International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:10, No:1, 2016

Use of Cloud Computing and Smart Devices in Healthcare

Nikunj Agarwal, M. P. Sebastian

Abstract**—**Cloud computing can reduce the start-up expenses of implementing EHR (Electronic Health Records). However, many of the healthcare institutions are yet to implement cloud computing due to the associated privacy and security issues. In this paper, we analyze the challenges and opportunities of implementing cloud computing in healthcare. We also analyze data of over 5000 US hospitals that use Telemedicine applications. This analysis helps to understand the importance of smart phones over the desktop systems in different departments of the healthcare institutions. The wide usage of smartphones and cloud computing allows ubiquitous and affordable access to the health data by authorized persons, including patients and doctors. Cloud computing will prove to be beneficial to a majority of the departments in healthcare. Through this analysis, we attempt to understand the different healthcare departments that may benefit significantly from the implementation of cloud computing.

Keywords**—**Cloud computing, smart devices, healthcare, telemedicine.

I. Introduction

HEALTHCARE at a distance (Telemedicine) relies on the use of telecommunication and information and communication technology (ICT). In the developing countries, the technological evolution is yet to take place in healthcare. There is an increase in the number of old age patients in India; hence, it becomes essential for healthcare institutions to invest more into Telemedicine. Telemedicine helps in saving lives during critical situations through technology. Moreover, the worldwide healthcare services in rural areas still remain as a major challenge [1]. Applications of wireless telemedicine systems include tele-cardiology, tele-radiology, and tele-psychology [2].

Healthcare as compared to any other service operations requires continuous and systematic innovation in order to remain cost effective, efficient and to provide high-quality services. Cloud computing could improve healthcare services and research [3]-[6], [8], [9]. Cloud computing refers to an on-demand, self-service Internet infrastructure that enables the user to access computing resources anytime ubiquitously [10]. It is a model to deliver computing resources as per the requirement and the need of different users. Cloud computing can reduce the EHR startup expense such as hardware, software, networking, personnel, and licensing fees, and hence, encourage the adoption.

Nikunj Agarwal is with Department of Information Technology and Systems, Indian Institute of Management Kozhikode, Kerala India (phone: 91-89-4312-7342; e-mail: nikunj05fpm@iimk.ac.in).

Sebastian M P is with Department of Information Technology and Systems, Indian Institute of Management Kozhikode, Kerala India.(e-mail: sebasmp@iimk.ac.in).

The three cloud service models are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). IaaS deals with the delivery of computing resources such as storage, network, and capacity of processing [11]. PaaS abstracts the infrastructures and supports a set of application program interface to cloud applications [11]. SaaS replaces the applications running on PC onto the cloud-computing environment [11].

Despite the benefits that are offered by cloud computing applications for healthcare, there are several managements, technology, security, and legal issues to be addressed before the implementation of cloud computing in healthcare [12]. Moreover, for increasing the addressability of patient care issues at any point in time, it becomes increasingly essential that the different stakeholders are able to ubiquitously access data over different wireless networks. Kuo reviews the literature and evaluates the opportunities and challenges from the viewpoint of management, technology, security, and legality [12]. In this paper, we critically analyze Kuo's viewpoints.

A. Management Aspect

Cloud computing approach speeds the deployment while maintaining vital flexibility (i.e. rapid elasticity and ubiquitous access to healthcare resources) [12]. This capability suggests that as demand changes, hospitals, and other healthcare providers do not need to adjust their infrastructures to accommodate changes. It is essential to estimate the importance of wireless entities within the hospitals to ensure endurance and ubiquitous access to the data. In addition, it becomes easier for the hospital management to store data as per the requirements of the doctors and moreover, their access to data from the cloud could be managed by the cloud-computing providers.

The major challenges in this context could be lack of trust in data security and privacy by users, organizational inertia, loss of governance, and uncertain provider's compliance [12]. Cultural resistance (or organizational inertia) to share data or change traditional ways of working would be a common management challenge in adopting cloud computing [12]. However, in practice, cloud environment offers more security to customer data than the traditional on premise server based data storage. The European laws set high compliance obligations for companies requiring them to protect the privacy and security of consumers' sensitive data including sensitive data that is stored in a public cloud. The level of data protection mandated for sensitive data under the four statutes in the US is roughly analogous to the data protection for sensitive personal data provided for consumers in the EU [13].

B. Technology Aspect

Smaller hospitals do not have the internal IT staff to maintain and service in-house infrastructure for applications such as EHRs [12]. Eliminating the new infrastructure cost and the IT maintenance burdens could remove many obstacles to EHR adoption [5], [7]. Cloud computing can increase the scalability, flexibility, and cost effectiveness of infrastructure. Some technical challenges related to the use of cloud computing in healthcare include resource exhaustion, unpredictability of performance, data lock-in, data transfer bottlenecks, and bugs in large-scale distributed cloud systems [12]. However, the lock in issues is less with IaaS platforms like Amazon. The infrastructure obsolescence issues are almost nil with SaaS clouds like Salesforce.

C. Security Aspect

The main barrier to the adoption of cloud computing in healthcare relates to data security [14]. The data security risks in the use of IT are hacker attacks, network breaks, natural disasters, public management interface, poor encryption key management, and privilege abuse [12]. However, the current cloud providers are better equipped to provide much better security than the on-premises security [13].

D. Legal Aspect

If the providers adopt better and clearer policies and practices, users would be better able to assess the related risks they face [12]. The use of cloud computing presents many legal issues such as contract law, intellectual property rights, data jurisdiction, and privacy [15]-[19]. Many countries now insist for their financial and health data to be in the servers within the country even if it is on the cloud, as a mandatory requirement. This increases the cost of cloud service.

In this paper, we attempt to understand how the Management aspect of the privacy and data sharing could be addressed. This aspect is one of the most critical among the different aspects. The storage and sharing of medical data in a cloud environment could raise concerns. The concerns are primarily due to the computing storage being managed by a third party service provider [20]. These concerns are due to the lack of trust in the service provider responsible for handling the data. The most critical tenet for utilization of health information across multiple organizations is to enable the flow of medical information so that the privacy of data is not compromised.

There were many security and privacy issues that were reported during the implementation of Health Insurance Portability and Accountability Act (HIPAA) in many organizations [15]. The most common issue encountered during the sharing of data was because of transmission and storage of the data. Three spheres are involved in the privacy protection of the stored data such as user sphere, joint sphere, and recipient sphere [18]. The hospital owns the data and outsources the storage of shared medical records to a third party cloud service provider. The datasets obtained may be published to a medical research center. The hospital serves as the data owner, the medical research center as the data recipient and the cloud service provider's hardware and software resources to supply the shared services encompass the joint sphere [20]. This model is suggested that combines the privacy by cryptography and privacy by statistics for strong guarantee against privacy protection. Privacy by cryptography is to ensure that encrypting of the data that can help to ensure that the unauthorized personnel cannot understand the data. A set of analytical and statistical techniques could be applied to understand the mechanisms to disclose the information.

In order to implement the privacy, the medical data can be vertically partitioned into three parts [20]. In this method of partitioning, it is suggested that the patient identification could be stored as a cipher text and the other parts required for the medical analysis could be stored as a plain text. The data can be retrieved back by merging the different components, checking for the integrity, and verifying the correctness of the data. The information could store in two different tables Ta and Te, and Ta comprising of sensitive patient specific information whereas Te consisting of information that can be used publicly by the scientific institutions for data analysis [20].

In this paper, we analyze the usage of Telemedicine applications that are being used by more than 5000 hospitals in the US. Through this analysis, we aim to understand the departments that are more likely to adopt the usage of Smartphones over Workstation on wheels (WOW). From the analysis, it is understood that currently there are lots of requirements for Wireless entities to access patient-centric data. If cloud computing could be implemented in the hospitals, then there could be a possibility of all the departments which make use of Telemedicine also benefiting from the implementation of cloud computing. We could understand from this analysis the departments that could benefit significantly from cloud computing. We assume that the different stakeholders accessing Telemedicine applications across hospitals would benefit in a major way upon shifting the data onto the cloud.

The research methodology used was secondary data analysis. The secondary data of the hospitals was gathered for over 5000 acute care US hospitals from The Dorenfest Institute for H.I.T. Research and Education Analytics database [21]. The data were analyzed using logistic regression in STATA/SE version 11.1 statistical software (STATA Corp, College Station, Texas).

II. Data Analysis

The α value considered for the study was 0.05. We have considered a p-value of 0.05 or less to indicate statistical significance with 95 percent confidence intervals for evaluating the results. The dependent variables considered for the study were growth of acute care hospitals in different departments such as HR (human resource), Ancillary, Cardiology, ICU (intensive care unit), Emergency, Trauma Care, Surgery, Pathology, Primary Care, Radiology, Urology, Orthopedic, Oncology, Obstetrics, Endocrinology, and ENT (Ear, Nose, and Throat). The dependent and the independent

variables were categorical. The independent variables considered for the study were planning of smart phones, usage of smart phones, usage of wireless local area network (WLAN), usage of WOW, WOW planned usage of tablet personal computer (PC), tablet PC planned, usage of personal digital assistant (PDA), and PDA planned.

TABLE I
LOGISTIC REGRESSION PERFORMED OVER VARIABLES

Departments/ Wireless Entities	Odds ratio	p value	95% confidence interval
HR			
Smart Phones Planned	2.0	<0.01	1.3-3.1
Ancillary			
Smart Phones Planned	2.0	<0.01	1.3-3.1
WLAN	1.0	0.93	0.7-1.5
Cardiology			
Smart Phones Planned	0.1	<0.01	0-0.4
ICU			
Smart Phones Planned	0.2	<0.01	0-0.5
Smart Phone	0.6	0.04	0.3-1.0
Emergency			
Smart Phones Planned	2.2	<0.01	1.4-3.3
Trauma Care			
WOW planned	1.4	0.09	0.9-2.2
Smart Phones Planned	0.1	<0.01	0-0.5
Surgery			
Smart Phones Planned	2.0	<0.01	1.3-3
Pathology			
Smart Phones Planned	2.5	<0.01	1.7-3.7

Table I shows the results of logistic regression computed over different wireless entities. The odds ratio for planning the smart phones for the HR departments is 2.0 with confidence interval of [1.3-3.1]. This suggests that HR department is two times likely to plan the usage of smart phones than use WOW. The ancillary departments are two times more likely to plan the use of smart phones than use WOW. ICU departments are six times more likely to adopt WOW than plan the usage of smart phones. Emergency departments are two times more likely to adopt smart phones over WOW. Trauma care departments are two times more likely to plan more usage of WOW than the current WOW usage in the hospitals. The surgery department is more likely to plan the usage of smart phones over the current usage of WOW. Pathology departments are two times more likely to plan the usage of smart phones over the current usage of WOW.

Table II shows that WOW is more than or equal to two times more likely to be used in Primary Care departments over other entities such as planning the usage of WOW, usage of tablet PC, planning tablet PC, usage of smart phones, usage of PDA. Moreover, primary care departments are two times more likely to adopt intrusion detection over the usage of WOW. Radiology departments are two times more likely to plan WOW and plan the usage of smart phones over the current usage of WOW.

Table III lists the logistic regression coefficients for the usage of WOW in different departments with reference variable being the usage of WOW.

TABLE II
LOGISTIC REGRESSION PERFORMED OVER VARIABLES

Departments/ Wireless Entities	Odds ratio	p value	95% confidence interval
Primary Care			
WOW Planned	0.1	<0.01	0-0.3
Tablet PC	0.5	0.01	0.3-0.8
Tablet PC Planned	0.4	<0.01	0.3-0.8
Smart Phones	0.1	<0.01	0-0.3
PDA	0.6	0.04	0.4-1.0
Intrusion detection	1.5	0.02	1.1-2.0
Radiology			
WOW Planned	1.5	0.03	1.0-2.3
Smart Phones Planned	2.3	<0.01	1.6-3.5
Urology			
WOW planned	0.1	<0.01	0-0.3
Smart Phones Planned	0.1	<0.01	0-0.5
Orthopedic			
WOW planned	0.4	0.01	0.2-0.8
PDA	0.4	<0.01	0.2-0.7
Oncology			
WOW planned	0.1	<0.01	0-0.3

TABLE III
LOGISTIC REGRESSION PERFORMED OVER VARIABLES

Departments/ Wireless Entities	Odds ratio	p value	95% confidence interval
Obstetrics			
Smart Phones Planned	0.2	<0.01	0-0.5
PDA Planned	0.4	0.01	0.2-0.8
Endocrinology			
WOW planned	0.1	<0.01	0-0.4
Smart Phones	0.1	<0.01	0-0.3
ENT			
WOW Planned	0.2	0.03	0.1-0.8
VoIP	0.2	0.01	0.1-0.6
Tablet PC	0.2	0.01	0.1-0.6
Tablet PC Planned	0.2	0.01	0.1-0.6
Smart Phones	0.2	0.01	0.1-0.7
PDA Planned	0.2	0.02	0.1-0.8
PDA	0.2	0.01	0.1-0.6

III. CONCLUSIONS

In this paper, we conduct a literature review to understand the benefits and challenges of implementing cloud computing in healthcare. We also analyzed the data of usage of Telemedicine applications for over 5000 hospitals to study the importance of different wireless entities for different departments, which may access the cloud facility. We could understand that implementation of cloud computing could benefit the healthcare institutions significantly. The departments that would benefit from the implementation of cloud computing include HR, Ancillary, Emergency, Surgery, Pathology, and Radiology. Moreover, cloud can address the implementation of security in Primary Care offices, which is now a major challenge.

IV. DISCUSSIONS

The ancillary departments are more likely to plan for smart phones than WOW. The reason that could be attributed to

planning smart phones may be due to increasing number of patients trying to get access to the medical reports (X-Ray, ECG) over the phone. Many of the current and emerging healthcare application requirements need wireless and mobile infrastructure. These requirements range from high-speed access to wireless networks to location tracking and monitoring abilities [22]. These infrastructures need not be managed by the hospitals with the implementation of cloud computing, as the resources will be managed on-demand by the cloud service provider. Many of the medical errors occur because of the lack of correct and complete information during the diagnosis [23]. The three main factors that improve the design of the Telemedicine systems are reliability, usability, and security [24]. The cloud providers can make the systems more reliable, usable and secure than by the conventional hospitals' IT administrators. Implementation of cloud computing thus can help the Telemedicine systems to address the privacy and security concerns.

The ICU departments are more likely to adopt WOW over Smart phones. This may be due to the fact that there are large numbers of critical cases in the departments that need immediate access to the EHRs of the patients. The ICU departments may need continuous monitoring of the patients and they may need to update the EHRs of patients continuously. WOWs may be more suitable for this setup. The WOWs are also more likely to provide immediate access to the medical records than the Smart phones. The Emergency departments are more likely to adopt smart phones over WOW. The reasons for their adoption may be due to the fact that there may be a large number of non-distanced communications between the nurses and the patients in cases of emergency. In addition, it may be likely that the doctor-on-duty may need to co-ordinate with the senior doctors over the smart phones. The implementation of cloud computing may ensure hassle free data access over the cloud and moreover, ensure that the privacy of the patient data is not compromised, as the authentication requirements are very reliable than in a conventional hospital setup. The Trauma care unit is likely to continue with the WOW usage rather than moving to the smart phones. The surgical departments are more likely to be planning for the smart phones than the WOW because of the need for follow-ups. The doctors can handle the follow-ups more efficiently in a cloud-supported environment. The pathology departments are more likely to plan for smart phones than WOW. This could be due to the fact that these departments require higher co-ordination with other departments in cases of emergency or in cases where the patient needs to undergo a surgery. The primary care departments are more subjected to intrusions as they handle a lot of sensitive data of the patients. The secure data encryption mechanisms in the cloud infrastructure make the intrusions useless. The radiology departments are more likely to plan for both WOW and Smart phones. This could be due to the increase in the number of patients in the hospitals requiring immediate attention in surgical departments.

REFERENCES

[1] T. Suzuki and M. Doi, "LifeMinder: an evidence-based wearable healthcare assistant," in *CHI'01 Extended Abstracts on Human Factors in Computing Systems*, 2001, pp. 127-128.

[2] C. S. Pattichis, E. Kyriacou, S. Voskarides, M. S. Pattichis, R. Istepanian, and C. N. Schizas, "Wireless telemedicine systems: an overview," *Antennas and Propagation Magazine, IEEE, vol.* 44, no. 2, pp. 143-153, 2002.

[3] C. Chatman, "How cloud computing is changing the face of health care information technology," *Journal of Health Care Compliance,* vol. 12, no. 3, 2010, pp. 37–70.

[4] J. T. Dudley, Y. Pouliot, R. Chen, A. A. Morgan, and A. J. Butte, "Translational bioinformatics in the cloud: an affordable alternative," *Genome Med*icine, vol. 2, no. 8, pp. 51, 2010.

[5] E. J. Schweitzer, "Reconciliation of the cloud-computing model with US federal electronic health record regulations," *Journal of American Medical Informatics Association,* vol. 19, no. 2, pp. 161-165, 2011.

[6] J. Haughton, "Year of the underdog: Cloud-based EHRs," *Health Management Technology,* vol. 32, no. 1, pp. 9, 2011.

[7] R. Zhang, and L. Liu "Security models and requirements for healthcare application clouds," Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, pp. 268-275, 2010.

[8] J. Kabachinski, "What's the forecast for cloud computing in healthcare," *Biomedical Instrumentation and Technology,* vol. 45, no. 2, pp. 146–50, 2011.

[9] A. Rosenthal, P. Mork, and M. H. Li, J. Stanford, D. Koester, P. Reynolds, "Cloud computing: a new business paradigm for biomedical information sharing," *Journal of Biomedical Informatics,* vol. 43, no. 2, pp. 342–353, 2010.

[10] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology,* vol. 53, no. 6, pp. 50, 2009.

[11] C. Gong, J. Liu, Q. Zhang, H. Chen, and Z. Gong, "The characteristics of cloud computing," In *Parallel Processing Workshops (ICPPW), 39th International Conference,* pp. 275-279, 2010.

[12] A. M. H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," *Journal of medical Internet research,* vol. *13,* no. 3, pp. e67, 2011.

[13] N. J. King, and V. T. Raja, "Protecting the privacy and security of sensitive customer data in the cloud," Computer Law & Security Review, vol. 28, no.3, pp. 308-319, 2012.

[14] D. Catteddu, and G. Hogben, "An SME perspective on cloud computing. Cloud Computing–SME Survey," *ENISA report,* 2009, Online: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey/at_download/fullReport.

[15] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541-562, 2013.

[16] P. C. Kocher, "The SSL Protocol Version 3.0. Internet Draft," *Netscape Communications Corporation*, USA, 1996.

[17] T. Dierks and C. Allen, "The TSL protocol," Internet Draft, 1997.

[18] S. Spiekermann and L. F. Cranor, "Engineering privacy," *Software Engineering, IEEE Transactions,* vol. 35, no. 1, pp. 67-82, 2009.

[19] Q. Ni, E. Bertino, J. Lobo, C. Brodie, C. M. Karat, J. Karat, and A. Trombeta, "Privacy-aware role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 3, pp. 24, 2010.

[20] J. J. Yang, J. Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," *Future Generation Computer Systems*, vol. 43, pp. 74-86, 2015.

[21] The Dorenfest Institute for H.I.T Research and Education Database, HIMSS Foundation, Chicago, IL, 2011.

[22] U. Varshney, "Pervasive healthcare: applications, challenges and wireless solutions," *Communications of the Association for Information Systems,* vol. 16, no. 1, pp. 3, 2005.

[23] L. T. Kohn, J. M. Corrigan, and M. S. Donaldson, "To err is human: building a safer health system. A report of the Committee on Quality of Health Care in America, Institute of Medicine," *The National Academies Press*, Washington D. C, USA, 2000.

[24] C. J. Fitch, "Information systems in healthcare: mind the gap," *Proceedings of the 37th Annual Hawaii International Conference*, pp. 8, 2004.