000162 [Accessed September 7, 2012]

[13] J. Haughton, "Year of the underdog: Cloud-based EHRs. Health Management Technology," 2011, 32(1). pp. 9.

[14] A. Kuo, " Opportunities and Challenges of Cloud Computing to Improve Health Care Services," Journal of Medical Internet Research ,2011, [Online] Available at: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3222190/.

[15] W. Jansen and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," .National Institute of Standards and Technology, US Department of Commerce.2011 [Online] Available::http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf [Accessed: September 12, 2012].

[16] M. Bamiah and S. Brohi, "Seven Deadly Threats and Vulnerabilities in Cloud Computing," International Journal of Advanced Engineering Sciences and Technologies (IJAEST) 2011, Vol No. 9, Issue No. 1, 087 – 090.

[17] CSA, "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" Cloud Security Alliance, 2009, [Online], Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[18] E., Mathisen, "Security challenges and solutions in cloud computing," in Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on, 2011, pp. 208-212.

[19] W. Chen,et al., "A Novel Hardware Assisted Full Virtualization Technique," in Young Computer Scientists, 2008. ICYCS 2008. The 9th International Conference for, 2008, pp. 1292-1297.

[20] S. Farrell, "Portable Storage and Data Loss," Internet Computing, IEEE, vol. 12, no. 3, pp. 90-93, 2008.

[21] R., Trope and C., Ray, "The Real Realities of Cloud Computing: Ethical Issues for Lawyers, Law Firms, and Judges, " [Online], Available at: http://ftp.documation.com/references/ABA10a/PDfs/3_1.pdf , 2009, [Accessed: September 9, 2012].

[22] K. Ramachandran, T. Margoni and M. Perry, "Clarifying Privacy in the Clouds, " in CYBERLAWS 2011 : The Second International Conference on Technical and Legal Aspects of the e-Society, IARIA,2011.

[23] F. Sabahi, "Cloud computing security threats and responses," Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, pp. 245–249, May 2011.

[24] M. Srinivasan, et al.,"State-of-the-art Cloud Computing Security Taxonomies A classification of security challenges in the present cloud computing environment," In: International Conference on Advances in Computing, Communications and Informatics (ICACCI-2012), ICACCI '12, ACM, 2012, CHENNAI, India.

[25] M. Poulymenopoulou, F. Malamateniou, and G. Vassilacopoulos, "E-EPR: a cloud-based architecture of an electronic emergency patient record," In Proceedings of the 4th International Conference on Pervasive Technologies Related to Assistive Environments (PETRA '11). ACM, 2011 , Article 35 , 7 pages

[26] R. Padhy, M. Patra, and S. Satapathy," SLAs in Cloud Systems: The Business Perspective," International Journal of Computer Science and Technology , March 2012, Vol. 3, Issue 1. Page no. 481 488.

[27] K. Mu-Hsing, "A Healthcare Cloud Computing Strategic Planning Model," Computer Science and Convergence, Lecture Notes in Electrical Engineering, 2012, Volume 114, Part 6, pp. 769-775.

[28] CPB UK Ltd," Security Survey Results - Threats Anticipated by Organisations," Business Technology Group (BTG), 2011 [Online] Available at: http://www.btg-uk.com/security-research.html