What challenges have to be faced when using the cloud for e-health services?

Fei Liu, Eric Rijnboutt, Dimitrios Routsis, Nicolaas Venekamp, Harry Fulgencio, Mohsen Rezai, Adriaan van der Helm
f.liu.2; e.h.j.rijnboutt; d.routsis; n.j.venekamp; h.fulgencio; m.rezai; a.o.j.van.der.helm@umail.leidenuniv.nl
Leiden Institute of Advanced Computer Science, Leiden University, The Netherlands

Abstract—E-health is becoming more important in today’s technological world. Healthcare is increasingly being supported by IT applications such as the emergence of cloud computing. But what are the challenges when using cloud computing in e-health?

Objective - This paper seeks to provide state-of-the-art information with regard to the challenges when implementing e-health applications in the healthcare sector. By doing this, it will be clearer what topics have to be researched further, to be able to successfully adopt cloud computing for e-health.

Methods - We used weighted sampling to select the articles we reviewed. We searched for information on different categories, combined with a few basic keywords.

Results - There are still some important challenges to face when using cloud computing to adopt e-health services. The categories of challenges we looked at are: technical, privacy, legal, organizational, economical and medical. All categories contain aspects that could make it hard to make full use of the e-health services.

Conclusions - To use cloud computing in e-health services is an option, but there will be more work to do to make it fully functional and applicable.

Keywords: Cloud computing, e-health, challenges

I. INTRODUCTION

As the internet-based processing and storage technologies have been rapidly developed, web computing resources have been more promising than ever [1]. A great example of this development is Cloud computing. Cloud computing is a model that enables users to have access to a shared pool of configurable computing resources (network, software, hardware) anytime from anywhere [2], [3], [4]. The distinction between cloud computing and cloud services is that the former is “an emerging IT development, deployment and delivery model, enabling real-time delivery of products, services and solutions over the Internet (i.e., enabling cloud services)” while the latter is “consumer and business products, services and solutions that are delivered and consumed in real-time over the Internet” [5]. From the service point of view, this model includes three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and infrastructure as a Service (IaaS) [2], [3]. It is composed of five essential characteristics (on demand self-service, broad network access, resource pooling, rapid elasticity and measured service) and four deployment models (private, public, community and hybrid cloud) [2]. More and more organizations are moving to the cloud in order to get advantage from the unique opportunities that cloud computing offers. Healthcare organizations could not be the exception to this trend. Cloud computing brings tremendous benefits to healthcare organizations such as high-level patient care, cost reduction, accessibility to the medical data and support to medical research and national security (epidemics) [6], [7], [8]. Although cloud challenges that need to be carefully addressed. These challenges vary from technical and organizational to legal and medical.

Opportunities and challenges of cloud computing in e-health is an interesting topic, it attracts many researchers. Analyzing cloud computing for ubiquitous mobile health using cloud computing [9], [10]; a strategic model for e-health [8]; and challenges and opportunities [6], but these studies did not elicit their respective research method. However, Kuo was able to create a model with four aspects (management, technology, security and legal) to strategically evaluate opportunities and challenges [8], while Abukhousa outlined the technical challenges [6]. However, the four related articles do not ground their findings on rigorous collection and analysis of articles regarding the issues or challenges that they mention in their papers. Nevertheless, few papers have conducted an extensive research on the current state of the challenges that e-health cloud face.

In this research paper, we conducted a study of the challenges of e-health services when adopting cloud computing. We tried to extend the existing model by Kuo [8] and Abukhousa, et al. [6] by analyzing published literatures. The following sections are about methods, results, discussion and conclusion. Under the results section, we defined and separated the main challenges of e-health services into six categories: technical, privacy, legal, organizational, economical and medical. Each category has a brief explanation, which allows the reader to gain insight in understanding their importance. The results of our findings are explained and evaluated in the discussion section, where we also provide implications for future research. Lastly, we concluded our major findings and their significance in the e-health services.

II. METHODS

The methodology we used for our paper on the challenges of using the cloud for e-health services is weighted sampling. Based on the brief related literature we derived some key themes whereby challenges are defined best. Using these themes for keywords ensure a thorough study on multiple disciplines is covered thereby showing the impact of the adoption of cloud computing. Additionally we used the keywords cloud computing, healthcare, e-health and cloud services. We got our articles via search engines, for example Digital Library Leiden University, Scirus.com and medical and technical journals. The
aim is to search for articles from 2008 and more recent that are peer reviewed.

Weighted sampling is a way of doing research in a structured way using keywords. These keywords contribute to results/output of digital libraries. Therefore digital libraries provide a way to look for specific information. Digital Libraries aim to rank documents. Ranking is determined by two basic values: keywords and links. Keyword, the location and frequency of a search term within a result account for one half of the algorithm. This is known as static ranking. The other one is links, the number of links to a page account for the second half of the algorithm - the more often a page is referred to by other pages, the higher it is ranked. This is known as dynamic ranking. Overall ranking is the weighted sum of the static and dynamic rank values. Scirus (Scirus is the most comprehensive scientific research tool on the web with over 575 million scientific items indexed at last count) does not use metatags, as these are subject to ranking-tweaking by users.

III. RESULTS

In the following sections the different categories of challenges, as outlined in section I will be discussed.

A. Technical challenges

1) Service/Data availability: According to eight recent studies, the users of e-health services, such as doctors and patients, demand high availability of the services and data. In other words, medical data and services must be available to users whenever it is required. Nowadays, cloud computing services face several functionality problems caused by network dysfunctions, hardware and software faults, security attacks or natural disasters. Therefore, e-health providers must provide solutions to these problems and ensure that these services will be continuously available with no downtime or performance degradation [6], [11], [12], [13], [14], [15], [16], [17]. Many problems link to the service availability of the cloud which concerns the availability of the data to the users [18].

2) Service/Data reliability: The information systems and the services of e-health in order to be reliable should be error-free as they have great influence on the medical decisions. As the number of cloud providers increases, the number of incorrect data or services becomes bigger. For that reason, e-health services should secure the validity of the data regardless any software, hardware, or network failures [6].

3) Scalability: Scalability is one of the main characteristics of cloud computing. It allows scaling up or down the number and capacity of the IT resources without interrupting users' normal work [3], [6], [8]. For that reason, scalability requires dynamic configuration and automatic reconfiguration [4], [7]. The challenges is to implement a dynamic infrastructure and maintain acceptable performance while scaling up or down.

4) Flexibility: The cloud that e-health services use should be flexible enough to change its services and infrastructures or add new ones, according to the different requirements of healthcare providers. These requirements focus on the quality of the services, operations, auditing and management. In order to cover these requirements with minimum effort and cost, e-health services should be easily configurable [6], [8], [16].

5) Interoperability: Interoperability is the ability of the system to provide servers and data integration among different cloud service providers from both internal and external clouds and the ability for easy migration to different systems. Generally, the design of healthcare systems is based on different data modeling constructs resulting in incompatible systems and databases [7], [19]. Healthcare organizations must integrate their existing systems with the newest web and cloud based systems and designers should focus on designing more interoperable systems. Moreover, they should include mechanisms to ensure secure information exchange and services integration [6], [20], [21].

6) System security: Security is the most critical issue for e-health services due to the sensitive information that it copes with, such as medical records. It deals with access control, audit control, authentication, authorization, transmission security and storage security issues [7]. When data is stored to open environments, security concerns rise for the exposure of private information to unauthorized entities [6]. Recently, many network incidents have happened during data transmission between terminal users and computers, such as Distributed Denial of Service (DDOS) Attacks, Man in the Middle Attacks, Port Scanning, IP Spoofing, and Packet Sniffing [8], [21]. Moreover, it is claimed that in virtualized environments that enable isolation between them, grids don’t deal with end user security [4], [21]. The Information Security Agency [22] recommends that e-health services should deal with the following top security issues: loss of governance, lock-in, isolation failure, compliance risks, management interface compromise, data protection, insecure or incomplete data deletion, and malicious insiders.

7) Data management: The amount of data stored in e-health services is increasing at a high rate as many healthcare organizations use e-health services. In addition, many files are duplicated in order to increase availability and reliability. As a result, the database’s language should provide efficient and scalable facilities for the process and retrieval of the data [6].

8) Maintainability: The challenge of maintainability is to provide clients’ services that will not be affected during any maintenance of the cloud infrastructure, services or platforms. Cloud resources and services must be designed for easy and reliable maintenance and testing models must be developed for the simplification of the process and reduction of the process time needed [6].

B. Privacy

Privacy concerns are a major factor that keeps patients from adopting e-health services [23]. Customers are not convinced on the privacy of their medical records and they want higher privacy levels before moving to the cloud. In order to overcome these issues, there should be separate storage, memory and routing between different tenants of the shared infrastructure. Moreover, there should be a strict access control to data (authorization) [17] and e-health services should use security standards to provide privacy and security of confidential information in a cloud environment [6]. Protecting privacy-sensitive data in the cloud is seen as a controversial topic and there is no exception for this when discussing information management within the e-health sector [23]. This subject is closely related
to security issues and together with privacy issues form the biggest delay in the fast adoption of cloud computing [18]. It is not surprising that companies are spending millions on protecting the data [7], like for example the Electronic Medical Records (EMR), considering the severe consequences. Protecting the data from malicious unauthorized access, misuse or public availability are key factors concerning privacy. Moreover, inconsistencies and loss of data are seen as huge risks that can result in severe consequences [24]. Although counter measures are being developed like standards and performance metrics, an exhaustive counter measure to adhere to federal regulations is not yet available. However, several models have been developed that address the availability and privacy issues. Zhang and Liu for example propose a model that addresses the issues of security, privacy and availability on the basis of security requirements with a focus on the Electronic Healthcare Records (EHR) [25]. Fan et al. propose a model that takes a more generic perspective on these issues as to offer support for a wider range of applications [24]. A challenge that still needs to be overcome is the interoperability between the service platforms considering that sharing privacy sensitive data on a larger scale requires integration of service platforms like e.g. Microsoft Vault [21].

C. Legal

Legal issues can play a vital role in the adoption of cloud computing in the health sector. Health data is confidential information between patients and doctors. By storing this information into the cloud, there will be questions concerning its availability and reliability because it is not clear where this data is stored and who is operating it. Increased use of e-Health services requires a legal and ethical environment that ensures data privacy, security and confidentiality. Privacy laws may differ from country to country but the encompassing goal is to protect the rights of an individual. One of the major barriers is that only authorized medical personnel has access to patient data, which is relevant to their day-to-day work [26]. Yet another problem remains: how can we define who has the right access to data, and how can we differentiate groups with their required rights. Assuring the cloud providers compliance with the privacy and security requirements imposed on healthcare organizations is a significant challenge [27]. The data that is being used in this industry is a great subject to the governments and individuals. There are state laws that establish certain common privacy security safeguards. They also impose discrete requirements which establish a legal standard. But these standards are not always consistent and are not concerned with the respect of the individuals. Every healthcare organization and healthcare provider is required to safeguard Protected Health Information (PHI) by the Health and Insurance Portability and Accountability Act of 1996 (HIPAA) [27] as modified by the HITECH Act and their implementing regulations. These laws establish a broad regulatory framework governing the privacy and security of PHI. The HIPAA Security Rule establishes 22 separate technology-neutral security standards, which include administrative, physical, and technical safeguards for electronic PHI (ePHI). Each of the standards comprises numerous implementation specifications that must be addressed in protecting the covered entities ePHI from reasonably anticipated threats and hazards [28].

D. Organizational

Due to the overall adoption of cloud computing the way we do business has changed. In e-health, service delivery is also dependent on IT. Transformations are necessary from the e-health viewpoint to make the right decisions on an organizational level. Cloud computing is commonly seen as a development on technical level, nevertheless it’s more than only a technical development. Benefits unfold as healthcare adopts cloud computing and as a result challenges on an enterprise scale arise. Hence, organizational change is of great importance to e-health services.

As stated in section I, cloud computing is about having data accessible anywhere at all time. Information technology is ubiquitous in healthcare. However, the needed resources are housed outside of the hospital’s own data center [29]. This way cloud computing tends to bring up a new problem with data ownership. With data ownership the question that comes to mind is who owns the data? [6]. Either dealing with research data or especially Personal Health Records (PHRs), it is sometimes inappropriate to be accessible for everyone. A few years ago the Electronic Patient Record System was introduced in The Netherlands, which caused a lot of discussion on the topic of data ownership. The goal was to design a system where healthcare records of patients, insurers, doctors, and pharmacies are accessible to stakeholders involved and improve the quality of healthcare. What if a data server is physically stored in The United States and the owner is a Dutch hospital, are the US allowed to access this data? The Dutch minister of Healthcare stopped the project as it couldn’t meet privacy standards [30]. Thus, privacy as well as security plays a pivotal role in the discussion of data ownership.

Decision-making has changed along the way, as with new technology come new barriers. Hospitals for example come up with a rationale not to implement the cloud because the cloud is not mature enough for the e-health sector (lack of transparency and lack of trust) and therefore look for other solutions. On the organizational level major decisions has to be made concerning upfront investments, or recurring costs for subscription using for example SaaS. The board of directors simply has to take into consideration factors like integrity, confidentiality, and availability and cloud services should therefore be analyzed with great care [31].

All in all, strategic importance and operational performance are arguments to be considered by a cloud vendor. Key to a proper implementation is governance, an issue concerning the enterprise as a whole.

E. Economical

With the rapid development of the healthcare industry and prosperity of healthcare-related organizations and products, a large amount of data storage is required. The traditional paper-based way and Electronic Health Records systems are limited by their capacity and cost of data storage. Cloud computing offers a pay-as-you-use model which allow providers achieve better resource utilization and enables users to avoid the costs of resource over-provisioning through dynamic scaling [32]. It is true that from the technology side, the implementation of cloud healthcare has clearly cost advantages. However, from the healthcare organization side, these advantages sometimes
may not outweigh the cost of implementing healthcare solutions. Some economical challenges in the adoption of cloud computing in the healthcare industry should not be ignored.

1) Administration expense of IT department: By implementing greenfield applications, the cloud-based solution in this case, healthcare organizations may operate more cost effectively. But by the addition of these applications, there will be new additional expenses. Buyers and administrators of IT departments who take charge of supporting healthcare delivery need to think about the transfer expenses carefully once they decide to adopt the cloud-based technology. Although cloud technology may be ready to be adopted and cloud services can be allocated to organizations respective units directly, the capital costs and other expenditures will become an expense item against the IT departments operating budget. Therefore, some reluctance may exist in the cloud healthcare implementation. This requires administrators to be aware of the possibility of purchasing cloud-based outright as applications instead of developing own infrastructure. It should be determined by each organization situation to choose whether to purchase from a public cloud, to be a community cloud implementation member, or build a private/hybrid cloud platform by itself. When purchasing a public cloud, administrators should take into account that a more integrated commercial platform can help to reduce implementation costs [33].

2) High adoption expense in rural areas and small clinics: In rural and underprivileged areas, healthcare organizations have no money to implement the technology and there is no infrastructure and associated education provided for them to use this technology properly. The same story happens to physician’s practices and small clinics, where most doctors work, which don’t have the capital to afford in-house cloud infrastructure by themselves even though they know a cloud based solution is cost-effective. To face this challenge requires government efforts to spur adoption of cloud deployments (especially SaaS-based deployments) and promote the awareness of health information among citizens [34].

3) Latency: Latency remains a formidable challenge as the immutable physical law of light speed. In the network field, there are demands for nearly instantaneous execution of machine-to-machine stock trades, which has led financial services companies to locate their data centers as physically close to stock exchanges as possible. The read/write speed limit of magnetic disks can only drop so far, but increased speed often goes along with decreased capacity: big disks are slow, and fast disks are small. Under the consideration of performance, convenience and security in many applications, computing is still dictated to be local. Saving customer data in data centers which are away from customers may reduce electricity costs, but the costs of latency are often outweighed by those savings [29].

F. Medical

Using IT systems to improve workflows is nothing new. Special attention should always be paid to the actual core process that is being influenced. In the case of e-health, this is the medical care. A lot of articles outline improvements that can be made on for example the quality and costs of healthcare. Nevertheless, there are also some challenges when trying to improve the medical care. One topic that is often discussed is trust. It is obvious that people want to get the best when talking about healthcare. The use of IT within healthcare often brings up some privacy and trust issues. That is why most users are reluctant to use IT, especially cloud computing, as part of the healthcare [35]. The use of computerized provider order entry (CPOE) systems is also an addition to healthcare systems using e-health. These systems are used to order medication for a patient, and communicate orders between different healthcare providers [36]. While overall impacts of using these systems are positive, there are some aspects to mention that are less positive. Using these CPOE systems takes for example more time from healthcare providers, because they need to fill in the data in an electronic system [37]. Another problem mentioned is that some providers may get excluded from processes because they’re not using the same system, or are not using any CPOE at all. This problem can also be linked to the interoperability problem mentioned in section III-A5. The impact on healthcare is the reduction of speed, which wouldn’t be expected when automating processes.

Healthcare could also be improved by the use of computerized decision support systems (CDSSs). These are systems designed to support practitioners in making clinical decisions [38]. While results have shown that the use of these systems can actually improve the process of decision making, it is also discussed that these systems need to fulfill four requirements to actually improve the process [39]. These are: automatic support for clinical processes, functional at any moment without any delay, recommendations can be incorporated in the workflow, and usage of the computer to generate support. When not incorporating one of these things, the system could fail in improving the workflow, and thus the medical care. A possible problem could be the reluctance of practitioners to accept a recommendation from a computer, when their own decision would be different.

As shown, systems that are already being used like CPOEs and CDSSs bring some challenges, because people have to get used to working with them. They will also have to accept the shortcomings of these systems, for example the extra time needed to use them.

IV. Discussion

In this literature review, recommendations from over thirty sources were analyzed and e-health implementation challenges are defined in six dimensions: technical, privacy, legal, organizational, economical and medical. Even though literature on e-health and cloud computing is widely available, research efforts and outputs for each of the subtopics are not equally distributed. The majority of the reviewed articles focus on the technical, privacy and legal challenges, while few refer to the organizational, economical and medical challenges.

With regard to standards and regulations, the use of cloud computing for e-health services hasn’t been discussed that well. While some studies mention the need to comply to the HIPAA for example [6], [7], and companies like Google and Microsoft have been introducing open source personal healthcare information platforms [33], the lack of standards is still pointed out as one of the main challenges when implementing cloud services [6]. The current medical standards, for example
ICD-10 [34] or SNOMED [6], aren’t adjusted to be used in cloud services. There is also a project initiated to look at the variety of security issues arising when using cloud services within healthcare, but it’s more used as a guideline than as a standard [25]. Of course there are standards regarding cloud computing, for example as mentioned by Ertaul [21], but those are outside the scope of this paper, as they are not focused on e-health applications.

There were also few researchers who propose solutions to the challenges listed above. This has to do with the healthcare industry still being in its early stage of cloud adoption. Therefore, further research on this topic must be done in order to fill in this gap and enhance a more comprehensive overview of the challenges and the corresponding solutions. In addition, when we analyze challenges, we should not ignore the trends in the industry. According to Moore’s law and Wright’s Law (which approximate the pace of technological progress), it is possible that new technology will be available which may be even better than cloud-based solutions. Can the privacy and security problems be solved with the improvement of related laws and standards? Is it possible that new problems will occur in the near future, taking into account the industry environment helps us to better analyze the explicit and potential challenges? Furthermore, the content in some of the dimensions is somewhat overlapping. For example, there are close relationships between technical issues and privacy issues which indicate their mutual dependence. Environmental parts were not mentioned in these papers. Thus, a more detailed, systematic and integrated way of analyzing these challenges is proposed for future study.

V. CONCLUSION

The literature review presents the reader with a comprehensive overview of the challenges for adopting cloud computing within the e-health sector. There are still a lot of problems that need to be considered when transitioning towards introducing the cloud, which were discussed in six different categories. The implications on security and privacy deemed paramount to the success and adoption of cloud computing as it is the cornerstone for the integrity of the data. Moreover, resolving the challenges in realizing interoperability between the different healthcare systems is a critical success factor as it enables one of the envisaged benefits for communication of information between different healthcare institutions. This new way of organizing information imposes a new organizational approach to storing, retrieving, using and communicating information which is why transitioning to the cloud cannot be seen as from a mere technical perspective, but also from an organizational and a medical perspective considering the approach to information will be different. Lastly the design of standards and the compliance to regulations are significant to the success of moving to the cloud.

ACKNOWLEDGEMENTS

We would like to acknowledge Dr. Hans Le Fever, program director of M. Sc. ICT in Business and the LIACS Department of Leiden University for funding the presentation of this paper.

REFERENCES


