A FRAMEWORK FOR SECURE HEALTHCARE SYSTEMS BASED ON BIG DATA ANALYTICS IN MOBILE CLOUD COMPUTING ENVIRONMENTS

Ahmed E. Youssef

College of Computer & Information Sciences, King Saud University, Riyadh, KSA
Faculty of Engineering, Helwan University, Cairo, Egypt

ABSTRACT

In this paper we introduce a framework for Healthcare Information Systems (HISs) based on big data analytics in mobile cloud computing environments. This framework provides a high level of integration, interoperability, availability and sharing of healthcare data among healthcare providers, patients, and practitioners. Electronic Medical Records (EMRs) of patients dispersed among different Care Delivery Organizations (CDOs) are integrated and stored in the Cloud storage area, this creates an Electronic Health Records (EHRs) for each patient. Mobile Cloud allows fast Internet access and provision of EHRs from anywhere and at any time via different platforms. Due to the massive size of healthcare data, the exponential increase in the speed in which this data is generated and the complexity of healthcare data type, the proposed framework employs big data analytics to find useful insights that help practitioners take critical decisions in the right time. In addition, our proposed framework applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of medical information. We believe that the proposed framework paves the way for a new generation of lower cost, more efficient healthcare systems.

KEYWORDS

Electronic Health Records; Big Data; Mobile Cloud Computing; Information Security; Healthcare Systems, HL7.

1. INTRODUCTION

The 21st century Healthcare Information Technology (HIT) has created the ability to electronically store, maintain, and move data across the world in a matter of seconds and has the potential to provide healthcare with tremendous increasing productivity and quality of services. It permits each provider to have his own database of patients' Electronic Medical Records (EMRs). Previous studies of the value of connected EMR systems estimated a potential efficiency savings of $77 billion per year at the 90% level of adoption; added value for safety and health could double these savings [10]. One problem in today's EMR systems is that they are highly centralized, each Healthcare Provider (HP) has its own local EMR system. This makes health information for any patient dispersed among different HPs and, therefore, its retrieval will be a challenge. The ability to universally access all patient healthcare information in a timely fashion is of utmost important [1, 10, 58]. Health information needs to be accessible and available to everyone involved in the delivery of patient healthcare from the researchers attempting to find causes, treatments, and cures for diseases to the patients themselves. Therefore, a high level of

DOI : 10.5121/ijasa.2014.2201

data integration, interoperability, and sharing among different healthcare practitioners and institutions is required in order to deliver high-quality healthcare to the patients they serve [54].

The revolution in healthcare data size is another problem in today's Healthcare Information Systems (HISs). This revolution is not just about the massive size of healthcare data, but we also witness an exponential increase in the speed in which this data is generated and a complex varieties of data type (i.e., structured, semi structured, unstructured). The Development of new technologies such as capturing devices, sensors, and mobile applications is a major source of healthcare data. Additional sources are added every day; patient social network communications in digital forms are increasing, collection of genomic information became cheaper and more medical knowledge/discoveries are being accumulated. Such big healthcare data is difficult to process or analyze using common database management tools. Obviously, capturing, storing, searching, and analyzing healthcare big data to find useful insights will improve the outcomes of the healthcare systems through smarter decisions and will lower healthcare cost as well, however, it requires efficient analytical algorithms and powerful computing environments. Finally, the increased reliance on networked healthcare data brings new challenges to securing medical records in EHR systems. Authenticating individuals and authorizing global secure access to patients' records are vital security requirements. Physical face-to-face methods of identifying and authenticating patients and providers no longer apply; methods of electronic identification and authentication are required. Moreover, electronic records are susceptible to inappropriate access, compromised data integrity, or widespread unauthorized distribution. New security measures are needed to secure patients' records on HISs.

In this paper we introduce a framework for secure HISs based on big data analytics in mobile cloud computing environments. This framework provides a high level of integration, interoperability, and sharing of EHRs among HPs, patients, and practitioners. It integrates distinct EMRs of a patient from different HPs distracted among different cities, states, and regions and store them in the Cloud data storage areas. Mobile Cloud computing technology [57-61] provides a fast Internet access, and provision of EHRs from anywhere and at any time with high availability. Due to the massive size of healthcare data, the exponential increase in the speed in which this data is generated and the complexity of healthcare data type, the proposed framework employs big data analytics to find useful insights that help practitioners take critical decisions in the right time. Our proposed framework applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of medical data. Authenticated healthcare providers, practitioners, and patients are authorized by the Cloud Service Providers (CSPs) at different levels of privilege and permissions to securely access EHRs and retrieve patients' information. We believe that the proposed framework paves the way for a new generation of lower cost, more efficient healthcare systems.

The rest of this paper is organized as follows: section 2 discusses the problem of integrating patients' EMRs dispersed among different CDOs. Section 3 discusses how mobile cloud computing solution improves integration, interoperability, and availability of EHRs. Section 4 explores the issue of "Big" healthcare data analysis. Security issues associated with EHR are discussed in section 5. Our proposed framework for HISs is given in section 6. Finally, in section 7, we give our conclusion remarks and future work.

2. INTEGRATING ELECTRONIC MEDICAL RECORDS

Today, there is a widespread use of EMRs or EHRs systems. These terms are used interchangeably by many in both healthcare industry and health science literature; however, they describe completely different concepts according to Health Information and Management System Society (HIMSS) Analytics [6, 7]. An EMR is a formatted record of patient health information

owned by a hospital or any healthcare provider. The data in the EMR system is the legal record of what happened to the patient during his encounter at the CDO and is owned and managed by one CDO [6]. A significant disadvantage to EMRs is that they cannot be easily and accurately electronically shared and distributed.

On the other hand, HIMSS defined the EHR as "a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Included in this information are patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data, and radiology reports. The EHR automates and streamlines the clinician's workflow" [7]. The definition of EHR system is "the set of components that form the mechanism by which EHRs are created, used, stored, and retrieved" [8, 9]. EHRs are typically composed of a subset of EMRs maintained by each CDO and is assigned to a patient. In [10] Zhang and Liu compared between EMR and EHR from different perspectives. This comparison is shown in Table 1.

Table 1: A comparison between EMRs and EHRs [10]

	EMR	**EHR**
Definition	The legal record of clinical services for patient within a CDO.	A subset of EMRs from one or more CDOs where patient received clinical services.
Owner	Owned by one CDO	Owned by several CDOs
Customer and Usage Scope	EMR systems are supplied by enterprise vendor and installed by hospitals, health systems, clinics, etc.	EHR systems are run by community, state, or regional emergence, or national wide emergence organization.
Right of patients	Patients can get access to some EMR information once authorized by the EMR owner	Patients are provided with interactive access as well as the ability to append information.
Interoperability with other CDOs	Each EMR contains the patient's encounter in a single CDO. It does not contain other CDO counter data.	Sharing information among multiple CDOs.

An EHR provide a mean of communication among clinicians contributing to the patient's care by sharing health information between different EMR systems in different CDOs. The challenge here is how to integrate distinct EMRs scattered in different CDOs in different cities, states, and regions to create unified EHRs. In our framework, the Cloud provides a solution for this problem by networking the CDOs and collecting patients' EMRs from the interconnected CDOs. It is also desirable to have a unified standard format for EHRs to support interoperability and data sharing.

3. HEALTHCARE MOBILE CLOUD COMPUTING

In recent years, mobile devices have started becoming abundant in many healthcare applications. The reason for the increasing usage of mobile computing is its ability to provide a tool to the user when and where it is needed regardless of user movement, hence, supporting location independence. However, it suffers some inherent problems such as limited scalability of users and devices, limited availability of software applications, resources scarceness in embedded gadgets, frequent disconnection and finite energy of mobile devices. In healthcare sector, the effect of these limitations is magnified due to the massive size, excessive complexity, and rapid generation of healthcare data. As a result, a wide range of healthcare applications are difficult to run in

mobile devices such as radiology processing and recognition, patients' social networking data management, genomic information and sensor data applications. In addition, progress in interoperation and sharing data among different EMR systems has been extremely slow due to the high cost and poor usability. What is needed is an environment that is capable of capturing, storing, searching, sharing and analyzing healthcare big data efficiently to provide right intervention to the right patient at the right time.

Cloud computing [15-29] provides an attractive IT platform to cut down the cost of EHR systems in terms of both ownership and IT maintenance burdens for many medical practices. Cloud environment can host EHRs and allows sharing, interoperability, high availability, and fast accessibility of healthcare data. Cloud Computing (CC) platforms possess the ability to overcome the discrepancies of mobile computing with their scalable, highly available and resource pooling computing resources. The main idea behind CC is to offload data and computation to a remote resource provider (i.e., the Internet) which offers broad network access. The concept of offloading data and computations in the Cloud, is used to address the inherent problems in mobile computing by using resource providers (i.e., cloud resources) other than the embedded devices themselves to host the execution of user applications and store users' data. The problems are addressed as follows: 1) by exploiting the computing and storage capabilities (resource pooling) of the cloud, mobile intensive applications can be executed on low resource and limited energy mobile devices, 2) the broad network access of the cloud overcomes the limited availability and frequent disconnection problems since cloud resources are available in anywhere and at any time, 3) the infrastructure of cloud computing is very scalable, cloud providers can add new nodes and servers to cloud with minor modifications to cloud infrastructure, therefore; more services can be added to the cloud, this allows more mobile users to be served and more portable devices to be connected [60].

A study by Juniper Research states that the consumer and enterprise market for cloud-based mobile applications is expected to rise to $9.5 billion by 2014 [61]. In healthcare sector we believe that this environment is very promising and is expected to change how healthcare services are provisioned. Mobile cloud computing technology will contribute to healthcare sectors in the following ways:

- Integrating healthcare data dispersed among different healthcare organizations and social media.
- Providing a shared pool of computing resources that is capable of storing and analyzing healthcare big data efficiently to take smarter decisions at the right time.
- Providing dynamic provision of reconfigurable computing resources which can be scaled up and down upon user demand. This will help reduce the cost of cloud-based healthcare systems.
- Improving user and device scalability and data availability and accessibility in healthcare systems.

Healthcare cloud can provide two deployment Models. These models describe the level of data sharing among different CDOs, patients, and practitioners when using the cloud. These models are:

- Private healthcare cloud: The cloud infrastructure is owned solely by a CDO. It may be managed by the CDO or a CSP and may exist on or off premise. The CSP provides the same capability in terms of security and privacy protection as those in the EMR system running by a CDO.
- Community healthcare cloud: The cloud infrastructure is shared by several CDOs and supports a specific community that has shared concerns (e.g., mission, security

requirements, and policy). It is managed by a CSP or by the CDOs and may exist on or off premise.

Healthcare services provided by healthcare clouds are classified as follows:

- Software as a Service (SaaS): Healthcare applications, such as EHRs, are hosted as a service and provided to practitioners, healthcare providers, and patients across the Internet, with no need to install and run on their own computer. Hosted applications can be accessed through web browsers from various client devices such as laptops, PDAs and cell phones. Multiple users can share the applications and avoid the trouble associated with software maintenance, upgrading and the need for additional licenses.
- Platform as a Service (PaaS): PaaS is a development platform that allows healthcare providers to not only deploy but also design, model, develop and test healthcare applications directly on the Cloud. It supports work in groups on collaborative healthcare projects where project team members are geographically distributed. This requires PaaS to provide development infrastructure including tools and programming languages.
- Infrastructure as a Service (IaaS): healthcare providers can directly use independent virtual machines that isolate the underlying physical hardware of the cloud from them. They can dynamically provision/release virtual computing resources based on their increasing/decreasing resource demand.

4. HEALTHCARE BIG DATA

Improving healthcare services and reducing medical cost are the ultimate goals of nations worldwide. However, the revolution of healthcare data size remains an obstacle that hinder achieve this goal. In 2012, worldwide digital healthcare data was estimated to be equal to 500 petabytes and is expected to reach 25,000 petabytes in 2020 [62]. Obviously, capturing, storing, searching, sharing and analyzing such big data to find useful insights will improve the outcomes of the healthcare systems through smarter decisions and will lower healthcare cost as well, however, traditional database management tools are no longer suitable to process these data. New efficient algorithms are required to accomplish this task. For example, in the United States, more than 71 million individuals are admitted to hospitals each year, according to the latest survey from the American Hospital Association. Studies have concluded that in 2006 well over $30 billion was spent on unnecessary hospital admissions. The Heritage Provider Network (HPN) arises the question: "*Can we identify earlier those most at risk and ensure they get the treatment they need?*" and it believes that the answer is "*yes*". To achieve its goal of developing a breakthrough algorithm that uses available patient data to predict and prevent unnecessary hospitalizations, HPN sponsored the Heritage Health $3 Million Prize Competition. Winning solutions will use a combination of several predictive models and the winning team will create an algorithm that predicts how many days a patient will spend in a hospital in the next year. Once known, HPs can develop new care plans and strategies to reach patients before emergencies occur, thereby reducing the number of unnecessary hospitalizations. This will result in increasing the health of patients while decreasing the cost of care [62].

Big data analytics is motivated in healthcare through the following aspects [62]:

- Healthcare data is now growing very rapidly in terms of size, complexity, and speed of generation and traditional database and data mining techniques are no longer efficient in storing, processing and analyzing these data. New innovative tools are needed in order to handle these data within a tolerable elapsed time.

- The patient's behavioral data is captured through several sensors; patients' various social interactions and communications.
- The standard medical practice is now moving from relatively ad-hoc and subjective decision making to evidence-based healthcare.
- Inferring knowledge from complex heterogeneous patient sources and leveraging the patient/data correlations in longitudinal records.
- Understanding unstructured clinical notes in the right context.
- Efficiently handling large volumes of medical imaging data and extracting potentially useful information and biomarkers.
- Analyzing genomic data is a computationally intensive task and combining with standard clinical data adds additional layers of complexity.

5. SECURITY ISSUES

In cloud-based HIS, security should be the top priority from day one. Patients' data should be protected with comprehensive physical security, data encryption, user authentication, and application security as well as the latest standard-setting security practices and certifications, and secure point-to-point data replication for data backup. These security issues have been extensively investigated for cloud computing in general [13, 14, 30-53]. A major challenge to healthcare cloud is the security threats including tampering or leakage of sensitive patient's data on the cloud, loss of privacy of patient's information, and the unauthorized use of this information. Hence, a number of security requirements should be satisfied by healthcare cloud computing systems. The main security and privacy requirements for healthcare clouds are discussed below [10, 13, 14]:

- Authentication: in a healthcare cloud, both healthcare information offered by CSPs and identities of users (HPs, practitioners, and patients) should be verified at the entry of every access using user names and passwords assigned to users by CSPs.
- Authorization: is an essential security requirement that is used to control access priorities, permissions and resource ownerships of the users on the cloud. Each cloud user is granted privileges based on his account. Patient can allow or deny sharing their information with other healthcare practitioners or CDOs. To implement patient consent in a healthcare system, patient may grant rights to users on the basis of a role or attributes held by the respective user.
- Non-repudiation: implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. In a healthcare system, technologies such as digital signatures, timestamps, confirmation receipt, and encryption can be used to establish authenticity and non-repudiation for patients, CDOs, and practitioners.
- Integrity and Confidentiality: integrity means preserving the accuracy and consistency of data. In the healthcare system, it refers to the fact that EHRs have not been tampered by unauthorized use. Confidentiality is defined by the International Organization for Standardization (ISO) in ISO-17799 as "ensuring that information is accessible only to those authorized to have access". Confidentiality and integrity can be achieved by access control and encryption techniques in EHR systems.
- Availability: For any EHR system to serve its purpose, the information must be available when it is needed. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service (DoS) attacks.

6. THE PROPOSED FRAMEWORK

One of the most important challenges in developing HISs is to provide mechanisms to analyze and obtain patients' information from multiple EMR/EHR repositories accurately, securely and fast. In the previous sections, we discussed the requirements for a new generation of secure HIS in a cloud computing environment based on big data analytics. In this section, we propose a framework for developing such systems. Figure 1 shows the proposed framework which consists of the following main components:

The Cloud: the first component is the cloud environment itself that hosts patient information and provides different types of service to authorized users. The cloud can be used as private or community environment according to the required level of data sharing. It makes these records ubiquitously accessible for patients, HPs, and practitioners. This component was discussed in detail in section 3.

The EHR: the second component is the EHR where distinct patient records are integrated from different units (pharmacy, registration, Lab,...) in many CDOs distracted in a city, state, or region and stored in the cloud. One critical issue here is the ability to link patients to their records without errors. This is achieved by the usage of a hybrid linking approach that combine statistical matching and Unique Patient Identifier (UPI) approach [1, 12, 55, 58]. The statistical algorithm is used first to retrieve patients' records from EMRs in different interconnected CDOs. The records are integrated and stored to form EHRs. UPI for each patient can then be used as a primary key to filter patient's information in EHRs and eliminate errors occur during statistical matching.

The Security Model: the third component is the one that guarantees protecting security and privacy in HIS. Encryption algorithms such as AES [2] and RC4 [3] and authentication techniques such as One Time Password (OTP) [4] and Two Factor Authentication (2FA) [5] can be applied to protect EHR from tampering and unauthorized access. The healthcare authority can now setup groups of clinician authorized to access patients' EHRs. It is also responsible for defining privileges for each group according to their specialization, disease type and complexity, and the role they play in treatment. The group may contain specialists, doctors, nurses, lab technicians, pharmacists, or other practitioners. Group members can be from different hospitals, cities, or regions; hence, the cloud facilitates sharing of medical records among group members to give perfect consultation. The healthcare authority assigns to each group digital signatures to sign the medical certificates provided by them. Signed medical certificates are available to the patient and are stored in his/her EHRs. The patient can authenticate diagnosis and consultations through these digitally signed certificates. For example, allowing specific group to access the medical record for patient-A, his family medical records, give the appropriate treatment decision, medications, and report the status of his health. Each member in one group may have different privileges according to his job and profession. On other hand, the patient is allowed to see only his medical records, access the results of medical tests, validate the integrity of his records, and verify the authenticity of medical certificate given by a group with a digital signature. The researchers take the statistical information without knowing the full information about the patients. The health insurance companies may verify the integrity of treatment decisions to their customers.

The Big Data Analytics: this component can deploy different tools that analyze multi-terabyte EHR databases in the cloud and give real-time insights about the data. CSPs offer many big data analytics tools such as:

- **Google Big Query:** uses Google's cloud infrastructure to store and query massive datasets in few seconds by enabling super-fast SQL like queries.
- **MapReduce:** is a software tool that enables cloud users to write application to process in parallel a vast amount of data on large clusters. It is divided into two parts: **Map**, a function that splits work to different nodes in the distributed cluster, and **Reduce**, another function that collects the work and resolves the results into a single value.

The CDOs: this component includes different healthcare organizations distributed across the country. Each organization consists of several clinical and administrative departments such as Radiology, Lab, Pharmacy, Billing, etc. These departments are integrated via the EHR unit in the cloud which enable data sharing and interoperability. Communications between different CDOs departments and the EHR is made possible using HL7 protocol which is a structured standard that is used as a means of exchanging information between healthcare applications. It defines a format for the transmission of health-related information [63].

The proposed framework for a new generation HISs aims to achieve the following goals:

- Provide healthcare services of high quality and low cost to the patients using a combination of big data, cloud computing and mobile computing technologies.
- Take advantage of the massive amounts of healthcare data and provide right intervention to the right patient at the right time.
- Provide personalized healthcare to the patient.
- Protect the security and the privacy of healthcare data.
- Bridge big data, mobile-cloud computing, information security and medical informatics communities to foster interdisciplinary works between them.

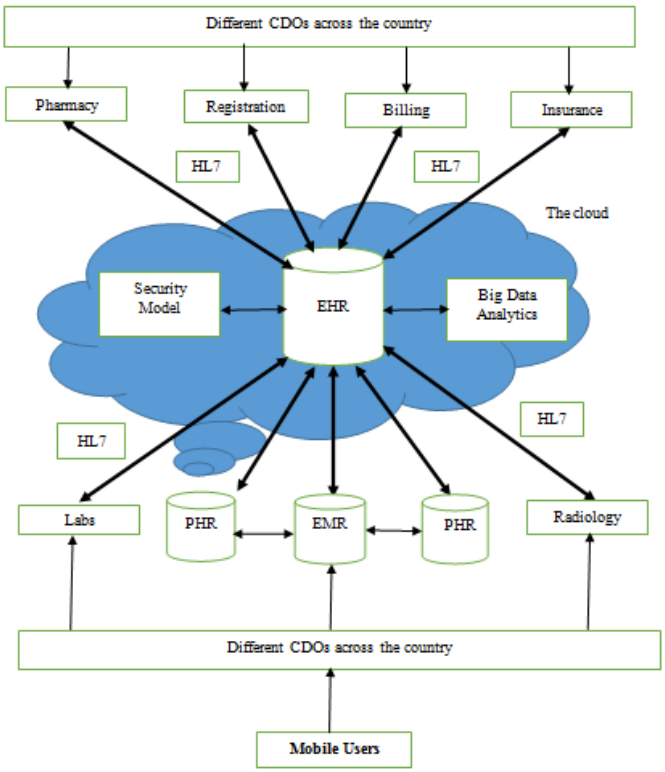

FIG. 1: A FRAMEWORK FOR EHR BASED ON MOBILE CLOUD COMPUTING AND BIG DATA ANALYTICS

7. CONCLUSIONS AND FUTURE WORK

This paper proposes a framework for secure Health Information Systems (HISs) based on big data analytics in mobile cloud computing environment. The framework provides a high level of integration, interoperability, and sharing of EHRs among healthcare providers, patients and practitioners. The cloud permits a fast Internet access, sharing, and provision of EHRs by authenticated users. Big data analytics helps analyze patient data to provide right intervention to the right patient at the right time. The proposed framework applies a set of security constraints and access control that guarantee integrity, confidentiality, and privacy of medical data. The ultimate goal of the proposed framework is to introduce a new generation of HISs that are able to provide healthcare services of high quality and low cost to the patients using this combination of big data analytics, cloud computing and mobile computing technologies. In the future we plan to design and implement HIS based on the proposed framework.

REFERENCES

[1] R. Hillestad, J. Bigelow, B. Chaudhry, P. Dreyer, M. Greenberg, R. Meili, M. Ridgely, J. Rothenberg, and R Taylor, “Identitity Crisis:An examination of the costs and benefits of Unique patient identifier for the U.S. health care sysetm”, TR The RAND Health Corporation, 2008.

[2] Federal Information Processing Standards Publication 197,"Specification for the Advanced Encryption Standards (AES)", 2001.

[3] S. Fluhrer, I. Mantin, and A. Shamir, "Weakness in the Key schedualing algorithm of RC4", 8th Annual International Workshop on Selected Areas in Cryptography, Springer-Verlag London, UK, 2001.

[4] M. Johnsson and A. Azam, " Mobile One Time Passwords and RC4 Encryption for Cloud Computing", Technical report, IDE1108, March 2011.

[5] http://en.wikipedia.org/wiki/Two-factor_authentication

[6] D. Garets and M. Davis, A HIMSS Analytics White Paper, “Electronic Medical Records vs. Electronic Health Records: Yes, There Is a Difference”, January 26, 2006.

[7] http://www.himss.org/asp/indIntellHome.asp

[8] Y. Kwak, " Intemational Standards for Building Electronic Health Record (EHR)", Enterprise networking and Computing in Healthcare Industry, 2005. HEALTHCOM 2005. Proceedings of 7th International Workshop on 23-25 June 2005 Page(s):335 - 338.

[9] ISO/TR 20514, "Health informatics — Electronic health record — Definition, scope and context ",2005.

[10] R. Zhang and L. Liu, “Security Models and Requitements for Healthcare Application Clouds”, IEEE 3rd International Conference on Cloud Computing, 2010.

[11] G. Federico, R. Meili, and R. Scoville, “Extrapolating Evidence of Health Information Technology Savings and Costs”, Santa Monica, Calif.: RAND Corporation, MG-410-HLTH, 2005.

[12] American Standards for Testing and Materials (ASTM), “Standard Guide for Properties of a Universal Healthcare Identifier (UHID)”, West Conshohocken, Pa.: ASTM, E1714-00, October 10, 2000.

[13] A. Youssef and M. Alageel, “Security Issues in Cloud Computing”, the GSTF International Journal on Computing , Vol.1 No. 3, 2011.

[14] Ahmed E. Youssef and Manal Alageel, “A Framework for Secure Cloud Computing”, International Journal of Computer Science Issues (IJCSI), Vol. 9, Issue 4, No 3, pp. 478-500, July 2012.

[15] GTSI Group, “Cloud Computing - Building a Framework for Successful Transition,” White Paper, GTSI Corporation, 2009.

[16] L. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A Break in the Clouds: Towards a Cloud Definition,” ACM SIGCOMM Computer Communication Review, Volume 39 Issue 1, pages 50-55, January 2009.

[17] M. Boroujerdi and S. Nazem, “Cloud Computing: Changing Cogitation about Computing,” World Academy of Science, Engineering and Technology, 2009.

[18] M. Miller, "Cloud Computing Pros and Cons for End Users", microsoftpartnercommunity.co.uk, 2009.
[19] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.
[20] R. Prodan and S. Ostermann, "A Survey and Taxonomy of Infrastructure as a Service and Web Hosting Cloud Providers", 10th IEEE/ACM International Conference on Grid Computing, 2009
[21] Wikipedia, http://en.wikipedia.org/wiki/Cloud_Computing.
[22] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing" Communication of the ACM, Vol. 53, No. 4, April 2010.
[23] K. Chard, S. Caton, O. Rana and K. Bubendorfer, "Social Cloud: Cloud Computing in Social Networks" 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10,2010.
[24] L. Tang, J. Dong, Y. Zhao and L. Zhang "Enterprise Cloud Service Architecture" 3rd IEEE International Conference on Cloud Computing,Miami, FL, USA, July 5-10,2010.
[25] W. Tsai, X. Sun, J. Balasooriya, "Service-Oriented Cloud Computing Architecture", 7th IEEE International Conference on Information Technology, 2010.
[26] T. Dillon, C. Wu and E. Chang, "Cloud Computing: Issues and Challenges", 24th IEEE International Conference on Advanced Information Networking and Appications, 2010.
[27] Introduction to Cloud Computing, White Paper,Dialogic Corporation, 2010.
[28] R. Buyya, J. Broberg, and A. Goscinski, "Cloud Computing Principles and Paradigms", John Wiley & Sons, 2011.
[29] NIST, http://www.nist.gov/itl/cloud/index.cfm
[30] K. Popvoic and Z. Hocenski, "Cloud Computing Security Issues and Challenges" MIPRO, Opatijia, Croatia, May 24-28, 2010.
[31] Ramgovind S, Eloff MM and Smith E. "The Management of Security in Cloud Computing" Information Security for South Africa (ISSA), Sandton, Johannesburg, 2-4 Aug, 2010.
[32] N. Gruschka and M. Jensen, "Attack Surface: A Taxonomy for Attacks on Cloud Services", 3rd IEEE International Conference on Cloud Computing, Miami, FL, USA, July 5-10,2010.
[33] K. Zunnurhain and S. Vrbsky, "Security Attacks and Solutions in Clouds", 2nd IEEE International Conference on Cloud Computing Technology and Science, Indianapolis, USA, Nov. 30- Dec. 3,2010.
[34] http://www.cloudsecurityalliance.org/
[35] SecureCloud 2010, http://www.cloudsecurityalliance.org/sc2010.html
[36] Cloud Security Alliance ,March 2010,"Top Threats to Cloud Computing V1.0"
[37] J. Bordkin, "Gartner:Seven Cloud-Computing Security Risks", 2008.
[38] M. Yildiz, J. Abawajy, T. Ercan and A. Bernoth," A Layered Security Approaches for Cloud Computing Infrastrucure", 10th International Symposium on Pervasive Systems, Algorithms, and Networks,2009.
[39] CSA, "Security Guidance for Critical Areas of Focus on Cloud Computing V2.1", 2009.
[40] J. Yang and W. Huang, "New network security based on Cloud Computing", Education Technology and Computer Science (ETCS), 2010.
[41] P. Mell and T. Grance, "The NIST Definition of Cloud Computing" Recommendation of NIST, Jan 2011.
[42] "Cloud Computing Security Considerations", Cyber Security Operation Cenetre, Technical report, 2011.
[43] I. Chuang, S. Li, K. Huang, and Y. Kuo, "An Effective Privacy Protection Scheme for Cloud Computing", In Proceeding of the 13th International Conference on Advanced Communication Technology (ICACT), 2011
[44] C. Wang, Q. Wang, K. Ren, and W .Lou, "Towards Secure and Dependable Storage Services in Cloud Computing", IEEE Transactions on Services Computing, Issue:99 , 2011.
[45] Q. Wang, C. Wang, K. Ren W. Lou, and J. Li, " Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE Transactions on Parallel and Distributed Systems, Volume : 22 , Issue:5, 2011.
[46] C. Băsescu, A. Carpen-Amarie, C. Leordeanu, A. Costan, and G. Antoniu, "Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies", In proceeding of IEEE International Conference on Advanced Information Networking and Applications (AINA), 2011

[47] R. Sravan Kumar and A. Saxena, “Data integrity proofs in cloud storage”, Third International Conference on Communication Systems and Networks (COMSNETS), 2011.
[48] W. Jansen and T. Grance, “NIST Guidelines on Security and Privacy in Public Cloud Computing”, Draft Special Publication 800-144, 2011.
[49] N. Robinson, L. Valeri, J. Cave, T. Starkey, H. Graux, S. Creese, and P. Hopkins, “The Cloud: Understanding the Security, Privacy and Trust Challenges”, Technical Report, RAND Europe, 2011.
[50] Q. Tong and Z. Shen, “The security of Cloud Computing System Enabled by Trusted Computing Technology”, 2nd International Conference on Signal Processing Systems (ICSPS),2010.
[51] A. Albeshri and W.Caelli, “Mutual Protection in a Cloud Computing Environment”, IEEE 12th International Conference on High Performance Computing and Communications (HPCC), Melbourne, 1-3 September 2010.
[52] http://csrc.nist.gov/archive/aes/rijndael/wsdindex.html
[53] Shucheng Yu, Cong Wang,KuiRen and Wenjing Lou, " Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", 2010
[54] M. Alnuem, S. EL-Masri, A. Youssef, A. Emam, “Towards Integrating National Electronic Care Records in Saudi Arabia”, The 2011 International Confernce on Bioinfomatics and Computational Biology, Monte Carlo Resort, Las Vegas, Nevada, USA, July 18-21, 2011
[55] A. Emam, A. Youssef, S. EL-Masri, and M. Alnuem “Towards Universial Patient Identifiers in KSA” IKE'11 - 10th Int'l Conference on Information and Knowledge Engineering, Las Vegas, Nevada, USA July 18-21, 2011.
[56] D. C. Leonard, Alexander P. Pons and S. S. Asfour,"Realization of a Universal Patient Identifier for Electronic Medical Records Through Biometric Technology", IEEE transaction on information technology in biomedicine, vol. 13, no. 2009.
[57] N. Fernando, S.W. Loke, and W. Rahayu, “Mobile Cloud Computing: A Survey”, Future Generation Computer Systems, vol. 29, pp. 84-106, 2013.
[58] A. R. Khan, M. Othman, S. Ahmad Madani, and S. U. Khan, “A Survey of Mobile Cloud Computing Application Models”, accepted in IEEE COMMUNICATIONS SURVEYS & TUTORIALS. file:///C:/Users/Administrator/Downloads/A_Survey_of_Mobile_Cloud_Computing_3.pdf
[59] K. Kumar and Y. Lue, “Cloud Computing for Mobile Users: Can Offloading Computation Save Energy”, Computer, Vol. 43, No. 4, IEEE Computer Socity, 2010.
[60] Ahmed E. Youssef, “Towards Pervasive Computing Environments With Cloud Services”, International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC), Vol.4, No.3, pp.1-9, June, 2013
[61] S. Perez, Mobile cloud computing: $9.5 billion by 2014, http://exoplanet.eu/ catalog.php, 2010.
[62] J. Sun and C. K. Reddy, “Big Data Analytics for Healthcare” Tutorial presentation at the SIAM International Conference on Data Mining, Austin, TX, 2013.
[63] http://www.interfaceware.com/hl7.html.