IBIMA Publishing
Communications of the IBIMA
http://ibimapublishing.com/articles/CIBIMA/2017/369309/
Vol. 2017 (2017), Article ID 369309, 18 pages
DOI: 10.5171/2017.369309

Research Article

Privacy and Security Issues in the Use of Clouds in e-Health in the Kingdom of Saudi Arabia

Emna Chikhaoui[1], Jawahitha Sarabdeen[2] and Rehana Parveen[3]

[1, 3] College of Law, Prince Sultan University, KSA

[2]Faculty of Business, University of Wollongong, Dubai

Correspondence should be addressed to: Jawahitha Sarabdeen; jawahitha@gmail.com

Received date: 14 April 2016; Accepted date: 30 March 2017; Published date: 30 May 2017

Academic Editor: Essa Saleh AlYounis

Abstract

Cloud computing is one of the most popular current trends in the field of information and communications technology (ICT). This technology allows more efficient computing by centralizing data storage and processing. Due to its tremendous advantages, this technology is maturing rapidly and is being adopted in many sectors including government, business, hospitals, and educational sectors. Information Technology plays a strong role in the health and patient care arenas with cloud computing slowly beginning to make its mark. However, despite the significant advantages for the utilization of cloud computing as part of Healthcare IT (HIT), security, privacy, reliability, integration and data portability are some of the significant challenges and barriers to implementation that are responsible for its slow adoption in the Kingdom of Saudi Arabia. When using the cloud for e-health security and privacy issues are most important, these areas should be addressed before cloud computing could be adopted successfully by all quarters. Patients, healthcare providers and other associated organizations are concerned about the privacy of customers' information and would like to see proper measures to protect privacy. In this paper, the researchers will discuss privacy and security challenges in using cloud computing e-health and available legislations, possible solutions to address challenges related to security and privacy issues in the use of cloud in the Kingdom of Saudi Arabia.

K**eywords:** Cloud computing, e-Health, privacy, security, and legislation.

Cite this Article as: Emna Chikhaoui, Jawahitha Sarabdeen and Rehana Parveen (2017)," Privacy and Security Issues in the Use of Clouds in e-Health in the Kingdom of Saudi Arabia ", Communications of the IBIMA, Vol. 2017 (2017), Article ID 369309, DOI: 10.5171/2017.369309

Introduction

Cloud computing is receiving a great deal of attention. It is a concept used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. In science, cloud computing is a synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time. The phrase also more commonly refers to network based services, which appear to be provided by real server hardware, and are in fact served up by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up (or down) on the fly without affecting the end user - arguably, rather like a cloud [1].

Cloud owners maintain computing facilities, data storage, and software that facilitate the daily routines and procedures of healthcare operations in a flexible and scalable way through effective service-level-agreements (SLAs) i.e., "pay as you use" contracts. Some healthcare providers have found an opportunity to shift the burden of managing and maintaining complex Health information technology to the Cloud or more appropriately to the Cloud service providers. Thus, in addition to removing the operational load off the shoulders of the healthcare providers, it also significantly reduces the operational and maintenance costs. [2].

Cloud Computing also opened a window of opportunity for healthcare providers to share part of their data with other stakeholders such as government agencies, health research institutes, authorized private companies such as insurance companies and other hospitals. Sharing patients' data serves different purposes that contribute to improve the quality of healthcare services. Yet this sharing needs to have strict regulations on who is sharing the data and how well the privacy of the patients is maintained. However, according to Kaletsch et al. [3], when dealing with privacy and sharing information several threats are involved. The top threats include social functions where, although users can choose to be anonymous, they could easily and involuntarily expose their identity or personal information. Another threat is the selling of medical information as some personal information may not be obvious enough to be excluded before the sale. In addition users may not find an explicit list of what was distributed or sold and cannot figure out what information about them was included. Further, there is the threat posed by Web analytics done by third parties who use any data available on the Web for user profiling and targeted advertising. In such case some privacy issues arise as such entities observe and record the users' behaviors and their traffic on the Internet thus violating their privacy. [4]

The role of Cloud Computing is very remarkable and it is one of the emerging technologies in the world of computers. Cloud Computing is a better way to run your, business instead of having your own resource you can use resources as services. Cloud runs on shared data centers virtually, hence the name Cloud Computing. Cloud Computing is used in education entertainment, medical, military operations, business and finance etc. This paper focuses on the role of cloud computing in health sector and its influence over the Kingdom of Saudi Arabia.

The health care environment is changing faster than ever before due to the demand of delivering higher quality medical services for less money, and increased competitively between health care services' providers. Hospitals, research clinics, private health care institutions and doctors are looking for solutions to increase daily activities, efficiency and decrease their spending [5]. Thus, cloud computing provides to the health care environment the opportunity to improve services for patients, to easily share information, to improve operational and maintenance costs. In addition information in the cloud is not as easily lost when compared to the paper documents or hard drives [6].

There are many new technologies emerging at a rapid rate, each with technological advancements and with the potential of making humans' lives easier. However, one must be very careful to understand the security risks and challenges posed in utilizing these technologies. Cloud computing is not an exception. In this paper key security considerations and challenges which are currently faced in the Cloud computing in Saudi Arabia are highlighted. The paper examines legal challenges that cloud computing poses in health sectors with particular attention paid to implications of cloud computing in the Kingdom of Saudi Arabia. It also presents several recommendations for legislative responses in the Kingdom of Saudi Arabia.

Objective of Research

- To explore the opportunities and barriers that cloud computing provides in health.
- To analyse and compare the current privacy and data protection legislation in the Kingdom of Saudi Arabia.
- To identify the security challenges created by the use of cloud computing in health.
- To suggest some measures to mitigate challenges arising from cloud computing.

Methodology

The purpose of this research is to analyze the use of cloud computing in health care and the existing legislations dealing with privacy in the Kingdom of Saudi Arabia. To achieve this objective, the researchers used the following methodology:

1. Content analysis where literature and laws regarding privacy and security concerns were analyzed.

2. Survey is also used. The survey collected data from associates working in health sectors in Saudi Arabia. The survey is used to understand the perceptions in the adoption of cloud computing, its advantages, disadvantages, challenges and concerns relating to trust, privacy, security, cloud models and existing legislations.

Literature Review

Cloud Computing

There is no single, commonly agreed-upon definition of "cloud computing". The United States National Institute of Standards and Technology has defined it as follows [7]:

"Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks ,servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Under this definition, the cloud model promotes availability and is composed of five essential characteristics, three delivery models and four deployment models.

Infrastructure as a Service (IaaS) provides users with processing, storage, networks, and other computing infrastructure resources. The user does not manage or control the infrastructure, but has control over operating systems, applications, and programming frameworks. Some common examples are Amazon, Go Grid, 3 Tera, etc. **Platform as a Service (PaaS)** enables users to deploy applications developed using specified programming languages or frameworks and tools onto the Cloud infrastructure. **Software as a Service (SaaS)** enables users to access applications running on a Cloud infrastructure from various end-user devices (generally through a web browser) [8].

Cloud facilities could be used as private clouds that are operated solely for one organization or **Public clouds** are open to the general public or a large industry group and are owned and managed by a Cloud service provider. It also could be of **Hybrid clouds** combine two or more clouds (private or public) that remain unique entities but are bound together by technology that enables data and application portability. **It could also be a community cloud's** feature infrastructure that is shared by several organizations and supports a specific community [9].

When considering a move to cloud computing, healthcare personnel (medical practices, hospitals, research facilities, etc.) need to carefully consider the type of application moving to the cloud (clinical and nonclinical applications). Clinical applications consist of EHRs, physician order entry and software for imaging and pharmacy use. Nonclinical applications include revenue cycle management, automatic patient billing, cost accounting, payroll management, and claims management.

In many cases, the type of application moving to the cloud will dictate the cloud deployment model that's utilized (private, public, and hybrid), addressing the specific security, privacy and availability requirements for that application. Initially, cloud deployments for clinical applications will take root in private or hybrid clouds given that these applications require the highest level of security, privacy and availability. Nonclinical applications are a better fit for public deployments but still must be carefully assessed. For example, an appointment with the psychiatry department may imply potential mental issues and, as such, must be protected as sensitive data.

Healthcare personnel must also consider the cloud service model (IaaS, PaaS, or SaaS) that best addresses their business requirements. However, these features have led to some security risks to cloud computing. The presence of huge computing resources and humongous amount of data has made cloud environment a lucrative target for hackers. Also, the cloud computing environment has raised various privacy concerns as well because the customers believe that they have lost control on the data which they have stored in the cloud. In the following sections we discuss various issues related to privacy in cloud computing, various laws and regulations, do a risk assessment and then provide a model to compute privacy ranking for a cloud.

Privacy and Security Issues In Cloud Computing

Privacy could be understood as the right of a person to have his personal data properly secured. Any data that could uniquely identify a person or, which is not supposed to be known to any person other than its owner and/or her immediate family, without her consent are called Private Data. It is therefore needed to maintain the confidentiality of private data. However, current cloud services usually cause these data to be exposed, on a machine owned and operated by an organization which is different from the data owner, in unencrypted form. In this section we present a brief overview of privacy, security and trust in the cloud. The most common issues related to privacy in cloud computing environment are [10]:

- Trust
- Uncertainty
- Compliance

A-Lack of user control: Complete control of user on the data is not possible in the cloud, since both the visibility and control of a user is reduced as soon as the cloud environment is used. The key aspects here are, that in cloud computing the personal data of a person are present on machines which are not owned or controlled by him/her, and therefore, there is the threat of the data being stolen, misused or even resold without authorization.

It is also not always possible for a cloud service provider to ensure that a person is able to access all of his personal data, what is the current location of the data, and what is currently being done with the data. It is also difficult to control the exposure of the data since many law enforcement agencies monitor the traffic flowing through their countries. There is also a risk of insecure deletion of data.

A cloud service provider may not guarantee complete and safe removal of data on receiving a deletion request. Provider lock-in is also a concern for any consumer; i.e.it is not easy to change the cloud service provider, as it is extremely difficult to get the data back from the cloud. It is very difficult to know which privacy breaches have already taken place and which are going to happen because of uncertainties regarding notifications. It is also difficult to identify the person at fault for such breaches.

B-Training and Expertise: The deployment and running of cloud services requires high skill jobs, but the unavailability of highly skilled people is a serious issue from the point of view of information security. Employees may also not understand the consequences their decisions could have on privacy. The rise of technology has also worsened the scenario, as more employees are now able to cause such privacy issues which may have far-reaching consequences. Therefore, it is essential to have proper management procedures in place like trainings etc. otherwise there are chances that employees may switch to cloud computing environment without considering the risks and their consequences.

C-Unauthorized Secondary Usage: The risk of unauthorized use of data either stored or processed in the cloud is always present. The authorized secondary usage of any user's data by the service provider to gain revenue is part of standard business model. However, the data could also be used in a way which is unacceptable to the user. Therefore, it is necessary for the cloud service providers and the customers to enter into a legally binding agreement which explicitly mentions as to how and up to what extent the data of a customer could be used. This will also enhance the trust between the customer and the cloud service provider.

D-Complexity of Regulatory Compliance: The global and distributed nature of cloud computing environment and the many laws present in different places around the world has made it very complex and difficult to ensure that all the laws and regulations which are applicable in a given case are complied with. What makes this complex is that in cloud computing environment the same information could be sometimes in different locations at the same time. It is very difficult to know exactly where the data are or if they are in transit at any given time. Another factor which complicates the compliance issue is the presence of multiple copies of the same data in the cloud, and each of these copies may be managed by different entities. The main properties which make compliance difficult are:

- Data Proliferation: Data proliferation refers to the prodigious amount of data, structured and unstructured, that businesses and governments continue to generate at an unprecedented rate and the usability problems that result from attempting to store and manage that data.

  This is the feature of cloud computing in which, to ensure the availability of some data, the cloud providers replicate that data in multiple locations. This happens in such a way that multiple parties may be involved. I t cannot be guaranteed that the data or their copies are not processed or stored in some certain jurisdictions. Deletion of all the copies of data upon receiving such request can also not be guaranteed. Therefore, any cloud computing service which involves both outsourcing and off shoring may raise some very complex and serious issues.

- Dynamic Provisioning: The problems related to outsourcing which cloud computing environment faces are quite similar to that in traditional outsourcing, but the dynamic nature of cloud computing environment makes many of the existing provisions which address these issues in static environment obsolete. It is not yet clear as to which party will be held responsible for ensuring that proper legal requirements of private data are met, or whether or not appropriate data-handling standards and procedure are followed.

E- Transborder Data Flow: Data protection regulations and privacy laws restrict the flow of private data outside the national borders, restricting not only the physical transfer of data but also the remote access to the data. All countries having data protection laws and national legislations have restricted such transfers. Personal information however can be transferred between some countries, if either some model contracts have been signed and approved by country regulator, or if the owner of the data has given his free consent. Model contracts are agreements containing data protection commitments, liability requirements of the company and the liability to the concerned individuals. However, model contracts are not very well suited to the cloud computing environment. The main reasons being: the uncertainty in cloud computing environment and the regulatory complexity, and the factor that this technique is not flexible enough for cloud, as approving model contracts and obtaining regulatory approval may result in long delays. Therefore, it is very difficult to understand which laws will apply when the routes of information flow are not known. Even if transit of information is not considered; enforcing transborder data transfer regulations in the cloud computing environment is still very difficult.

F-Litigation: A government may force a cloud service provider to give them the data stored in the cloud. All they have to do is to show that the requested data are relevant to some case for a subpoena. To avoid similar situations at the hands of some non-governmental entities, the contract between the cloud service provider and the cloud subscriber should include provisions that decide the response of the cloud service provider upon receiving any such subpoena requests.

G-Legal Uncertainty: Legal frameworks have played very important role in the protection of the personal and sensitive information of any user. The basic concepts of such legal frameworks are generally technology neutral, and therefore they would still be applicable on cloud computing envir onment. Still these frameworks need to be updated keeping the current and future technologies in consideration.

The dynamic nature of cloud computing environment combined with various transborder interactions have introduced l egal aspects which must be considered carefully while processing the data. However, there are legal uncertainties regarding the right of privacy in cloud computing environment. Legal frameworks are yet to decide whether encrypting the private data may be considered as proc essing and how to guarantee that the processed data are private data or not. All these challenges have not yet been addressed in any legal frameworks and therefore the uncertainties regarding the legal situations still remain the same [11].

Providers of cloud services should collaborate with each other and with government stakeholders to invest in research to advance the protection of privacy for users through the reinforcement of existing procedures and creation of new architectures and systems. This applies in particular to identity and access management, data encryption, data deletion, and addressing causes of failure and security loopholes [12].

Privacy is considered to be a fundamental human right around the world; this has led to a large amount of legislation in the area of privacy. Nearly all countries' national governments have imposed local privacy legislation. In addition, privacy regulations in emerging technologies are surrounded by uncertainty. This paper aims to clarify the uncertainty relating to privacy regulations with respect to Cloud Computing and to identify the main open issues that need to be addressed in the Kingdom of Saudi Arabia.

Cloud Computing In Health Sectors in the Kingdom Of Saudi Arabia, Opportunities and Challenges

Health services in Saudi Arabia have developed enormously over the last two decades, as evidenced by the availability of health facilities throughout all parts of the vast Kingdom. Saudi Arabia Ministry of Health is the world's single largest healthcare provider. It operates 255 hospitals and 1,200 primary health clinics in the Kingdom, with ambitious growth plans. A further 120 hospitals and 1,000 clinics are currently under construction. Alongside the physical expansion, the Ministry wants to ensure a world-class level of connectivity between locations. To work effectively the primary healthcare clinics, gatekeepers to the Kingdom's health, must be linked to specialist centers. Clinicians want to be able to share patient data, securely and seamlessly, as they deal with 130 million patient visits each year [13].

Health care services in Saudi Arabia have been given a high priority by the government. During the past few decades, health and health services have improved greatly in terms of quantity and quality, as evidenced by the availability of health facilities throughout the Kingdom. The Saudi healthcare sector is structured to provide a basic platform of healthcare services to all, and is primarily managed by the Government through the Ministry of Health (MoH) and a number of semi-government organizations who specifically operate hospitals and medical services for their employees. In addition, the private sector operators are also playing a key role in providing quality healthcare services in the Kingdom.

The Saudi Ministry of Health (MoH) provides over 60% of these services while the other government agencies provide 20% and the private sector the remaining 20%. According to the Saudi Arabian General Investment Authority (SAGIA), in 2005 KSA spent US$ 13 Billion on health care, 25 percent of which was supplied by the public sector. According to the World Health Report (2000) of the World Health Organizations (WHO), the Saudi Health Care System is ranked 26th among 190 countries in terms of overall health system performance, and is well ahead of many advanced countries[14].

As healthcare remains one of the most important sectors in any community, many technologies have emerged and been funded by governments to improve healthcare delivery outcomes in the Kingdom of Saudi Arabia. Numerous factors indicate that the Saudi healthcare sector will continue with its rapid growth in the coming years, the most telling of which is the growing desire among the current population to improve their well being. With surging healthcare demand, strong government support, a robust economy and a thriving ICT community, the Kingdom is right on track to become a regional and global leader in IT healthcare systems development and adoption as well. Healthcare spending in Saudi Arabia is expected to grow by 10.3 percent this year to SR98 billion over 2012's SR88.9 billion.

The Saudi government has announced that major projects involving healthcare, along with other key sectors such as education, will get additional funding and strong governmental focus in the coming months. At the same time, the Kingdom's IT expenditure is projected to increase by around 6.6 percent to SR15.3 billion this year. These parallel developments are expected to open up major opportunities in healthcare-related cloud computing adoption and investments in smart systems, among others [15].

Information and Communications Technology Projects of the Ministry Of Health in the Kingdom Of Saudi Arabia Provides:

Health Information System (HIS) for hospitals: Creating electronic files for patients, providing all MoH hospitals with electronic health systems, connecting all hospital systems, using technologies of cloud computing, improving the Kingdom's capabilities in conducting vital semi-direct surveillance, analyzing necessary information for the management of infectious diseases, statistics monitoring and data representation through early diagnosis, monitoring the arrival of pilgrims and vaccines given to each pilgrim in their country and required medication, using the electronic fingerprints to document information, implementation of a "statistical system" program to examine the workflow in the hospitals of Holy Sites e.g. entering data of reviewers, patients admitted to hospitals and health centers in the regions of Makah and Al Medina during Hajj season and "Umrah", executing the program of statistical systems during Hajj season, processing, analyzing and presenting data to be used in planning and decision making [16].

There are number of technologies in the Kingdom; the most common technologies that are designed to improve healthcare services in the kingdom of Saudi Arabia are MHR (Medical Health Record), PHR (Personal Health Record), and HER... EHR has many definitions, such as the electronic record that stores patient's medical history information in a health record system, accessible and managed by care providers. Despite its positive impact on healthcare services; its adoption progress is slow in most healthcare institutions worldwide; especially in developing countries due to several common challenges. Several studies found that the main barriers for its adoption are: high purchase costs, high maintenance costs, physician's resistance Shortage in skilled IT staff.

Patients in rural areas suffer from travelling to large hospitals carrying their paper health records and crossing the land to reach the specialized physicians and medical care in large hospitals with EHR systems. Moreover, patients registered in independent EHR systems in different hospitals also suffer from transferring their files to other hospitals. Such difficulties can be defeated by integrating EHR systems in healthcare institutions [17].

But EHR integration (the process of patient information sharing among health care providers and exchanging it over the Internet with other healthcare providers) remains a challenge and a serious concern since it is exposed to theft, security violation, and difficulties from transfer from one hospital to another. Cloud computing technology used is a form of cloud computing service software applications that can give information to the public. Mobile devices such as Mobile phones and tablets used as tools to give information and education on global health against all diseases, while for the diagnosis and health complaints or illness will be using the software interactive form of open consultation. Expected health education application in the form of cloud computing services to maturity to think of health care with a touch of paranormal medical quack or not, they not to give in to existing health services. The public will better understand the meaning of health and act more preventive in maintaining personal health, family and surrounding environment on an ongoing basis [18].

Research-based cloud computing services for health information on the discussion still revolve around web services and how users adapt to those services, this is due to the fact that the technology of cloud computing services is still a new technology, there are several things to consider when making a service in cloud computing such as the characteristics of the service, a security system that will be given to the user, and how to improve services to users.

The concept of 'open service' is a process of real-time two-way communication between doctor and patient by using the technology of cloud computing services. The aim of the concept is to enhance the physician's role in serving the society in general, to deliver health information and preventive measures taken by the community, and to keep up the their health and the health of their surroundings.

The cloud service consumer neither manages nor controls the underlying cloud infrastructure including network, virtual machines, operating systems, storage, or even personal application capabilities, with the possible exception of limited user-specific application configuration settings. Recent survey of cloud computing in Saudi Arabia indicates that 70 % of Medical officers reported that they will need and use cloud computing in the near future. In health sectors, many organizations, managers, and experts believe that the cloud computing approach can also improve services and benefit the patient.

Content Analysis Finding: Saudi Laws and Regulations on Privacy Protection

Saudi Arabia up to date has not passed a comprehensive legislation on privacy or data protection per se though it devised a strategic plan for privacy protection. However, there are certain general available laws that can be extended to protect e-health data and education data privacy. "Data" under article 1(4) of the Anti-Cyber Crime Law are defined as information, commands, message, voices or images which are prepared or have been prepared for use in computers. This definition could include saved, processed, transmitted or constructed data. If the private information of a person is processed by computers, then this definition could include private data within the definition. However, there is no available definition of "personal date" given in any existing legislation though one could define it as any information relating to a living and identifiable individual. Similarly privacy is not legally defined but could be interpreted as a right associated with the dignity of an individual. Anti-Cyber Crime Law in articles 3-5 penalizes violation of private data that are transmitted via information networks without consent or authorization. Violation of these provisions will warrant a penalty up to SAR 3,000,000 in fine and a maximum of four years of imprisonment. Thus any personal information including e-health data that are available via cloud will be protected against unauthorized collection, usage or misuses.

The Basic Law of Governance which is the Constitution of Saudi Arabia in article 40 provides protection of privacy. The protection covers privacy of telegraphic, telephonic, postal and other means of communication. It prohibits interception or eavesdropping of private communication except for legal purposes. Similarly the Civil Service regulation in article 12 prohibits the civil servants from disclosing secret or confidential information they acquired while at work. The Constitutional provisions could be applied to protect e-health information of patients in private sector and the public sector employees are bound by the Constitution and Civil Service regulation. These two laws could be easily applied to cover any unlawful use, collection and disclosure of information of e-health patients or educational institutions or the students.

The Telecommunications Act and its Bylaws also could be applied in protection of privacy or data privacy. Article 37(7) prohibits the telecommunication service providers from intercepting data or calls carried on public telecommunication networks. Article 37(13) criminalizes intentional disclosure of information or content that have been intercepted. The bylaws in article 56(1) state that a service provider shall not disclose information other than users' name address and telephone number without prior consent from the users or otherwise required by law. It also requires to take all reasonable steps to ensure the confidentiality of users' communication (article 57 (1)). Article 58 (2) and (3) of the bylaws mandates the operators of telecommunication facilities and networks to respect the privacy of users. The bylaw also states that user information shall not be collected without informing the users about the purpose for which the information is collected. It also prohibits collection, usage, maintenance and disclosure of personal information for undisclosed purposes. Thus, if the telecommunication service providers are also providing cloud services for healthcare facilities or educational service facilities, they are expected by law to adhere to privacy or data protection rules under Telecommunications Act and its Bylaws. Any unauthorized use, disclosure and transmission of information will be punishable by this law. This law imposes a fine not exceeding SAR 5,000,000.

The Electronic Transaction Act also mentions the privacy protection of users of the services of certification service providers. The law in article 1(11) defines "electronic data" as data with electronic features in the form of texts, codes, images, graphics, sounds or any other electronic form, either collective or separate. Article 18(5) requires the certification authority to maintain and ensure that their staff maintains the confidentiality of information obtained in the course of business unless authorized by the certificate holders. This authorization must be either in writing or electronic form. Oral authorization is not considered as authorization under this law. Article 23 (2 - 4) states the following as offence:

1. A certificate holder's use of information concerning the applicant, for purposes other than certification without the applicant's consent in a written or electronic form.
2. A certificate holder's disclosure of information accessed by virtue of his work without the certificate holder's consent in a written or electronic form, or as provided for by law.
3. A certification service provider's provision of false or misleading information to the Commission, or misuse of certification services.

In the event, the e-heath or education cloud service providers or the users obtain certification from a certification authority, any breaches of private information provided in the course of business need to be kept secret by the certification authority unless authorized. Any abuse will warrant a fine up to SAR 5,000,000 fine and a maximum of 5 years of imprisonment or both. In addition, the Healthcare Professions Practices Regulation requires the health practitioner to protect the personal information of patients. This law could be applied even if the service is provided via cloud computing facilities.

The KSA Healthcare Practice Code requires that a health practitioner safeguards the secrets of patients which he comes across while carrying out his profession except inter alia where written approval of the relevant patient is obtained. Violators of such confidentiality requirements can be subject to a fine not exceeding 20,000 Saudi Riyals (approximately US$ 5,333) and other disciplinary penalties such as the suspension of practicing license. Such penalties may be increased based on the severity of the relevant breach or its reoccurrence.

It is to be noted that legislation in the Kingdom provides criminal and civil liabilities for violation of data privacy in general. In claiming civil liability, it must be shown that the damages are actual, direct and tangible but not future profit or loss of goodwill as future profit or loss of goodwill is considered speculative and lacks tangibility.

The government of Saudi Arabia is determined to provide the best health care facilities to its citizens. In this cause, the government spent billions to upgrade the systems including IT infrastructure. The effort resulted in international recognition of the hospitals in the Kingdom. For instance, the King Faisal Specialist Hospital & Research Center ranked in top 5% worldwide for safety, quality of care and efficiency in new global rating by HIMSS Analytics Asia. Similarly, it is concentrated in providing better education provisions. Availability of comprehensive legislation on data privacy will definitely complement the government's effort to have an international recognized heath sector.

Survey Findings

Surveys have been distributed among private and public hospitals to see their familiarity with cloud computing and their concerns about privacy, confidentiality and security. The results of the surveys are shown as follow:

The Kingdom of Saudi Arabia is a leading economy in the Middle East region. The Kingdom has a sound IT infrastructure and is represented by all major IT companies including Microsoft, HP, Hewlett Packard, SAP and Oracle. In other words, the Kingdom's business world is in a position to implement the new models and emerging technologies including Cloud Computing. Saudi Arabia is currently the largest ICT market in the Middle East and expectations for the upcoming years indicate this will continue. To measure the awareness and impact of Cloud Computing and apprehensions which might delay the use of Cloud Computing in Saudi hospitals and universities, this research conducted a survey of private and government hospitals and universities of Saudi Arabia. The survey found that most of the respondents agreed that cloud computing is very effective in health sectors.

Lack of knowledge and weak laws dealing with privacy is the biggest barrier to cloud computing adoption. Most of the respondents said that they "don't know enough about cloud computing to know what the barriers are". Many hospitals' personnel believe that it can improve health care services, benefit health care research and change the face of health sectors. More than half of the respondents indicated that they would be moving to the cloud within two to three years. However, a sizeable minority of respondents also said they had no plans whatsoever to move their IT to the cloud.

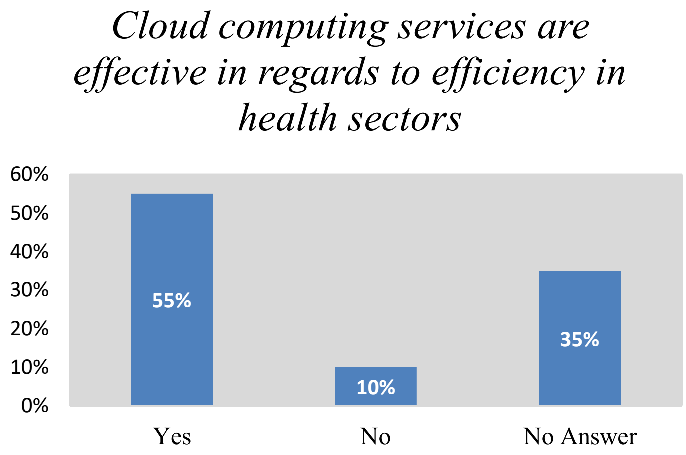

Figure1

Figure 1- is showing the result of the question on cloud computing services where 55% of the respondents agreed that the cloud computing services are effective to improve efficiency in health sectors. 35% of the respondents said no and the rest (10%) respondents did not answer.

Cloud computing is a new way of delivering computing resources and services. Many hospitals' personnel believe that it can improve health care services, benefit health care research and change the face of health sectors.

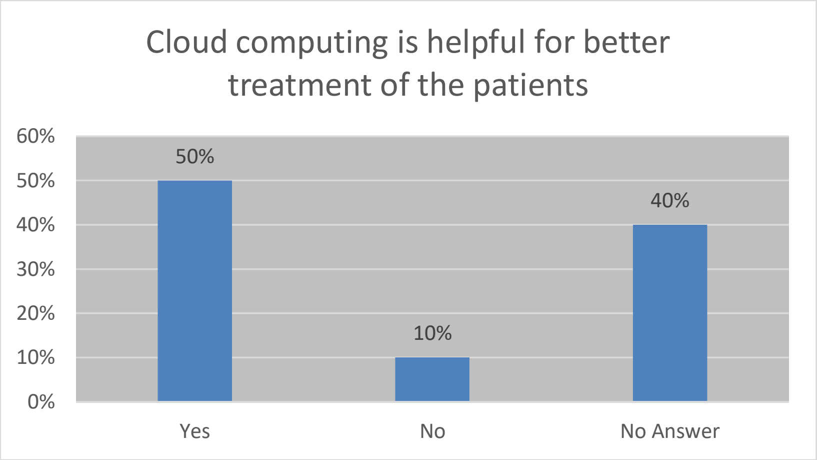

Figure 2

Figure 2- is showing the result of the question on better treatment via cloud. 50% of the respondents agreed that cloud computing is helpful for a better treatment of the patients, 40% of them said no and the rest (10%) did not answer. Most of the respondents were of the view that patients are better advocates for their own health care; they are more educated about their disease and increasingly demand access to the latest technologies. At the same time, they seek the best care at the best cost and are willing to investigate their options. As a result, the demands for accessing personal records are increasing and organizations need to keep up their systems.

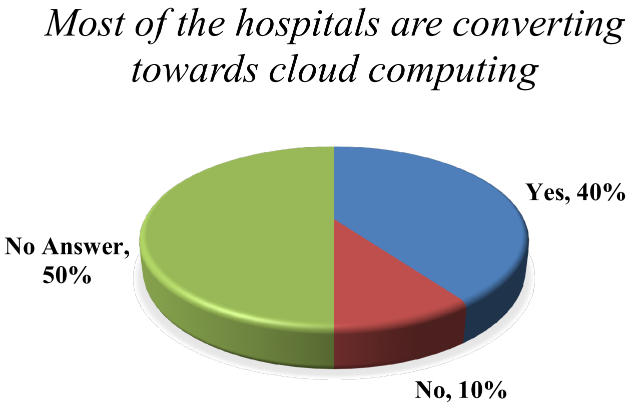

Figure 3

Figure 3- is showing the result of the question on the hospitals that are converting their services towards cloud computing. 55% of the respondents agreed that most of the hospitals are converting towards cloud computing. 10% of them said no and the rest of them did not give an answer. Whereas more and more companies are adopting cloud computing for its convenience and flexibility, the healthcare industry has been slow in adopting this new trend. But gradually many hospitals and clinics are recognizing the benefits of cloud computing and embracing this technology to revolutionize their procedures.

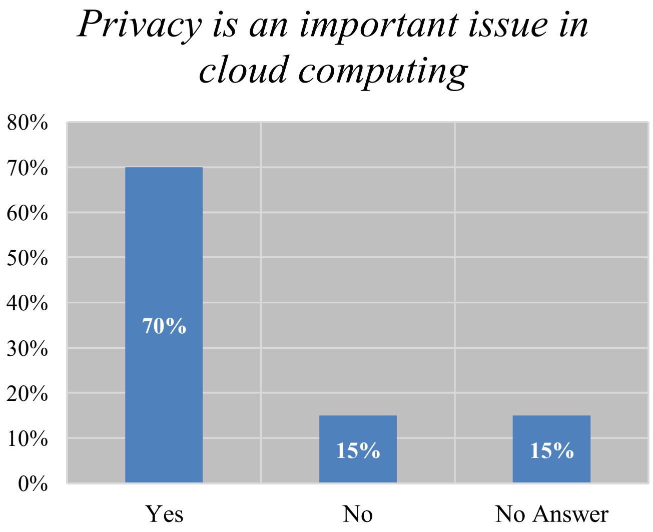

Figure 4

Figure 4- is showing the result of the question on privacy is an important issue in cloud computing. 55% respondents agreed that privacy is an important issue in health sectors, 25% of them said no and the rest (10%) did not answer. Privacy ranks at the top of the list of reasons for slow adoption rate of cloud computing. Putting personal health information into a third party, remote data center raises red flags where patient privacy laws are concerned. The possibility that patient data could be lost misused or fall into the wrong hands affects the adoption of cloud computing in health sectors.

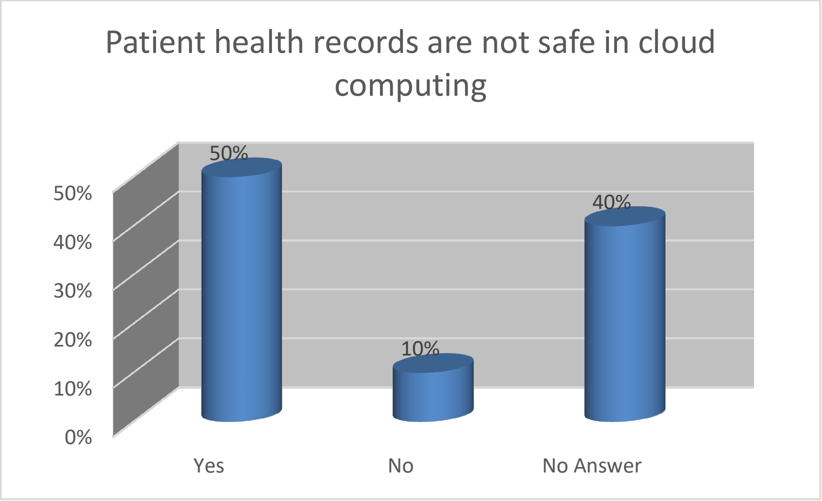

Figure 5

Figure 5- is showing the result of question patients' 50% of the respondents agreed that Patient health records are not safe in cloud computing in health sectors. 40 % of them said that data are safe and the rest (10%) did not answer. Most of the respondents compared the hospital data with bank data and they explained that "it is secured just like your bank account and you do not need to worry about the security".

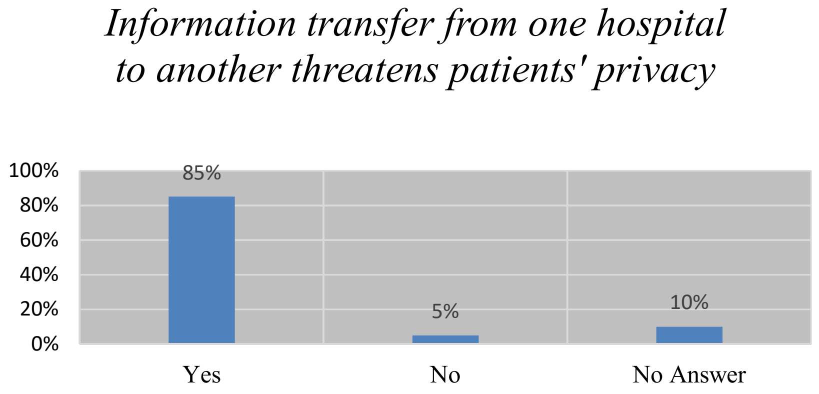

Figure 6

Figure 6- is showing the result of the question on information transfer and privacy. 85% of the respondents agreed that the information transfer from one hospital to another threatens patients' privacy while 5% said no and the rest (10%) did not answer.

Healthcare is a highly regulated industry, and the data used and maintained by healthcare organizations are subject to stringent regulation. Although cloud computing technologies are on the rise in the healthcare industry as with any new technology, their adoption is held back by regulatory hurdles and concerns related to security and confidentiality of patients' information. Putting personal health information into a third party remote data center and other hospitals raises major concerns. The possibility that patient data could be lost, misused or fall into the wrong hands affects patients' privacy.

Conclusion and Recommendations

On the basis of survey findings we observed that this is the right time for the health care community in Saudi Arabia to consider the use of cloud computing as a strategic enabler and tactical vehicle for delivering timely and effective IT-enabled health services for Saudi Arabia. Cloud computing offers the health care system some very attractive economic advantages over traditional computing deployment models, thus the cost avoidance and savings can be redirected to the front lines of care delivery. Cloud computing has the potential to solve many pressing issues in the application of IT in health. It offers opportunities for innovative IT-enabled approaches to improving the health and wellbeing of Saudi Arabians by leveraging distributed health resources in organized ways. The cloud allows providers and more importantly health care delivery organizations with the opportunity to focus less on managing IT and more on delivering care to their patients.

However, one must utilize the appropriate cloud model for the application, ensure the service level agreement with their vendor(s) is appropriate, and the right privacy and security controls are in place.

In recent years, health has enjoyed the uninterrupted development of new information technologies solutions. This has led to several benefits in terms of new hardware infrastructure, new specific and more sophisticated medical applications, increased speed in data processing, etc., that have allowed improving and speeding up the health services. The growth of data produced by the medical and clinical community requires the introduction of advanced techniques and resources in terms of computational and storage capabilities. In order to meet the needs of medical departments, hospitals must continuously improve the level of the modern system by using advanced science and technology innovation.

The new technologies in E-Healthcare are an important part of medical treatment and follow up procedures. The needs in this community range from patient registration, appointment with physician, medical prescription and record of clinical diagnostics, to laboratory tests or surgical procedures that are recorded in Electronic Patient Record (EPR) and specific applications [20].

In the Kingdom of Saudi Arabia, healthcare sectors need to modernize their IT infrastructure, to be able to provide safer, faster and more effective and efficient healthcare delivery which requires massive up gradation of their existing IT infrastructure and involves huge upfront capital expenditure and sizeable operating expenses. Cloud technology is the only technology which mitigates the need to invest in IT infrastructure, by providing access to hardware, computing resources, applications, and services on a ‘per use' model, which dramatically brings down the cost and simplifies the adoption of technology. Several EMR vendors are offering their solutions as a cloud-based offering, providing an alternative approach to help hospitals better manage the otherwise massive capital IT investments that would be needed to support EMR implementations. However, there is an ongoing debate within healthcare as to the viability of cloud-based solutions given the need for patient privacy and sensitive personal information [21].

Taking into consideration cloud computing for health care organizations, the applicable systems must be adaptable to various hospitals’ needs and organizational sizes. Many clinical systems and hospitals deal with processes that are mission critical, and can make the difference between life and death. Cloud computing for healthcare will need to have the highest level of availability and offer the highest level of security and privacy in order to gain acceptance in the health sectors especially in a competitive market place.

Hence there might be a need to create a system of 'Healthcare-specific Cloud' that specifically addresses the security and privacy requirements for healthcare [22]. Early successes of cloud-based physician collaboration solutions such as remote video conference physician visits are being trialed. Extending such offerings to a mobile environment for rural telehealth or disaster response is becoming more real with broader wireless broadband and Smartphone adoption.

Partial solutions will not win over industry resistance. Healthcare-specific Cloud solutions from technology vendors that understand the intricacies of healthcare can build winning solutions. We are convinced that traditional healthcare IT vendors will benefit from aligning and collaborating with each other; such healthcare domain-specific clouds can be created, creating a transformational shift in the healthcare industry [23].

Increased use of e-Health services requires a legal and ethical environment that ensures data privacy, security and confidentiality. While exchanging the medical data or patient health history, there must be respect for human rights and privacy within health personal, health organizations or between countries. The security of health information is a critical responsibility of every health care organization [24].

This is especially important while outsourcing information computing services in a cloud to assure an appropriate level of information security. Actually a specific framework for security management in cloud computing for health care does not exist. A fundamental step for the success of health care into the cloud is the in-depth understanding and the effective enforcement of security and privacy in cloud computing [25]. Despite the potential gains achieved from the cloud computing of e-health services, information security and privacy is still questionable and the security problem becomes more complicated under the cloud model [26].

Although some countries adopted privacy law and tried to have laws in health sector, privacy is still an issue for most of the countries, including Saudi Arabia.

Privacy, security of information and confidentiality are the issues raised in Saudi Arabia as to moving to the cloud in the health sector. Cloud computing paradigm is still relatively young in terms of maturity and adoption. The expectation is that it will undergo several changes in the future, in terms of resources, issues, risks, and ultimately best practices and standards. However, there are some sought advantages that can potentially provide value for institutions of higher education. On-demand services can resonate positively with the current university tight budgets across the nation and other parts of the world. Several benefits of the transition to cloud computing were pointed out in this paper along with concerns regarding the general implementation. The key question remains whether or not it makes sense from a strategic point of view to move to cloud computing and the answer is that it depends on various factors that were mentioned above.

Since Saudi Arabia is not having a comprehensive legislation on data privacy, the researchers recommend EU style of data protection with a view to adopting its provisions to regulate the collection, possession, processing and use of personal data by the data user (individual, organization and government). By providing safeguard to the data, the government could promote confidence among the consumers, patients and the users of both networked and non-networked industries and to accelerate uptake of e-health facilities.

Acknowledgements

This work was undertaken as part of the Microsoft research project on Privacy and Security Issues in the Use of Clouds in E-Health Sectors in the Kingdom of Saudi Arabia. We are grateful to Microsoft for funding this research project. We are thankful to Microsoft for providing access and resource for this project.

References

Wikipedia the free encyclopedia, cloud computing from https://en.wikipedia.org/wiki/Cloud_computing (27 June 2014).

Teng, C.C.; Mitchell, J.; Walker, C. A Medical Image Archive Solution in the Cloud. In Proceedings of the 2010 IEEE International Conference on Software Engineering and Service Sciences (ICSESS), Beijing, China, 16–18 July 2010; pp. 431–434.

Kaletsch, A.; Sunyaev, A. Privacy Engineering: Personal Health Records in Cloud Computing Environments. In Proceedings of the 32nd International Conference on Information Systems (ICIS 2011), Shanghai, China, 4–7 December 2011; pp. 1–11.

Eman AbuKhousa, Nader Mohamed * and Jameela Al-Jaroodi, e-Health Cloud: Opportunities and Challenges, *Future Internet* **2012**, *4*(3), 621-645; doi:10.3390/fi4030621.

Cloud Computing Advantages for the Health Care Industry from http://www.rickscloud.com/5-cloud-computing-advantages-for-the-healthcare-industry/

Buford David, February 2010, Cloud computing A brief introduction LAD Enterprises Inc.p4.

NIST Cloud computing ,version 15 http://csrc.nist.gov/groups/sns/cloud computing

Torry Harris, cloud computing overview , http://www.thbs.com/

http://archivehealthcare.financialexpress.com/201109/itathealthcare04.shtml

http://www.cisco.com/web/IN/about/network/cloud_computing.html

Pearson, S. (2012). Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing, 3-42

Adesh Chandra, March-April 2013 Privacy Issues and Measurement in Cloud Computing:, International Journal of Advanced Research in Computer Science volume 4, No. 4.

http://www3.weforum.org/docs/WEF_IT_AdvancedCloudComputing_Report_2011.pdf,Dated May 22, 2014.

New Strategic Initiatives – Case of the Saudi Health Ministry International Journal of Academic Research in Economics and Management Sciences January 2014, Vol. 3, No. 1

Saudi Gazette 10 march 2014 http://www.saudigazette.com.sa/

Ministry of Health, Saudi Arabia (http://www.moh.gov.sa/), Dr. Padmakumar Ram New Strategic Initiatives – A Case Study of the Saudi Health Ministry, January 2014, Vol. 3, No. 1, International Journal of Academic Research in Economics and Management Sciences,241.

Yang, C. Teng Chen,L., Chou,W and Chieh Wang, K. (2010). Implementation of a Medical Image File Accessing System on Cloud Computing. Computational Science and Engineering (CSE), 2010 IEEE 13th International Conference on 11-13 Dec. 2010 Hong Kong, 321-326.

Abdullah Alshwaier,Ahmad Youssef and Ahmed Eman, Jan 2012,A New Trend for e-learning in KSA using educational clouds.AI Journal of ACIJ vol 3,No 1.

Simon Elliot, June 8 2012,privacy & data security blog published by SNR Denton,.

A Survey of Cloud Computing Architecture and Applications in Health Carmelo Pino and Roberto Di Salvo Department of Electrical, Electronics and Computer Engineering (DIEEI) University of Catania Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)

R. Anand , Dr. S. K. Srivatsa, An Implementation of Health Care Industry through Cloud Computing Technology, International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)p.332-333.

D. Ardagna and B. Pernici, June 2007. “Adaptive service composition in flexible processes,” IEEE Trans. Softw. Eng., vol. 33, no. 6, pp. 369–384.

Vishal Gupta, Adoption of Cloud Computing in Healthcare VP Advanced Services and Leader Healthcare Practice (East), Cisco from http://www.hospitalinfrabiz.com/adoption-of-cloud-computing-in-healthcare.html Retrieved on 28 June 2014.

http://www.hospitalinfrabiz.com/adoption-of-cloud-computing-in-healthcare.html

R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,2009, “Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616.
1 R. Zhang and L. Liu, , July 2010 “Security models and requirements for healthcare application clouds,” inProceedings of the 3rd IEEE International Conference on Cloud Computing (CLOUD '10), pp. 268–275.

M. Almorsy, J. Grundy, and I. Müller, 2010. “An analysis of the cloud computing security problem,” inProceedings of the Asia Pacific Cloud Workshop, Colocated with Asia Pacific Software Engineering Conference (APSEC '10), Sydney, Australia.