Security and privacy issues and requirements for healthcare cloud computing

Goce Gavrilov
University American College Skopje

Vladimir Trajkovik
Ss. Cyril and Methodius University in Skopje

Security and Privacy Issues and Requirements for Healthcare Cloud Computing

Goce Gavrilov[1], Vladimir Trajkovik[2]

[1]Health Insurance Fund of Macedonia, Macedonia bb, Skopje, Macedonia
gavrilovgoce@yahoo.com

[2]Faculty of computer science and Engineering, “Ss. Cyril and Methodius” University, Rugjer Boskovikj 16, Skopje, Macedonia
trvlado@finki.ukim.mk

Abstract. Information technology is increasingly used in healthcare with the goal to improve and enhance medical services and to reduce costs. One of the areas with greatest needs having available information at the right moment and with high accuracy is healthcare. With the widespread use of electronic health record (EHR), building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community. Cloud computing paradigm is one of the popular health IT infrastructure for facilitating EHR sharing and EHR integration. Healthcare clouds offer new possibilities, such as easy and ubiquitous access to medical data, and opportunities for new business models. However, they also bear new risks and raise challenges with respect to security and privacy aspects. Ensuring the security and privacy is a major factor in the cloud computing environment.

In this paper, we will present current state of the art research in this field. We focused of several shortcomings of current healthcare solutions and standards, particularly for platform security, privacy aspect and requirements which is a crucial aspect for the overall security of healthcare IT systems.

Keywords: cloud computing, electronic health record (EHR), privacy, security

1 Introduction

Using of information technology in the healthcare (healthcare IT) has become increasingly important in many countries in the recent years. There are continuing efforts on national and international standardization for interoperability and data exchange. Cloud computing aims to incorporate the evolutionary development of many existing computing approaches and technologies such as distributed services, applications, information and infrastructure consisting of pools of computers, networks, information and storage resources [17]. It is still an evolving paradigm but has shown tremendous potential to enhance collaboration, agility, scale, and availability although its definitions, issues, underlying technologies, risks, and values need to be refined. Cloud computing has been defined by the US National Institute of Standards and Technology (NIST) defines cloud as follows:

"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. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployment models." [14].

In traditional IT environments, clients connect to multiple servers located on company premises. Clients need to connect to each of the servers separately. In Cloud Computing clients connect to the Cloud. The Cloud contains all of the applications and infrastructure and appears as a single entity. Cloud Computing allows for dynamically reconfigurable resources to cater for changes in demand for load, allowing a more efficient use of the resources. Virtualization in Cloud Computing allows distributing computing power to cater for load fluctuations. Standard web protocols provide access to Cloud Computing and control is centrally managed in various data centers.

In the healthcare field, cloud computing offers great potential for quick access to healthcare information. IT infrastructure in the healthcare is very complex and for this reason United States Congress has taken additional measures to protect the patient's private data under HIPAA (Health Insurance Portability and Accountability Act). Cloud computing can help patients to gain access to their medical data from anywhere in the world via the Internet. The healthcare domain needs increased security and privacy levels. In order to achieve this requirements cloud computing technology has to be more carefully managed. The matter is less technical and more ethical and legal. On the international basis the ISO (Technical Committee 215) [24] and the Health Level 7 consortium (HL7) [25] define standards for e-health infrastructures.

In this paper, we will present current state of the art research in this field. We present an overview of the security and privacy issues in the healthcare cloud and requirements for implementation of cloud computing in healthcare. The paper is organized as follows: In Section 2, we present an overview of abstract model of healthcare cloud. Section 3, gives some aspect of the security and privacy issues in the healthcare cloud. Also, in this section we present the requirements for building a healthcare cloud. In section 4, we give a systematic overview of the threats in the privacy and security sensitive context of healthcare clouds. Section 5 discusses cloud computing as a solution supporting healthcare information systems, and Section 6 concludes the suggested solution.

2 Model of the Healthcare Cloud: Overview

By NIST, cloud computing model consists of five characteristics, three delivery models, and four deployment models [3]. The five key characteristics of cloud computing are: location-independent resource pooling, on-demand self-service, rapid elasticity, broad network access, and measured service [26]. The author of the [3], [5] and [14] describe each of these characteristics and models. These five characteristics represent the first layer in the cloud environment architecture (see figure 1).

According to the different types of services offered, cloud computing can be considered to consist of three layers: IaaS- Infrastructure as a Service is the lowest layer that provides basic infrastructure support service, PaaS – the Platform as a Service layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications and SaaS - Software as a Service is the topmost layer which features a complete application offered as service on demand [5].

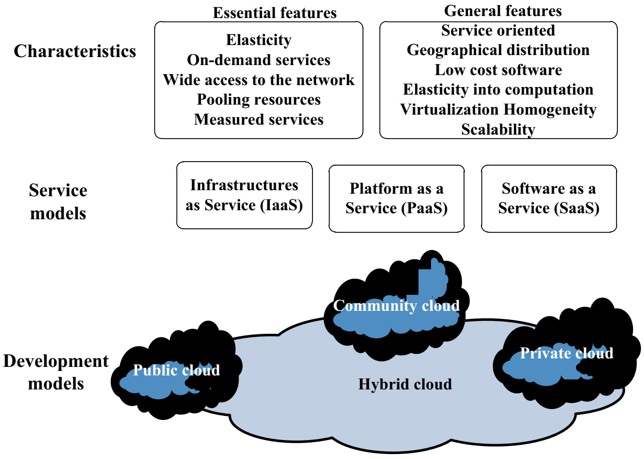

Fig. 1. Element and characteristics of the cloud

IaaS model provides the capability for consumers to provision processing, storage, networks, and other fundamental computing resources, in which consumer is able to deploy and run arbitrary software, including operating systems and applications. IaaS refers to the sharing of hardware resources for executing services, typically using Virtualization technology. With IaaS approach, potentially multiple users use available resources. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components. In the IaaS cloud model, the healthcare application developers hold full responsibility for protecting patients' security and privacy.

PaaS offers an integrated set of software that provides everything that a software developer needs to build an application- an online environment for quick development of web applications using browser-based development tools. PaaS model aims to protect data, which is especially important in case of storage as a service. The data needs to be encrypted when hosted on a platform for security reasons. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. In this type of cloud service model, two levels of protection for security and privacy are required.

SaaS– business applications hosted and delivered as a service via the web. These kinds of applications do not require installation of additional computer programs, the most popular being the e-mail in a web browser. This layer provides capability for consumers to use the provider's applications running on a cloud infrastructure. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities. In this type of cloud service model, the security and privacy protection is provided as an integral part of the SaaS to the healthcare consumers.

Cloud computing is offered in four different forms: Private clouds– are owned by a single organization and are being used only in that organization; Community clouds – belonging to several organizations and allowing access only to those concerned for certain actions; Public clouds – are held by a company selling cloud services to the general public; Hybrid clouds – a composition of two or more types of clouds (private, public or community) that remain unique entities but are linked by standard technologies that enable portability of applications [3], [17].

Zhang and Liu [5] define the concept of Personal Health Record (PHR), Electronic Health Record (EHR), and Electronic Medical Record (EMR) in the healthcare cloud computing. The terms of EHRs and EMRs are used alternately in both: healthcare industry and the press or health science literature. Both EMRs and EHRs are critical to the grand vision of healthcare digitization for improving safety, quality and efficiency of patient care and reducing healthcare delivery costs [5]. Furthermore in this paper we use the following terms:

- Health professional: person who delivers health care services, e.g., physician, dentist, pharmacists, etc.
- Health care provider: organization that provides services of health professionals, e.g., doctor's practice or hospital.

The terms of EHRs and EMRs are used alternately in both: healthcare industry and the press or health science literature. Both EMRs and EHRs are critical to the grand vision of healthcare digitization for improving safety, quality and efficiency of patient care and reducing healthcare delivery costs.

- EMR is the legal record of what happened to the patient during their encounter at a Care Delivery Organization (CDO) across inpatient and outpatient environments and is owned by the CDO. EMR is created, used and maintained by healthcare practitioners to document, monitor, and manage health care delivery within a CDO.
- EHR- database of medical data objects and health-related data managed by health professionals. EHR is a subset of EMR record maintained by each CDO and is created and owned by the patient.
- Personal Health Record (PHR): database of medical data objects and health-related data managed by a patient.

It is very important to ensure the availability of medical data to all the locations a patient is present in. Several examples and developments are already available in literature and presented in the following.

In [1], a model is presented as an integrated EMR sharing medical data between medical units. The application is developed on a cloud platform that keeps the EMR system on the form of SaaS and can be used by Government, Hospitals, Doctors, Patients, Pharmacies and Health Insurance Organizations, through the Internet. This system allows access to national data sharing; the data center is common to all units. Communication between the data center and the healthcare organizations is done via HL7 messages. All patient data are stored and accessed in the same location over the Internet from any healthcare organizations.

In the paper [2], [4] are presented two examples of using cloud computing in Indian healthcare based on SaaS types of cloud computing. First presents the architecture and implementation of cloud computing system in India healthcare system and discusses its strengths and weaknesses. The author of the [7], [12] presents the utilization of telemedicine and wireless sensor network and devices in the cloud computing environment.

Hans at all in [9] discuss the general problems of e-health systems and provide a technical solution for the protection of privacy-sensitive data, which has not been appropriately addressed yet for end-user systems (simple model of e-health cloud and advanced e-health cloud Infrastructure). They describe an abstract model of e-health clouds, which comprehends the common entities of healthcare infrastructures.

3 Problems of Healthcare Clouds

In this section, we give an overview of the threats in the privacy context and security aspect of e-healthcare clouds. The processing of healthcare data of patients has technical, but also legal problems that one has to deal with them. It seems unlikely that any technical means could completely prevent cloud providers from abusing customer data in all cases, so we need a combination of technical and nontechnical means to achieve this. We focus a little on the technical aspects but more on the legal aspects.

Löhr at all [9] have developed the concept of technical aspect of the privacy context and security aspect in the e-health cloud computing. The key segments that affect the technical aspects of security and privacy in healthcare clouds are: data storage and processing (data centers where store data, client platforms and mobile storage devices), management of e-health Infrastructure (cryptographic key management, management of certificates and hardware/software component), usability and user experience. Most of these problems can be overcome by the providers of cloud computing services, maintenances of the e-healthcare infrastructure and users themselves.

The legal aspects refer to the privacy legislation and regulations in the countries where use cloud computing. Policies on the creation of privacy legislation in the European Union (EU) and the United States (US) are differing. Privacy in the US is dispersed among various different sector specific laws and these sectors include the health care sector for the HIPAA. The EU has a different approach concerning legislation. The EU approach to legislation favors participation among businesses and governments as opposed to the US self-regulation approach. The EU set the privacy regulations up to the front as opposed to relying on industry self-regulation.

Research on the various security issues surrounding healthcare information systems has been developed over the last few years. ISO/TS 18308 standard gives the definitions of security and privacy issue for EHR. The Working Group 4 of International Medical Informatics Association (IMIA) was set up to investigate the issues of data protection and security within the healthcare environment. Its work to date has mainly concentrated on security in EHR networked systems and common security solutions for communicating patient data [5]. Choice of the International Classification of Diseases, 10th revision (ICD-10) and ICD-10-CM, for the standard of codification in the EMR system are very important in the healthcare information system [1]. For the data exchange between the entities involved in the healthcare cloud computing, it is necessary to use of HL7 standard which is widely being adopted by health care institutions in several nation-wide. Countries that wish to allow use of cloud computing in healthcare information systems, in their laws, have to provide appropriate provisions to include the previously mentioned standards and some new that relate to the security and privacy of data.

4 Healthcare Cloud Privacy and Security Concept

Security and privacy in the healthcare cloud computing are more than just user privileges and password enforcement. Cloud computing platforms are multi domain environments in which each domain can use different security, privacy, policies and procedures, and trust requirements and potentially employ various mechanisms, interfaces, and semantics, secure data-backup strategy, third-party certification. Such domains could represent individually enabled services or other infrastructural or application components. In healthcare cloud, security should be the top priority from day one. In healthcare cloud applications, some of the security and privacy issue and requirements are orthogonal to the concrete cloud service model or cloud deployment model used. In this section, we briefly present these issue and requirements. Security in Cloud Computing consists of established security solutions such as encryption, access management, firewalls and intrusion detection. In internal Clouds computing the IT department has the ability to install all available security solutions it sees fit but in external Cloud Computing the security depends on the Cloud Service Provider (CSP). Some CSPs do not provide flexibility in the choice of security solutions, while others allow the implementation of client security requirements.

The emergence of cloud computing is a recent development. The security issues in Cloud Computing [14] are organized into several general categories: trust, architecture, identity management, software isolation, data protection, and availability. Cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the security issues involved can be viewed as known problems cast in a new setting. Jansen [14] describes all of the security issue in detail. Security of the cloud infrastructure relies on trusted computing and cryptography.

Some countries in the world [9], like Austria, the German electronic Health Card (eHC) system under development, or the Taiwan Electronic Medical Record Template (TMT), took some activities of the e-healthcare security. In Germany each insured person will get a smartcard that not only contains administrative information (name, health insurance company), but also can be used to access and store medical data like electronic prescriptions, emergency information like blood group, medication history, and electronic health records. The smartcard contains cryptographic keys and functions to identify the patient and to encrypt sensitive data. Recalling the definition of EHR, PHR, EMR, securing issue from the previous paragraph and the possibilities of the eHC, we can define the minimum requirements for cloud computing security concept.

The concept of Cloud Computing brings many uncertainties with respect to compliance with privacy regulations. There are no clear answers on which privacy regulation requirements apply to Cloud Computing. CSPs must assure their customers and provide a high degree of transparency into their operations and privacy assurance. Privacy-protection mechanisms must be embedded in all security solutions. In a related issue, it's becoming important to know who created a piece of data, who modified it and how, and so on. Ensuring privacy and security of health information, including information in EHR, PHR and EMR is a key component to building the trust required to realize the potential benefits of health information exchange in cloud computing. CSPs must provide some Service Level Agreements (SLA) issues and requirements if it wants to offer services of cloud computing.

The migration into a cloud computing environment is in many ways an exercise in risk management. The risks must be carefully balanced against the available safeguards and expected benefits, with the understanding that accountability for security remains with the organization. Both qualitative and quantitative factors apply in an analysis. Too many controls can be inefficient and ineffective, if the benefits outweigh the costs and associated risks. An appropriate balance between the strength of controls and the relative risk associated with particular programs and operations must be ensured.

5 Cloud Computing as a Solution Supporting Healthcare Information System

In the healthcare field, cloud computing offers great potential for quick access to medical information and healthcare information. Healthcare IT infrastructure is very complex and for this reason organization has taken additional measures to protect the patient's private data. Cloud computing can support different healthcare information systems by sharing information stored in diverse locations. All the medical data (EMR, EHR, PHR) are stored in a private cloud and all the participants in the healthcare can access medical patient data when is needed according to their privileges of access. In this case, the medical act is performed quickly, and the typing errors reduced, all of this driving to higher quality. This is one of example of using cloud computing in healthcare.

The authors of [2], [4] give description of some examples of using cloud computer technology in the Indian healthcare sector. In the healthcare area exist many examples of using cloud computing technology, some of them related of using wireless network technology [7] and so-called "Health ATM" [12] based on Google CSPs. All of these examples use some type of cloud computing model or hybrid of them.

The huge benefit of using cloud computing in healthcare, is the possibility of all stakeholder can find data from anywhere and from any place. The costs of the IT infrastructure will be cheaper because the healthcare units will only rent the infrastructure to store healthcare data as it need and will no longer need the latest equipment for the applications used, managed or maintained. They need only computers or devices with access to Internet. In emphasizing the cost and performance benefits of the cloud computing in healthcare, some fundamental security problems have been left unresolved. Determining the security of complex computer systems is also a long-standing security problem that overshadows large scale computing in general. Attaining the high assurance qualities in implementations has been an elusive goal of computer security researchers and practitioners, and is also a work in progress for cloud computing. Few research papers have systematically studied the impact of cloud computing on healthcare IT in terms of its opportunities and challenges. Table 1 shows some of opportunities and challenges from the viewpoint of management, technology, security, and privacy.

Table 1. Cloud computing opportunity and challenges

Aspects	Opportunities	Challenges
Technology	Infrastructure scalability and flexibility Reduction of IT maintenance Advantage for green computing	Bugs in large-scale distributed cloud systems Unpredictable performance Data transfer bottlenecks Resource exhaustion issues
Management	Computing resources available on demand Lower cost of new IT infrastructure Payment of use as needed	Organizational inertia Lack of trust by health care professionals Loss of governance Provider’s compliance
Privacy	Development of guidelines and technologies Protect customer’s data and privacy from provider’s commitments Fostering of regulations by government for data and privacy protection	Privacy issues Data jurisdiction issues
Security	Increasing data security at replication of data in multiple locations Strengthening resilience- dynamically scaled defensive resources More resources available for data protection	Privilege abuse Poor encryption key management Public management interface issues Failure separation

Security of the cloud infrastructure relies on trusted computing and cryptography. Healthcare data must be protected in a manner consistent with policies, whether in the organization’s computing center or the cloud. No standard service contract exists that covers the ranges of cloud services available and the needs of different organizations.

6 Conclusion

Using the cloud computing technology in a healthcare may considerably improve the access to information, which can be done be much easier. The scalability, that is the key of the cloud computing, can offer more resources needed for certain operation at any time. The collaboration between healthcare units is an opportunity offered by cloud computing for healthcare staff. With this technology can be checked the availability of a physician, a medical specialist, a product or a service at different times and in different cases.

Security and privacy issues of cloud computing are delaying its fast adoption, but it has become very popular and we needed to provide security mechanisms to ensure its secure adoption. While security and privacy services in the cloud computing can be fine-tuned and delivered in new ways and by new types of service providers, there need to be frameworks that efficiently deliver cloud-based security services and provide a desirable solution to customers based on their requirements.

Although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment, especially when it comes to medical data. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Implementation of the privacy and security standards that are currently under development within the cloud community, including business associate contracts that specify auditable, enforceable performance metrics and sharing of liabilities, should allow such a system to achieve compliance with federal privacy and security regulations. There are still many challenges to fostering the new model of cloud computing in healthcare.

Cloud computing is a new model of computing that promises to provide more flexibility, less expense, and more efficiency in IT services to end users. It offers potential opportunities for improving EHR adoption, health care services, and research. When a healthcare organization considers moving its service into the cloud, it needs strategic planning to examine environmental factors such as staffing, budget, technologies, organizational culture, and government regulations that may affect it, assess its capabilities to achieve the goal, and identify strategies designed to move forward. Cloud computing presents a compelling opportunity for consumers of IT and producers of information services.

References

1. Pardamean, B., Rumanda, R. R.: Integrated Model of Cloud-Based E-Medical Record for Health Care Organizations. In 10th WSEAS International Conference on E-Activities, pp. 157-162, December 2011
2. Srivastava, P., Jada, R., Razdan, P.: Cloud Computing in Indian Healthcare Sector. In Proceedings of ASCNT-2011, CDAC Noida, India, 2011
3. Lupşe, O.S., Vida, M. M., Tivadar, L. S.: Cloud Computing and Interoperability in Healthcare Information Systems. In INTELLI 2012: The First International Conference on Intelligent Systems and Applications, 2012
4. Karthikeyan, N., Sukanesh, R.: Case Study on Software as a Service (SaaS) Based Emergency Healthcare in India. In European Journal of Scientific Research, ISSN 1450-216x, Vol.69 No.3, pp. 461-472, 2012
5. Zhang, R., Liu, L.: Security Models and Requirements for Healthcare Application Clouds. In IEEE 3rd International Conference on Cloud Computing, July 2010
6. Rolim, C. O., Koch, F. L., Westphall, C. B., Werner, J., Fracalossi, A., Salvador, G. S.: A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions. In Second International Conference on e-Health, Telemedicine and Social Medicine, 2010
7. Perumal, B., Rajasekaran, P. M., Ramalingam, H. M: WSN Integrated cloud for automated telemedicine based e-healthcare applications. In 4th International Conference on

Bioinformatics and Biomedical Technology, IPCBEE vol.29. IACSIT Press Singapore, 2012

8. Nalin, M., Baroni, I., Sanna, A.: E-health drivers and barriers for cloud computing adoption. In International Conference on Cloud Computing & Services Science, Netherlands, 2011
9. Löhr, H., Sadeghi, A. R., Winandy, M.: Securing the E-Health Cloud. In Proceedings of the 1st ACM International Health Informatics Symposium, IHI 2010
10. Dandapani, A., Palani, D.: Cloud Computing (Implementation in Health Care Technology and Solution for Instant Medication using Cloud). In International Conference on Computing and Control Engineering, April 2012
11. Schweitzer, E. J.: Reconciliation of the cloud computing model with US federal electronic health record regulations,Journal of American Medical Information Association, may 2012
12. Botts, N., Thoms, B., Noamani, A., Horan, T. A.: Cloud Computing Architectures for the Underserved: Public Health Cyberinfrastructures through a Network of HealthATMs. In Proceedings of the 43rd Hawaii International Conference on System Sciences, 2010
13. Rashid Al Masud, S. M.: A Novel Approach to Introduce Cloud Services in Healthcare Sectors for the Medically Underserved Populations in South Asia. In International Journal of Engineering Research and Applications, Vol. 2, Issue 3, pp.1337-1346, May-Jun 2012
14. Jansen, W. A.: Cloud Hooks:Security and Privacy Issues in Cloud Computing. In Proceedings of the 44th Hawaii International Conference on System Sciences, 2011
15. Clarke, A., Steele, R.: Secure and Reliable Distributed Health Records: Achieving Query Assurance Across Repositories of Encrypted Health Data. In 45th Hawaii International Conference on System Sciences, 2012
16. Al Zain, M. A., Pardede, E., Soh, B., Thom, J. A.: Cloud Computing Security: From Single to Multi-Clouds. In 45th Hawaii International Conference on System Sciences, 2012
17. Takabi, H., Joshi, J. B. D.: Policy Management as a Service:An Approach to Manage Policy Heterogeneity in Cloud Computing Environment. In 45th Hawaii International Conference on System Sciences, 2012
18. Morin, J. H., Gateau, B.: Towards Cloud Computing SLA Risk Management: Issues and Challenges. In 45th Hawaii International Conference on System Sciences, 2012
19. Huu, T. T., Koslovski, G., Anhalt, F., Montagnat, J., Vicat, P., Primet, B., Elastic, J.: Cloud and Virtual Network Framework for Application Performance-cost Optimization. Published online: 4 November 2010, © Springer Science+Business Media B.V. 2010
20. Rimal, B. P., Jukan, A., Katsaros, D., Goeleven, Y.: Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach. Published online: 7 December 2010, © Springer Science+Business Media B.V. 2010
21. Caron, E., Desprez, F., Muresan, A.: Pattern Matching Based Forecast of Non-periodic Repetitive Behavior for Cloud Clients. Published online: 6 January 2011, © Springer Science+Business Media B.V. 2011
22. Diaz, R. G., Ramo, A. C., Agüero, A. C., Fifield, T., Sevior, M.: Belle-DIRAC Setup for Using Amazon Elastic Computer Cloud Providing Homogeneous Access to Heterogeneous Computing Resources. Published online: 13 January 2011, © Springer Science+Business Media B.V. 2011
23. Vaquero, L., Caceres, J., Lindner, M., Merino, L. R.: A Break in the Clouds: Towards a Cloud Definition. In ACM SIGCOMM Computer Communication Rev, pp. 50–55, 2009
24. Health Level Seven International (HL7), http://www.hl7.org/
25. International Organization for Standardization (ISO). Technical Committee 215, Health Informatics, http://www.iso.org/iso/iso_technical_committee?commid=54960
26. Hassan, T., James, B. D., Gail-Joon, A.: Security and Privacy Challenges in Cloud Computing Environments. In IEEE journal & magazines, vol. 8 Issue 6, pp. 32-39, 2010
27. Sunyaev, A., Pflug, J.: Risk evaluation and security analysis of the clinical area within the German electronic health information system. Published online: February 2012, Springer