Factors Limiting the Adoption of Cloud Computing in Teleradiology

Opeoluwa Ore Akinsanya, Maria Papadaki, Lingfen Sun
School of Computing
University of Plymouth, UK

Abstract

Cloud-based medical data sharing continues to change the way healthcare is conducted in hospitals. It is significantly supporting the 'patient-centricity' trend in providing medical services, and provides clinical team-based care delivery, clinical research, and point-of-care access to demographic and medical information, regardless of the location of the patient and the medical practitioners. Despite these benefits of cloud-based medical data sharing, the adoption in healthcare seems rather limited mainly due to security concerns. The significant contribution of this paper focuses on the identification and comparison of technical security and organizational factors that aids limited adoption of Cloud in teleradiology. Data was collected from relevant healthcare practitioners through interview conducted over the telephone and supported by a form of open-ended questions. The analysis revealed that against popular opinion, organizational factors such as Economics and Adoption Costs, Cultural Resistance, and Legal Rules, were major limiting factors. Future research will focus on proposing a cloud medical data sharing maturity model, which would support healthcare organizations to benchmark, assess and eventually improve the related services.

1. Introduction

Secure exchange of Protected Health-related Information (PHI) including medical images and reports has been an indispensable part of quality medical care and radiology practice in particular. Cloud-based medical data sharing supports secondary use of data and data analytics in various specialties including Radiology, Pharmacology, Nano medicine, and Genetics. Likewise, it provides comprehensive access to PCs, networks, smartphones and network-enabled medical devices [1]. Secure access of diverse specialties to patient data across multiple Electronic Health Records (EHRs) would rapidly streamline, prioritize, and analyze complex patient data.

Cloud-based medical data sharing can also make EHRs and other clinical information systems affordable for smaller healthcare providers that were previously uneconomical to support. For example, Scotland NHS Grampian hosts EHR computing services for the highly dispersed island populations of NHS Shetland and NHS Orkney. This support the provision of locum physicians, remote clinics and emergency air response, and the cost of scaling up capacity is lower for cloud-based systems compared to traditional health IT business models.

Correspondingly, the major reasons for sharing medical images have been to establish a longitudinal imaging record for the patient and provide historical examinations usually to compare with a current examination. Resulting to massive increase in quantity of medical images produced as the patient grows older, which is a big challenge for hospitals as they have to store, manage, share and process these images while reducing patient care costs. In addition, the lack of ubiquitous platform and increasing movement of patients between doctors, hospitals, and geographic locations are also major challenges associated with sharing radiology images [2]. The growth in medical imaging technologies such as 3D imaging, Positron Emission Tomography and Magnetic Resonance (PET/MR) scan has also resulted in tremendous increase in memory size required to store images [2]. As a result, image sharing media has evolved from the use of analogue films, Compact Discs (CDs), Picture Archiving and Communication System (PACS), to Cloud Computing. The last medium of image sharing has encountered organizational-related challenges for which this research is part of solutions being developed.

Cloud-based medical messaging platform adopted by East Kent NHS Trust provided its clinical staff with the ability to access medical records and other data on their mobile devices and web browsers. It collects clinical workflows and information, sends about 600 handovers and 1000 messages each week, and enables medical staff to communicate and discuss patient needs leading to a more effective care provision [3]. Inclusive introduction of integrated Care (INCA) project based on cloud, supports integrated healthcare by creating access to better integrated network of socio-sanitary care e-services outside of hospitals, reducing unnecessary hospital admission and enabling effective working of medical professionals across provider boundaries in Spain, Croatia, Cyprus and Latvia.

In France, a single patient-centric, cloud-enabled portal solution launched more than ten years ago has experienced tremendous growth and already enables more than 1,500 biology labs, 130 hospitals and 15,000 primary care physicians to share information between them and with patients. The physicians can access their lab results using their mobile devices. More than 14 million reports have been distributed via this portal, of which 5 million were targeted at patients.

Despite the many benefits of cloud-based medical data sharing, it also has several technical and organizational drawbacks. These include service reliability, disaster recovery, integration and interoperability, data portability, costs, organizational culture, re-imbursement and insurance, end users' assessments and trust, standards, and data privacy legislation.

This paper aims to present the results obtained from an interview on technical and organizational factors limiting the adoption of cloud-based sharing in healthcare.

The remainder of the paper is organized as follows; Section 2 expounds on the research methodology, whereas section 3 presents highlights of the main interview findings. Section 4 expands on the interview findings with relevant discussions supported by literature, the latter sections 5 presents the conclusion, and future research.

2. Methodology

This research used purposive theoretical sampling to select participants according to criteria specified by the researcher and based on initial findings. Early analysis of data reflected issues that needed exploration; hence the sampling process was guided by the on-going theory development. Data collection and analysis involved constant comparison between results and new findings in order to guide further data collections. For these reasons the development and identification of variables did not take place prior to data collection instead as part of the data collection process. Consequently, the variables were initiated by the participants and further developed and hypothesized by the researcher. Data was collected until no new or relevant data emerges regarding a category and relationships between categories were established [4].

Unstructured interviews by means of telephone calls were chosen, with the aim to identify participant's emotions, feelings, and opinions regarding the particular research subject. Open-ended questions were asked to allow the participants create opinions for responding, offering flexibility in terms of the interactions during the interview, thereby facilitating the generation of conclusions that were not initially meant to be derived regarding a research subject. With this, was an increased risk of the interview deviating from the specified research aims and objectives. This was curbed by the use of semi-structured questionnaire as an interview guide towards the satisfaction of research objectives [5]. In order to ensure the validity and reliability of the study, it was designed and conducted within five months, providing adequate time for sending questionnaires to participants and reducing the risk of history and maturation from very old related projects. Also, the questionnaire was piloted before been applied to guard against the threat of instrumentation. Regarding the demographics of the participants, in the absence of a selection bias, the analysis did obtain a well-balanced demographic set. As it is for every study, this study had its limitations, the study sample was very small - a bigger sample would probably enhance the reliability of the research, and in some cases, participants may have spoken from a point of bias. Despite the limited number of participants, they had vast experience ranging from IT manager, specialist with over 30 years' experience in the installation of clinical systems in large healthcare organization and maintenance of health information systems, researcher involved in a healthcare data sharing project, staff at an organization that provided healthcare data sharing solution to healthcare organizations, professor at radiological sciences department, top researcher at a healthcare imaging informatics group, and a participant had several years of experience in healthcare information sharing and lead in a national healthcare record sharing project. Interviews provided appropriate structure to obtain results as seen in the next section.

3. Interview Findings

The research question that informed this study:

'*Technical security contrasted with Organizational culture: which is the major reason for the limited adoption of cloud teleradiology?*'

Participants specified a number of challenges they encountered. The specified challenges fit under these major categories: (a) static access control solutions, (b) anonymizing images and transmission media, (c) security solutions interrupting clinical workflow, (d) technical security-related limitations to adoption, and (e) management-related limitations to adoption. Hence, this section is primarily concerned with these categories.

3.1. Static Access Control Solutions

Most of the participants considered the access control solutions presently adopted to be unfit for the dynamic environment of healthcare. The widely-adopted access control solution was the role-based mechanism despite the variation in authentication it was still considered a great challenge especially with the medical practitioners. The authentication method such as username/password was also stated to have been abused by medical practitioners as they either use the word ‘password’ as password, or other weak passwords when allocated usernames. In other cases, where only alphanumeric passwords were accepted the medical practitioners had their passwords written on post-it notes and stuck to their desktops. Hence, the adoption of a new single sign-on authentication mechanism using a smart card and reader attached to their desktop computers, but there is the issue of resisting change – the hospitals organizational executives still felt they needed username and password to be secured.

However, the greater challenge remains the role-based access control; unlike administrative staff at the hospital, medical practitioners can be transferred between departments, wards or units weekly or monthly. So, presently there are questions on how do the medical practitioners have enough access rights to do their jobs effectively, but also apply the principle of least privilege.

Apart from the challenge previously stated, another related challenge stated is that most of the implemented access control solutions in teleradiology are considered to be at their basic levels and could be improved in regard to duration of access granted especially in multiple sharing collaboration healthcare environments. In another view, most problems related to access control solutions were not totally with the technology but the deployments of the technology, as most hospitals believe the solutions to be one-size-fits-all “plug and play” solutions.

3.2. Anonymizing Images and Transmission Media

It was stated that due to the frequent occurrence of hacking attack on patients’ privacy and electronic health records, the hospital is very careful about how they deal with patients’ data between transmission media and outside sites. A measure implemented to deal with this is that the transmitting media must be fully encrypted by a specific encryption technology required by the hospital in accordance to government standards for healthcare. In clinical research, it is a standard rule to anonymize patients’ images before been transmitted to the students, however for hospital use, anonymizing the patients’ images before transmission reveals the implemented system is very weak. However, more efforts are placed on securing the transmission media by encrypting the line between the hospital and the cloud provider’s data center.

Previously, transmitting healthcare data especially images between Picture Archiving and Communication Systems (PACS) was a challenge because of the compatibility issues between the systems but with the introduction of DICOM protocol, this has served as a middleware for transmission and standard for imaging systems. In the same view, to enhance swift transmission of healthcare images between the cloud and hospital where there is limited network, wireless area network (WAN) accelerator devices are placed at the transmission line to optimize the bandwidth on WAN, compress the images into zip files, and transmit them faster. This does not in any way affect the quality of the images transmitted.

3.3. Security Solutions Interrupting Clinical Workflow

Based on experiences, the ideal computer system to a medical practitioner entails a doctor walking into his office, expects the computer to automatically recognize him and logs him on to the patient’s record he wants access to, without been authenticated. The recent employment of a tap-on/tap-off (single sign-in authentication mechanism) using a smart card and a card reader attached to the computer system, ensures the dynamic movements of the doctor between wards and computer systems – this solution is context-sensitive.

Similarly stated, in use is a policy that ensures automatic logout once the computer system is inactive for a period of time - most times 10/15 minutes. This may be an inconvenience to doctors but they accept that level of inconvenience knowing that security is a big concern, but this does not interrupt clinical workflow. To avoid this, the doctor could temporarily lock the computer system rather than been logged out automatically. This ensures when the doctor is not around, no one gets inappropriate access to the computer system and patients’ data. In addition, if the doctor logs on to another computer system, the doctor get a notification that they have been/are logged on to another system as a form of audit trail.

In contrast, implementing fingerprints as a security solution which involves the removal of medical hand gloves to have the doctor’s fingerprints read is a big problem and especially in an emergency department. One of the major reasons for the slow adoption of teleradiology technology is because the solutions are not engineered to fit the appropriate workflow. Overall, the challenge is not from the technical point of view with the computer systems but from the deployment and implementation of access control mechanisms. This needs to be improved, not only on the part of the IT professionals and hospitals but also on the part of the doctors. The solution has to be realistic, contextual, protects what needs to be protected, and address the weak links in the chain.

3.4. Technical Security Related Limitations

There are some few factors, technical security is one of them and mostly the first reason people give but it is not the most important as stated by NO. Technical security is a concern but not a barrier. Most of the cloud providers are regarded as technical cloud architects (TA1) providing all the required technical security and access control mechanisms attached to their data centers. Hence, the technical security limitations are not principally of integrity and privacy as about disaster recovery, maintaining continuity of healthcare service in a busy 24/7 hospital. Other technical challenges include the use of earlier/older teleradiology applications which are not cloud computing compatible. Next is the need to assure the hospital management executives on and ensure the un-interrupted availability of data when data is transferred to the cloud.

Another challenge is related to the performance of teleradiology - latency, there is the need for fast performance of web solutions and reduced waiting time for images to load. Cloud computing is actually not presently as secured as private networks but that is not the problem, there is the problem of ensuring the security of the records' database but with the use of service level agreement of the cloud provider it is not a major issue. Presently, there are too many vendors and solutions which create questions related to availability - like how do the solutions deliver data? Is it in a very quick manner? Is it implemented at an urban or remote area? How do you overcome delayed data transmission (latency) over the network? Also, where is the data stored? Vendor-lock in is not an issue because most vendors acts as middleware in addition to the use of DICOM-compliant systems.

Furthermore, as against the generalization that centralised national database for healthcare data are less secured and face more security risk than regional-based databases, from experience it is been shown that security risk is actually less when using centralised database for healthcare data than when using regional database. This is because the centralised database is usually TA1 type of data center with full resilient backup for disaster recovery, and the access into the data center is incredibly well controlled, and also considered more cost effective.

3.5. Management Related Limitations

All participants agreed and stated organizational challenges are mostly responsible for the limited use of cloud teleradiology the major barriers are organizational cultural resistance, legal regulations, economics, and cost. Healthcare management executives are constantly looking for cost reduction, so IT professionals have to balance associated risks with cost involved. Another major factor in adoption is economics; lots of economic factors drive decisions in healthcare management, for instance, funding from country, state, county or (non-) government agencies for the overhead cost of implementing the system. This also applies to international efforts, so several other factors apart from security will majorly determine the decision of a hospital's adoption. Mainly, the healthcare organizational executives are looking for ways to cut cost yet improve clinical care.

Furthermore, once the hospital adopts cloud there will be reduced need for the IT professionals who look after the internal hardware systems, also radiologists will be affected by the disruptive technology. In a bid by healthcare organizational executives to cut cost, a radiologist can be replaced by another at a different location wherever the accreditation applies. Hence, there will be staff members resisting the adoption within the hospital resulting in organizational culture resistance. Also included was the challenge of differentiating between patients' images to be kept in storage for long term and those to be kept for short term. There is also the trade-off between using big vendors better equipped to meet the requirements and the smaller vendors that are cheaper. Hence, questions on how do the providers implement the paradigm to the standard the hospital requires? How do the providers work around complying with the hospital policies? Also, it should not be costly that the hospital can no longer afford to adopt the paradigm into their systems.

Overall, the participants stated that healthcare organizational executives are not barriers they only need to be educated and completely understand the requirements, challenges, and what needs to be done to adopt the paradigm. To implement the paradigm the budget to be allocated depends on what the challenges are, their criticalities, their impact, and how much it's going to cost. But most times, more budgets will be allocated to organizational challenges because security is just a small part as management touches on a lot of different things; workflow and implementation.

4. Discussions

In electronic healthcare systems, access control must be based strictly on controlled permissions that are available through roles just-in-time, only to proper users and until they accomplish specific tasks. It is therefore necessary to have this support in a flexible and effective manner. It can be inferred that there are quite some limitations on the role-based access control model(s) adopted for healthcare. However, as earlier stated despite all these limitations the deployment of the solution at the hospital is another factor to be considered. The first step towards the task of defining and implementing an access control model is the development of an access control policy, as it constitutes an essential basis for a secure system. It is the framework that expresses the need for selecting and implementing countermeasures within a system [6].

An access control policy must specify what are the rules and procedures to follow in order to provide access to confidential information. If this access control policy is properly modelled by a generic but adaptive model, it is easier to find the exceptions or unique characteristics and model them also, according to the specificities of the system. Another important aim is to make the end users of the system intervene as part of its development and implementation. This is extremely important in the healthcare environment where much resistance to change and novelty is usually found.

In another regard, the cloud must conform to the workflow of the hospital or the workflow must be modified that the cloud does not hinder it. In order to achieve these conditions, healthcare administrators are challenged to reach an optimum level of security while negotiating the trade-offs associated with the expense, acceptance, and usability of potential solutions which must respond to the unique requirements of the hospital. User authentication mechanisms for data access controls and audit are vital to any comprehensive security solution. There is a range of possible technical solutions for authentication; these solutions vary in terms of their cost, complexity, and assurance levels. The challenge of identifying an optimum solution lies in the fact that there are a multitude of forces acting on the design decisions and ultimately the adoption of authentication mechanisms [7].

In addition, addressing workflow in data access security is a very difficult problem with many socio-technical complications. While there has been advancement in the development of data access technologies, when the technologies are placed in context they rarely work as intended or difficult to integrate into the system. In a healthcare environment there is a need to balance information security without impeding the quality, timeliness, and effectiveness of healthcare delivery.

With any authentication mechanism, there is an inherent trade-off between security strength and usability [8]. Mechanisms that are easy to use frequently relinquish some security strength, just as those mechanisms that offer stronger security often prove more cumbersome to use. Mechanisms that provide usability and strength come with greater financial costs. While there are many security approaches available, the authentication method of choice for now for most industries, is the traditional username/password pair. The username/password method for authentication has the advantage of being both simple and economical.

However, problems arise when users have to manage a large number of unique username/password combinations as they navigate all of the applications required for the job. There is an increasing push toward stronger, more abstract passwords. However, these are difficult to remember causing users to be reluctant to change them or they write them down thus subverting the mechanism and causing a security breach.

Currently single sign-on (SSO) technologies have emerged as an effective means of addressing these authentication challenges. SSO provides practitioners the ability to log in to the network once and then be able to navigate the countless number of applications seamlessly without the need to enter authentication credentials for each application. SSO promises to improve usability of authentication for users of multiple-systems, increase compliance, and help curb system maintenance costs. However, difficulties emerge in trying to fit authentication that is individually oriented into a hospital that is collaborative in nature.

SSO authentication approaches improve security by increasing user compliance through more usable software, for collaborative technologies to be effective, technology must be flexible and be able to adjust to the situation. Though, improving the overall usability of authentication solutions and the effectiveness of the technology itself is not enough; the context within which the technology is used will greatly affect its usefulness. This is considered one of the reasons for the limited adoption of the technology as it is said not to be engineered to fit within the healthcare context.

Moreover, medical practitioners require high availability of the cloud services, service and data availability is crucial for practitioners who cannot effectively operate unless their applications and patients' data are available. They are expected to be available and reliable without interruptions or performance degradation. Cloud services could experience failures due to software and hardware faults, network faults, security attacks, and natural disasters among many others, as these resources are distributed over the Internet, they will not offer better availability compared to owning and maintaining IT infrastructures within the premises of the hospital. However, hardware and software installations, upgrades, and reconfigurations could be managed such that they are done without any service interruptions for the hospital.

In addition, quality is an issue that can affect successful development and implementation. The quality both actual and perceived, of data entered into systems and then utilized for health care is critical not only for ensuring systems are utilized but more importantly, for the safety and well-being of patients. All important decisions regarding single human or society health are taken depending on the data provided. Hence, the patients' data stored in the cloud must be consistent and constantly in a valid state regardless of any software, hardware, or network failures. While the cloud services must be error-free, they must also be easily configurable to meet with different needs within minimum effort and cost [2].

On the same track is interoperability, which involves defining an agreed-upon framework or open protocols that allow easy servers and data integration among different cloud service providers or cloud types, including secure information exchange and services' integration [9]. An approach is to use the Service-Oriented Architecture (SOA); it provides interoperability between the cloud components and users, by making services easily accessible through standardized models and protocols without bothering about the underlying infrastructures, development models, or implementation details [10].

Furthermore, it is of great importance to ensure the cloud provider cannot access or use the hospitals' database/data. This relates to the need for efficient security mechanisms, with the wide range of security requirements among healthcare providers, the hospital's security requirements and policies must be fully reflected in cloud services. This service should not lead to high computation and involve high communication costs rendering them incompetent in the cloud [11]. In addition, the cloud should be very flexible in adding new needed services to support healthcare processes. While cloud services must be flexible to meet different healthcare requirements, they also must be easily configurable to meet with different needs. In other words, the configuration of cloud services to meet different requirements must be achieved with minimum effort and cost.

In relation is slow performance due to low bandwidth resulting in image latency. Remote rendering does not always provide sufficient display latency for all medical imaging applications when the server must be accessed over the internet, neither does high bandwidth network in a remote data center overcome the limitations of relatively low bandwidth and shared communication links. Delay in accessing medical images stored in the cloud may cause dangers to patient's life, especially during surgery.

The organizational factors include lack of trust in data security and privacy by users (practitioners and executives), organizational culture resistance, legal regulations, cost reduction and economics. Beyond the general belief that trust in data security and privacy by users is at the heart of the resistance that healthcare managers have to the cloud, economics and cost have been discovered to be at the heart of the resistance. One advantage achieved from the adoption of cloud computing technology is to reduce operating costs and increase the relative operational benefits for a given hospital. However, the adoption of cloud computing technology is usually a large project and a huge undertaking for hospitals. The given hospital or group of hospitals has to have sufficient budget, adequate human resource support, ample time, and good executive manager's involvement, then the adopting of cloud computing technology will be met in a positive manner. To this end, it can be seen these resources are highly critical to the success of adoption.

Another major factor is the financial investment required to develop, implement and maintain e-health, and lack of financial support and high initial costs were identified as barriers to adopting cloud computing in healthcare [2]. Inasmuch as hospitals are built to provide healthcare services they are also commercial organizations. In most cases when cloud telemedicine is adopted stakeholders bear the overhead costs while the patients enjoy the benefits. Aspects that require attention include how to manage shared resources, production capacity, marginal costs and the use of salaries and charges as proxies for opportunity costs. Also, organizational executives may be unconvinced about such expansions, particularly when they are satisfied with current methods of working, wish to maintain the status quo, and may perceive such as diverting financial resources away from under-resourced clinical care. The diversion of funds allocated for local developments was cited as a major reason for the limited progress with implementing the strategy.

In addition, healthcare providers require good performance of the cloud services. Service performance is critical to healthcare providers; they cannot operate effectively except their applications and patients' data are readily available when required. Having high performance services can be costly. A trade-off between acceptable performance level and service cost is required [12]. Hospitals have culture, policies, procedures, workflows, medical processes and documentation however transferring to cloud technology would change the traditional ways of sharing data and affect employees. Resulting in resistance and is a common management challenge to adopting cloud computing. It is necessary for a plan to implement smooth transition to the new technology.

The use of cloud computing in healthcare results to many legal issues such as contract law, intellectual property rights, data jurisdiction, and privacy [13]. Among them, data jurisdiction is a major concern. Physical storages for the cloud are typically widely distributed across multiple jurisdictions, each of which may have different laws regarding data security, privacy, usage, and intellectual property. For instance, privacy acts such as HIPAA can be applied on data only within the USA, while the Personal Information Protection and Electronic Documents Act (PIPEDA) operates within Canada, while the cloud provider could (without notice to the hospital) move part of the hospital's information to another jurisdiction resulting in patients' data having more than one legal location at the same time, with contradictory legal consequences [7].

Furthermore, there are still no adequate legislations and guidelines for clinical, technical and business practices of healthcare in the cloud paradigm, and this includes the lack of standards for medical informatics, policies, interoperability, and transmission methods. As a result, more technical, social and ethical concerns will arise. Currently, there are some standards and classifications for general health information systems some of which can be adopted for the e-Health Cloud. Examples are the International Classification of Diseases tenth revision (ICD-10), and Systematized Nomenclature of Medicine (SNOMED) [14, 15]. The e-Health Cloud adopted some of these defined standards and classifications to enable better data sharing among several healthcare organizations.

Compared with the patients and executive organizational staff, practitioners may accept technology decisions differently. Predominantly, practitioners are not technology literate in spite of their general competence and learning capacity. Having experienced highly demanding educational and specialized training, practitioners are experts in their own profession and accustomed to practice in a particular way or style similar to that in which they were trained. From prior studies, practitioners are usually unenthusiastic about the implementation of information systems that interferes with their traditional routines; therefore seldom give positive responses about the system [9]. In addition, practitioners usually practice with relatively high autonomy.

Individual and collective outlooks towards the perceived value of IT systems may lead to a more general resistance to using these systems. Resistance to the development of systems by practitioners and executive organizational staff can create further problems after systems are implemented and the limited use of health informatics applications has meant that their potential has not always been realized. This emphasizes the need not only to involve practitioners in the development of systems and in the interpretation of results, but also to provide sufficient explanation and information at the point of care for practitioners to trust the systems [16].

5. Conclusion

The findings strongly suggested that organizational challenges are the most significant barrier in the adoption of cloud-based data sharing. As such, further research will focus on developing a maturity model, which will help organizations to assess and improve their methods and processes and eventually improve the maturity of their services.

6. References

[1] Lounis, A., (2014) Security in cloud computing. Universit´e de Technologie de Compiegne.

[2] Mendelson, D.S., Erickson, B.J., Choy, G., (2014). Image sharing: evolving solutions in the age of interoperability. J Am Coll Radiol 11:1260–9. https://doi.org/10.1016/j.jacr.2014.09.013.

[3] Moore-Colyer, R., (2016) Cloud, big data and AI lead NHS digital transformation. https://www.v3.co.uk/v3-uk/feature/2459001/cloud-big-data-and-ai-lead-nhs-digital-transformation. Accessed 15 May 2018.

[4] Creswell, J.W., Habib, L., (2009). Third Edition Research Design Qualitative, Quantitative, and Mixed Methods Approaches Library of Congress Cataloqinq-in-Publicaticn Data. SAGE PublicationsSage UK: London, England, London

[5] Langkos, S., (2014). Chapter 3 - Research Methodology: Data collection method and Research tools. University of Derby.

[6] Ferraiolo DF, Kuhn DR, Chandramouli R (2001) Proposed NIST Standard for Role-Based Access Control. ACM Trans Inf Syst Secur 4:224–274

[7] Mehraeen, E., Ghazisaeedi, M., Farzi, J., Mirshekari, S., (2016) Security Challenges in Healthcare Cloud Computing: A Systematic Review. Glob J Health Sci 9:157. https://doi.org/10.5539/gjhs.v9n3p157.

[8] Malina, L., Hajny, J., Fujdiak, R., Hosek, J., (2016). On perspective of security and privacy-preserving solutions in the internet of things. Comput Networks 102:83–95. https://doi.org/10.1016/J.COMNET.2016.03.011

[9] Dünnebeil, S., Sunyaev, A., Blohm, I., et al., (2012). Determinants of physicians' technology acceptance for e-health in ambulatory care. Int J Med Inform 81:746–760. https://doi.org/10.1016/j.ijmedinf.2012.02.002.

[10] Abu Khousa E., Mohamed, N., Al-Jaroodi, J., (2012) e-Health Cloud: Opportunities and Challenges. Futur Internet 4:621–645. https://doi.org/10.3390/fi4030621.

[11] Yang, C-T., Shih, W-C., Chen, L-T., et al., (2014). Accessing medical image file with co-

allocation HDFS in cloud. Futur Gener Comput Syst. https://doi.org/http://dx.doi.org/10.1016/j.future.2014.08.008

[12] Lian J-W., Yen D.C., Wang, Y-T., (2014) An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. Int J Inf Manage 34:28–36. https://doi.org/10.1016/J.IJINFOMGT.2013.09.004

[13] Griebel L., Prokosch H-U., Köpcke F., et al., (2015). A scoping review of cloud computing in healthcare. BMC Med Inform Decis Mak 15:17. https://doi.org/10.1186/s12911-015-0145-7

[14] Hanna R.P., Ruth S., Pohjonene, (2010) Cross-border teleradiology - Experience from two international teleradiology projects. Elsevier 73:20–25. https://doi.org/10.1016/j.ejrad.2009.10.016

[15] NHS, (2011) The UK Edition of SNOMED CT as the Fundamental Standard for Clinical Terminology within the NHS in England Requirement and Draft for a Fundamental Information Standard

[16] Gaylin D.S., Moiduddin, A., Mohamoud, S., et al., (2011) Public attitudes about health information technology, and its relationship to health care quality, costs, and privacy. Health Serv Res 46:920–38.https://doi.org/10.1111/j.1475-6773.2010.01233.x