A Security based Framework for Interoperability of Healthcare Systems

Iroju Olaronke
Computer Science Department
Adeyemi College of Education
Ondo, Nigeria

Ikono Rhoda
Computer Science Department and Engineering Department
Obafemi Awolowo University
Ile-Ife, Nigeria

ABSTRACT

The healthcare domain requires the seamless, secured and meaningful exchange of health related information for effective and efficient patient care. These information are highly sensitive and they are meant to be highly confidential. However, health related information are usually distributed across several heterogeneous and autonomous healthcare systems which makes the interoperability process prone to abuse, medical fraud, inappropriate disclosure of patients' information for secondary purposes by unauthorized persons and misuse. The effects of inadequate security and privacy in healthcare include monetary penalties, loss of revenue, damage to the healthcare system reputation, risk of receiving less information for optimum care, decreased quality of patients' care as well as threat to patients' lives. Consequently, effective information protection within the healthcare domain is highly significant. Hence, this paper examines the security and privacy policies that safeguard sensitive and confidential information in healthcare systems during the exchange and use of vital health information. The paper also proposes a security based framework that seeks to mitigate security risks in healthcare, and thus protect the integrity, confidentiality, and access to health related information.

General Terms

Interoperability, security, privacy.

Keywords

Interoperability, healthcare, security, privacy.

1. INTRODUCTION

The ubiquity nature of Information and Communication Technology (ICT) is rapidly revolutionizing the healthcare system from the traditional paper based system to electronic based systems. Hence, technologies like electronic health records (EHR), electronic medical records (EMR), personal health record system (PHR), and computer-based patient record system (CBR) are swiftly emerging within the healthcare industry. In addition, the use of the internet has tremendous effects on the healthcare system by providing cost effective, timely, efficient and patient-centered care. The use of the Internet and electronic health systems have also changed the way information is acquired, processed, stored, exchanged, displayed and used within the healthcare industry. Furthermore, patients' information are usually stored in diverse autonomous electronic healthcare systems across the healthcare community. This has no doubt led to the fragmentation of patients' information in proprietary heterogeneous systems across healthcare organizations [1]. Nevertheless, for healthcare providers to have access to a clear, detailed and complete picture of a patient during care in a timely manner, health information exchange and interoperability among the diverse electronic healthcare systems are necessary. However, one of the major challenges of interoperability within the healthcare domain is security and privacy problems. Thus, interoperability becomes an intractable problem in healthcare when the security and control of health-related information cannot be guaranteed across healthcare institutions. Thus, the healthcare system is characterized by high cost, risk of receiving less information for patients' optimum care and decreased quality of patients care. Consequently, this paper reviews the security and privacy policies that safeguard sensitive and confidential information in healthcare systems during the exchange and use of health information. The paper also proposes a secured framework that seeks to mitigate security and privacy risks in healthcare.

2. INTEROPERABILITY

According to Moen [2], interoperability is the ability of independent systems or components to exchange meaningful information reliably and quickly without errors. The National Alliance for Health Information Technology also defined interoperability as the ability of different information technology systems and software applications to accurately, effectively, and consistently exchange data/information and also to use the information that has been exchanged [3]. Furthermore, Yum and Drogemuller [4] viewed interoperability as the ability of diverse computer programs to exchange/share information without any loss of content or meaning. Simply, interoperability can be viewed as shown in Figure 1. In Figure 1, it is assumed that the people on the left have information that the people on the right needs, and that the data in one system is accessible to the other system. Hence, interoperability is achieved if the receiving system and users properly comprehend the meaning of information they receive and they are able to use this information [5]. Interoperability is divided into two major architectural layers. These include syntactic and semantic interoperability [6,7,8]. Syntactic interoperability is concerned with the exchange of data between diverse systems or applications without taking into consideration the meaning of the data [9]. Khan et al. [10] viewed the concept of semantic interoperability from two perspectives. These include data interoperability and process interoperability. Data interoperability refers to the correct interpretation and understanding of the information exchanged between healthcare systems while process interoperability ensures seamless communication amongst diverse healthcare systems by developing shared understanding of their process artifacts. The benefits of interoperability in healthcare include easy access to health related information, reduced medical errors and healthcare cost, as well as the increase in the quality of healthcare. However, at the point of information exchange (syntactic interoperability) amongst heterogeneous healthcare systems and information use (semantic interoperability); there is always a need to protect patients' information from inappropriate disclosure, loss of integrity and unauthorized access. This will ensure a high degree of trust amongst healthcare professionals and their patients. Hence, physicians will be able to receive adequate information from the patients for optimum care, clinical outcome and operational efficiency analysis [11].

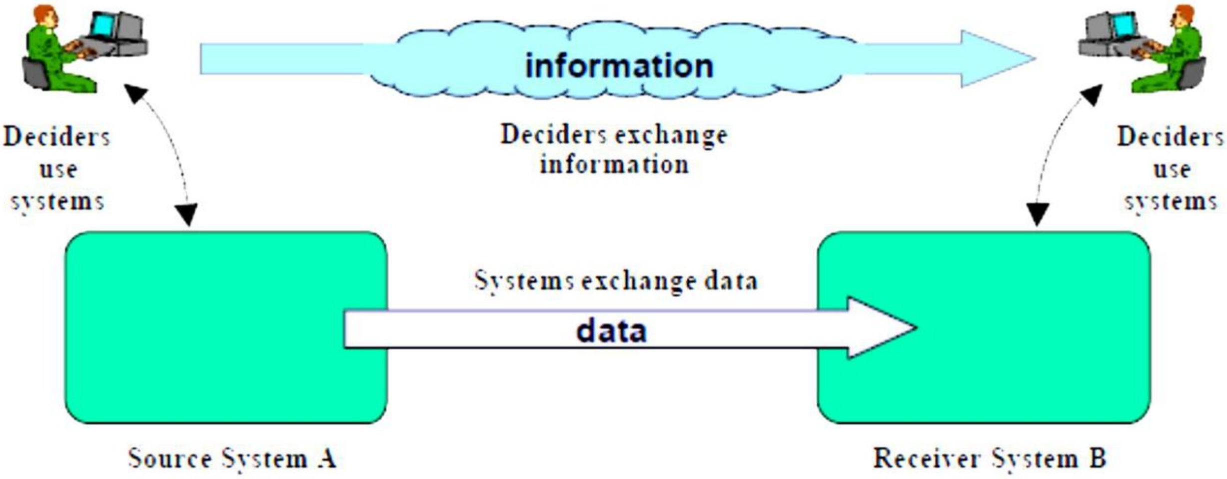

Fig1: The concept of interoperability [12]

3. PRIVACY ISSUES IN HEALTHCARE

The term privacy according to Cooper and Collman [11] has diverse meanings depending on the context of use. Privacy according to [13] is the right of individuals to prevent their information from being revealed to others; the claim of individuals to avoid surveillance or interference from other individuals, organizations or the government. In the context of healthcare, privacy is defined as individual ownership and control over personal health information [14]. Privacy can also be explicitly viewed in healthcare as the ability to protect patients' information from unauthorized access and disclosure [11]. Furthermore, Appari and Johnson [15] viewed privacy as an underlying governing principle of patient-physician relationship for effective delivery of healthcare. Thus, privacy can be defined as a way of ensuring the confidentiality of patients' information. Privacy however is usually a herculean task in healthcare. This is because the healthcare domain is susceptible to data fraud and medical identity theft due to the nature and content of information it acquires, stores and transmits, such information includes the social security number of the patient, insurance identification, payment information, and medical provider information amongst others [16]. Hence, one of the effects of data breaches in the healthcare domain is high cost. For instance, in the United States of America, the economic impact of data breaches in hospitals is $6 billion [17]. Unfortunately, most healthcare providers have little or no protection to prevent, monitor, or remedy data breaches [18]. Thus, the proliferation of the misuse of health related information is exponential. For instance, on September 20, 2010, a computer flash drive which contained the the names, addresses, Social Security Numbers (SSNs), and protected health information (PHI) of 280,000 Medicaid members was stolen from the corporate offices of a health plan, also the Personal health information of Congresswoman Nydia Velasquez, country singer Tammy Wynette and octomom Nadya Suleman were accessed by unauthorized individuals. This resulted in civil fines and humiliation to reputable health systems [16]. In addition, in 2011, employees of the UCLA health system had access to celebrities' records without proper authorization [19]. Furthermore, the General Accounting Office of the United States of America estimated that 10% of health expenditure reimbursed by Medicare accounts for healthcare was paid to fraudsters, identity thieves and fraudulent health service providers [20]. As a consequence, the improper disclosure of patients' information has resulted in diverse privacy laws and regulations such as the Health Insurance Portability and Accountability Act (HIPAA), National Health Information Technology and Privacy Advancement Act of 2007and Technologies for Restoring Users 'Security and Trust in Health Information Act of 2008, Red Flags Rule, The American Recovery and Reinvestment Act (ARRA). These policies were established to prevent breaches of sensitive healthcare information. According to Cooper and Collman [11], the HIPAA ensures that patients have legal rights concerning their personally identifiable healthcare information. HIPAA allows patients to have a right to how their information are revealed and used for other purposes apart from treatment, payment and other medical operations.

It grants patients the authority to have access to their medical records as well as modify these records. It also establishes responsibilities for healthcare organizations to protect and restrict the use or improper disclosure of patients' information. The HIPAA ensures the confidentiality, integrity, and availability of protected health information (PHI) across the covering entities which include health plans, healthcare clearing houses, and healthcare providers [13]. The HIPAA however does not make provisions for the business associates of the covering entities. This no doubt interrupts the secured exchange of health related data [11]. The goal of the National Health Information Technology and Privacy Advancement Act of 2007and Technologies for Restoring Users 'Security and Trust in Health Information Act of 2008 is to enhance privacy protection by granting incentives to de-identify health information for secondary purposes, establish health information technology and privacy systems, bring equity to healthcare provision, and increase private enterprise participation in patient privacy [15]. The Red Flags Rule on the other hand was established to avert medical identity theft as well as to detect, prevent and protect sensitive health information. The major drawback of the Red Flags Rule is that it is does not specify whom the rules apply to. This therefore accounts for the non-compliance of healthcare industry to this rule. The American Recovery and Reinvestment Act (ARRA) was setup to overcome the drawback of HIPAA. The ARRA makes provision for the data privacy and security of the business associates of the HIPAA covering entities. However, nearly 85 percent of hospitals do not act in accordance with this Act. Thus, the inability of federal authorities' to enforce the use of existing privacy rules in electronic healthcare systems. This heightens patients distrust in the use of electronic health information systems to provide adequate privacy protections. Hence, the healthcare domain is burdened with privacy challenges [11].

4. SECURITY ISSUES IN HEALTHCARE

Interoperability as previously defined is the meaningful exchange of information. However, it is not enough for the information to be transmitted from point A to B. The exchange of information must be done in such a way that the principle to which the recipient applies the received information is consistent with its use as intended by the source [21]. Thus, security becomes a cause of concern such that the content of the information exchanged is protected from unauthorized users and sufficiently complete so that it still has meaning to the recipient [21].

The National Institute of Standards and Technology [22] defines information security as the preservation of data's confidentiality, integrity, availability and accountability (commonly referred to as the "CIA" triad). Confidentiality in this definition refers to the ability to make data available to authorized persons or processes. For instance, a medical record of a cardiac patient which reveals a diagnosis of HIV would be undisclosed from cardiology researchers if HIV status is irrelevant to their research [23]. Integrity refers to the ability to maintain data or information or the ability to prevent the data or information from being altered in an unauthorized manner. Integrity according to the National Institute of Standards and Technology [22] is defined as guarding against improper information modification or destruction. It also guards against accidental damage to the system. Integrity ensures that changes made to the system by authorized users do not result in loss of data consistency. Hence, data integrity ensures that the data is accurate and complete without any unauthorized modifications or alterations. Availability refers to the ability to ensure that data or information is accessible and useable by authorized persons in a timely manner. According to Petković et al. [24], availability is the ability of up-to-date information to be accessible when needed at a required level of performance and at the appropriate place. Data availability is seen to be more vital than data confidentiality most especially in emergency cases. Accountability refers to the ability to audit, review as well as appraise the actions of all parties and processes which interact with the information and to determine if the actions are appropriate.

There are quite a number of security violations that take place in healthcare systems. These include unauthorized view of patients' information, unauthorized modification to patients' information, unauthorized destruction of patients' data, denial of service (DoS) attacks, eavesdropping of patient information over a network, information theft, billing for services not rendered, duplicate claims, unbundling of healthcare services, and referral kickbacks. The healthcare system is adversely affected by these security violations. Hence, the quality of patient care is reduced as health care providers' ability to diagnose and treat patients accurately may be impaired due to the unwillingness of patients to divulge necessary health information and this could have life-threatening consequences. In addition, healthcare research, public health and quality initiatives are undermined because the data in patient medical records are usually incomplete or inaccurate [24]. Furthermore, unauthorized access to patients' information can be used by malicious individuals to remotely deliver harmful treatment to patients such as the induction of high doses of insulin to a diabetic patient. In view of the security violations hampering effective healthcare services, the HIPAA (1996) security policy was established. The HIPAA security policy was established to ensure the implementation of administrative safeguards in the form of policies and personnel, physical safeguards to protect information infrastructure, and technical safeguards to monitor and control intra and inter organizational information access [25]. However, the HIPAA security policy has not been fully enforced in healthcare systems. This explains the increase in security breaches in healthcare systems. Hence, the urgent need to provide a framework that will support both privacy and security in healthcare systems. Consequently, patients' information would only be made available to authorized parties during care.

5. RELATED WORKS

A lot of works have been done on security of healthcare systems. Burgsteiner et al. [26] proposed a framework which provides secure communication for mobile e-health applications. The framework allowed users to securely connect and process medical data according to current legal regulations through a secured communication server which acts as a relay between the mobile devices and data storage. Chen et al. [27] and Blobel [28] developed role-based access control systems (RBAC) to manage a wide range of access control policies based on complex roles commonly found in healthcare organizations. However, these systems do not address patient consent. Aramudhan and Mohan [29] proposed a secured based system for exchanging sensitive patient information between multiple parties, while enforcing all required security and privacy policies along with patient consent. Khan et al. [29] used distributed multi-agent environments, where each environment consists of intelligent agents which employed handshake protocol for secured information exchange. However, this system does not address malicious agents based on the assumption that an agent's malicious activity can be detected by its corresponding environment.

6. PROPOSED FRAMEWORK

The proposed framework is as shown in Figure 2. The framework is based on two assumptions. First it is assumed that user A wishes to exchange health information (syntactic interoperability) on system A to user B on system B over a network. Second, it is also assumed that system user A wishes to use the information on system B (semantic interoperability). During the process of health information exchange, the framework adopts an intrusion detection and prevention system. The function of the intrusion detection and prevention system is to first monitor the network or systems activities for malicious activities or health information policy violations. If a malicious activity is detected, the intrusion detection system notifies the security administrators of the sending system (system A) by signalling with an alarm. Then, the intrusion prevention system resets the connection or blocks the network traffic from the suspected malicious source or shuts down the network connection.

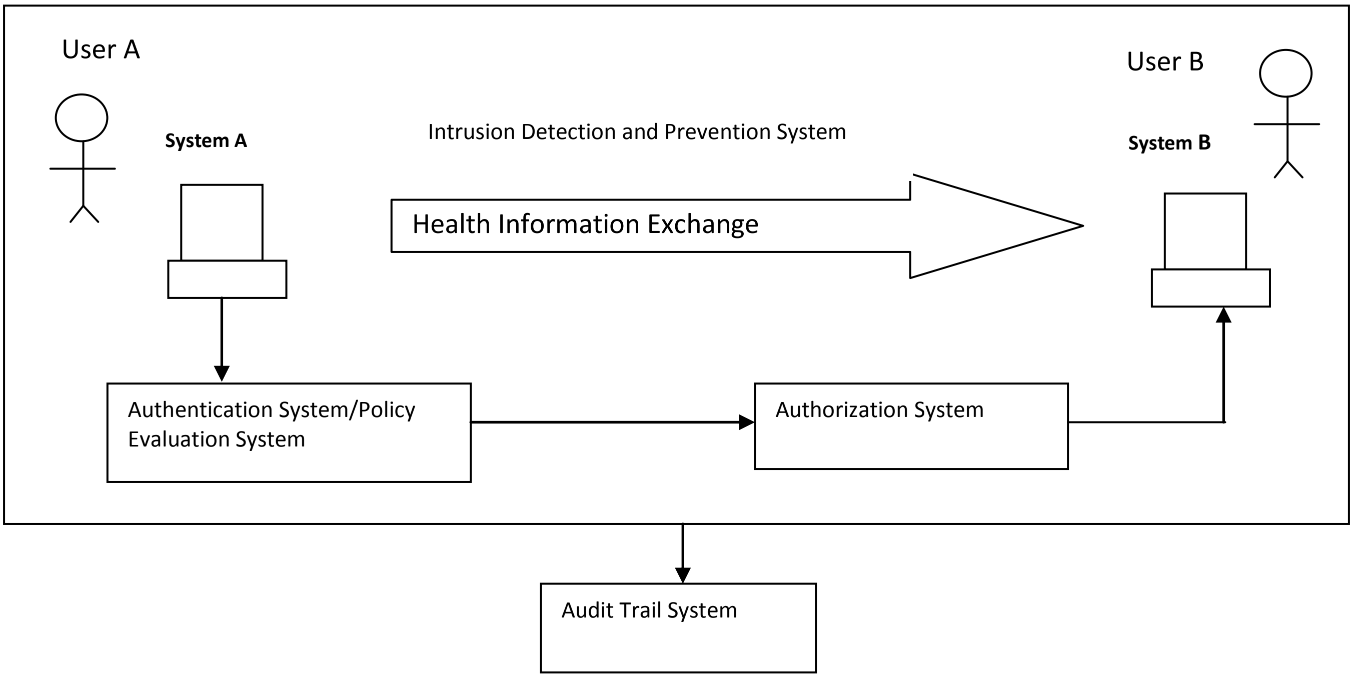
User A
User B
System A
Intrusion Detection and Prevention System
System B
Health Information Exchange
Authentication System/Policy Evaluation System
Authorization System
Audit Trail System

Fig 2. Proposed Framework

However, during information use, the proposed framework allows user A to submit its login details which includes the user id, a secret password, the Machine Access Control (MAC) address of system A, and a health data privacy policy which supports patients consent (such as HIPAA policy). Once these details are authenticated, the user is granted access on system B. Thus, the aim of the authentication system is to identify the system users as well as the system involved in the interoperation process. However, the user and the system will not be authorized to use the information on system B until the authorization process is done. The authorization system is a rule based system that is based on the concept of roles. The framework supports a user with diverse roles. The users are allowed to enter queries based on their roles, that is, their functionality and the nature of the job that they perform (such as doctors, pharmacists, radiologists etc). This will grant the users a particular view of the system, that is, the user is granted a particular view of the system based on their roles. The rules in the system determine the validity of the request made by the users. A request that cannot be verified by the system is rejected. The users are thus granted a particular view of the system B based on their roles and their compliance to the rules in the authorization system. Thus, the authorization system ensures that the right person accesses the system for appropriate use. In addition, the authorization process limits the actions the users can perform on the system. Such actions include read authorization, insert authorization, update authorization and delete authorization. The read authorization allows reading only, the insert authorization allows insertion of new data to the system only, and update authorization allows modification while delete authorization allows the deletion of data. For instance, a medical doctor accessing the system might be granted the right to read authorization insert authorization and not delete authorization. This implies that the medical doctor can read and insert new data on the system; however, the medical practitioner is not granted the right to delete records on the system. The audit trail system constantly monitors all activities that take place during information exchange and use. The audit trail system monitors who accesses the data, which data is accessed and when the data was accessed. In order words, the audit trail system constantly keeps log of all transactions in the system. Figures 3, 4 and 5 show the flowcharts that depict the activities that take place in the intrusion and prevention system, the authentication system and the authorization system respectively.

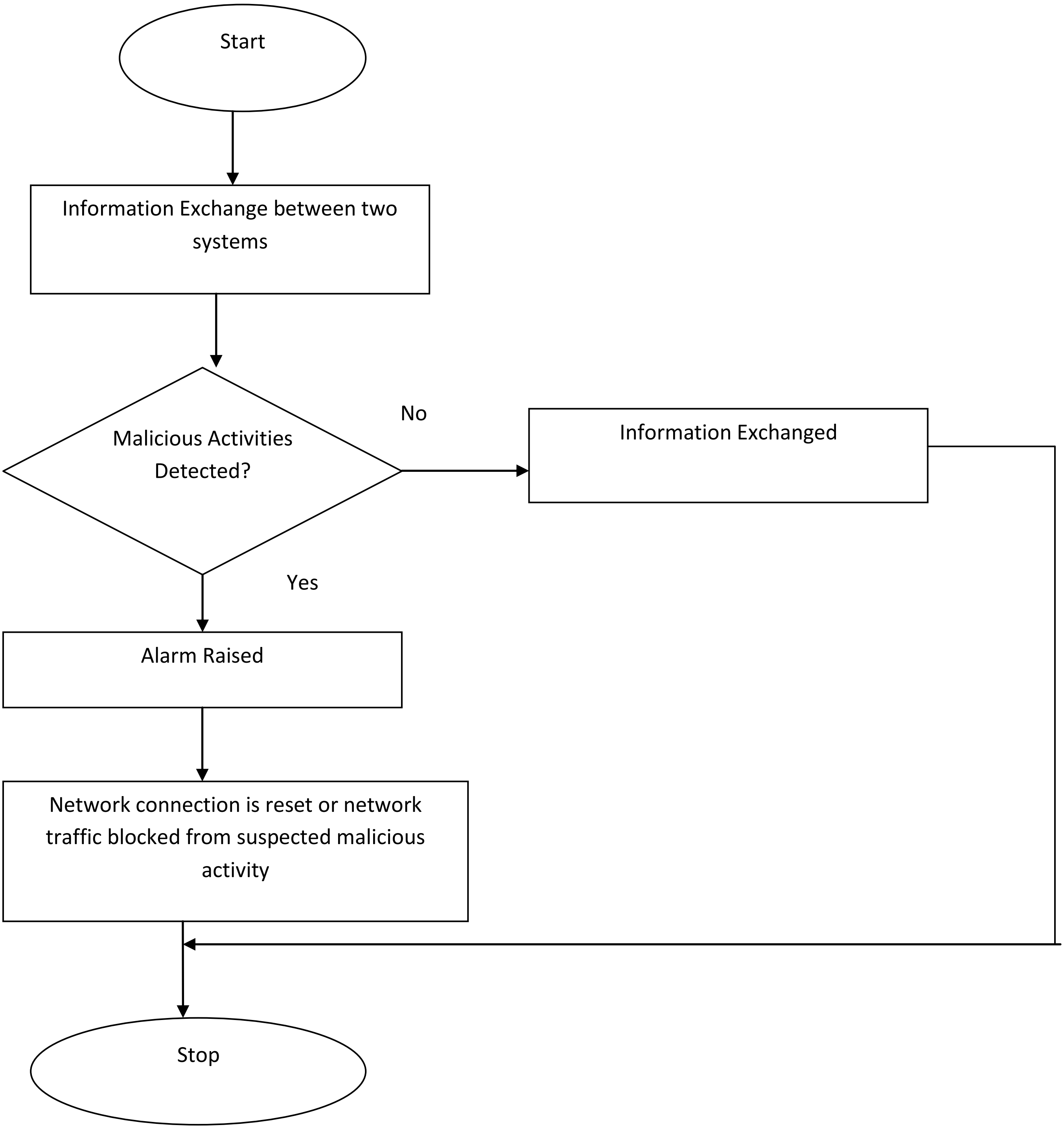
Start
Information Exchange between two systems
Malicious Activities Detected?
No
Information Exchanged
Yes
Alarm Raised
Network connection is reset or network traffic blocked from suspected malicious activity
Stop

Fig. 3: A flowchart depicting the intrusion detection and prevention activities in the proposed framework

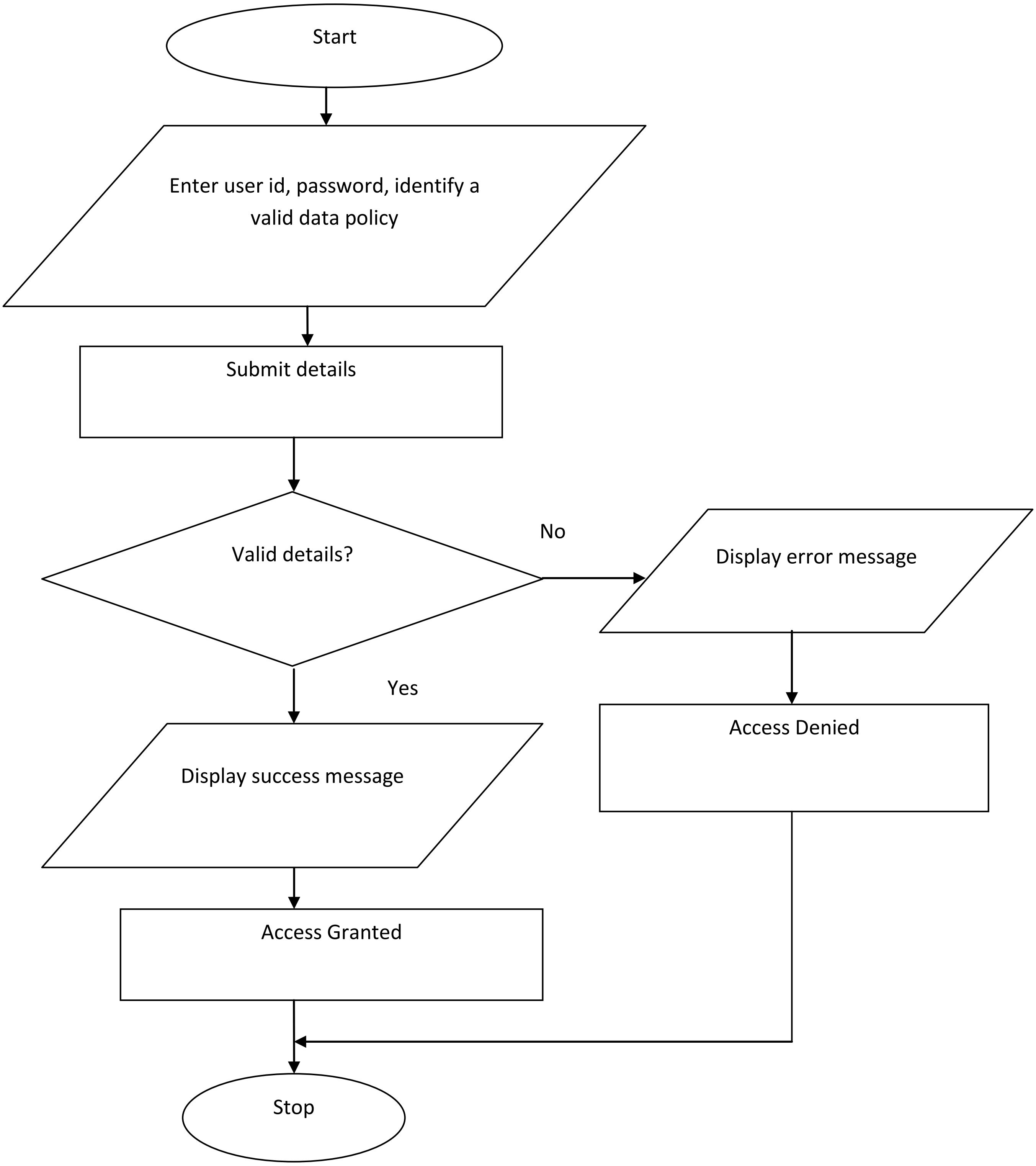

Fig.4: A flowchart depicting authentication process in the proposed framework

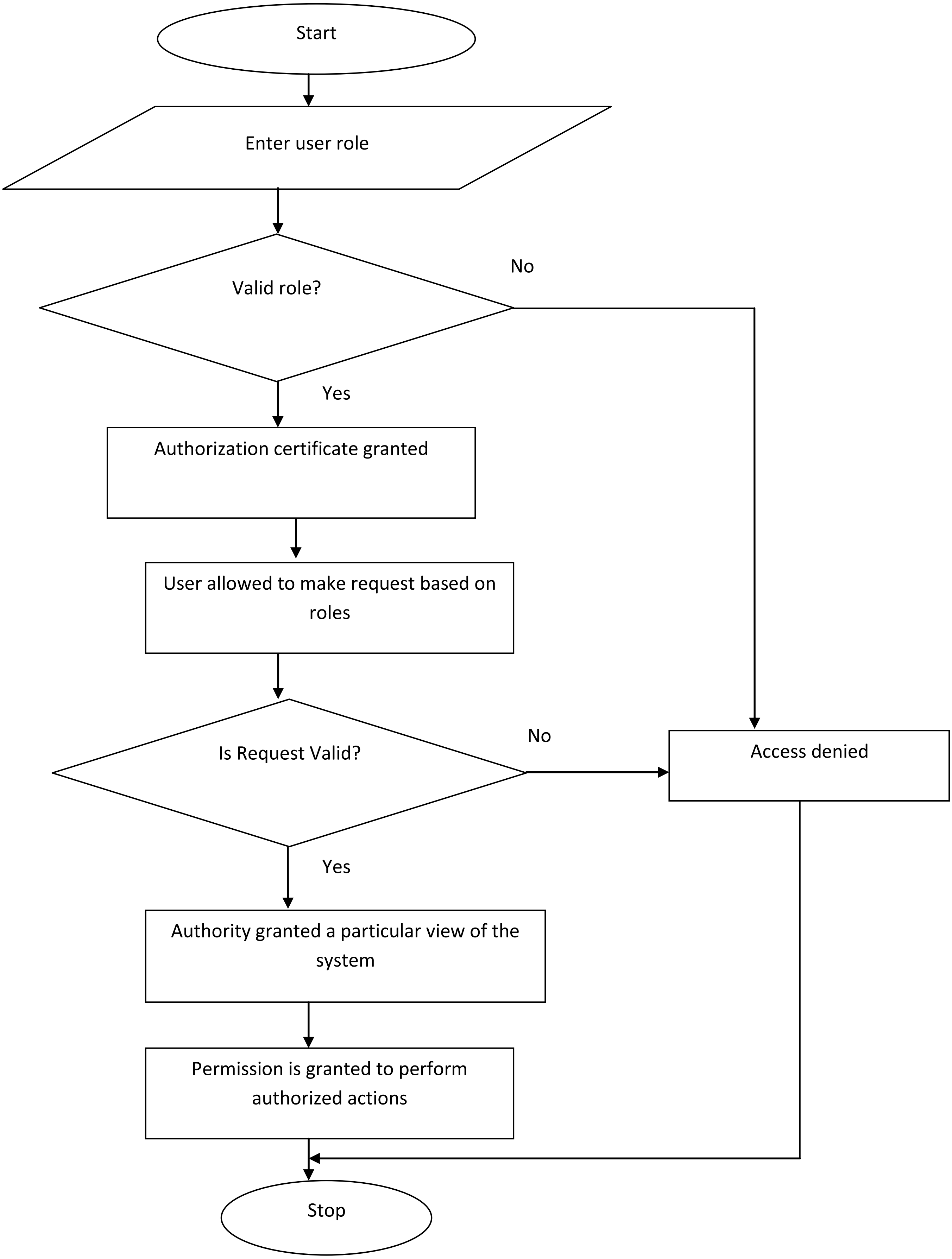
Start
Enter user role
Valid role?
No
Yes
Authorization certificate granted
User allowed to make request based on roles
Is Request Valid?
No
Access denied
Yes
Authority granted a particular view of the system
Permission is granted to perform authorized actions
Stop

Fig.5: Flowchart depicting the Authorization Activities in the Proposed Framework

7. COMPARATIVE ANALYSIS OF THE PROPOSED FRAMEWORK WITH EXISTING SYSTEMS

One of the distinctive features that distinguish the proposed framework form the existing framework is that the proposed framework takes into consideration the security of health related information during syntactic and semantic interoperability. This implies that the proposed framework considers the security of health information during the exchange of information between two or more systems and when the information is used by the users. However, existing security based interoperability systems only consider the security of health information during information use (semantic interoperability). Furthermore, the proposed system has an audit trail system which monitors the activities and transactions in the system. This is in contrast with existing interoperability systems, this is because they do not keep track of the activities that takes place within the system.

8. CONCLUSION

Interoperability is very vital within the healthcare community because it facilitates the seamless exchange of health-related information amongst caregivers and patients for clinical decision making. However, health related information are usually distributed amongst diverse heterogeneous systems. This introduces security and privacy risks such as information misuse and unauthorized access to health information to the healthcare industry. Consequently, this paper proposes a framework that mitigates both security and privacy risks in healthcare. This will in turn increase the confidentiality and integrity of patients' information, and also control access to health information.

9. REFERENCES

[1] Iroju O. Soriyan A. Gambo I. and Olaleke J. 2013. Interoperability in healthcare: benefits, challenges and resolutions. International journal of innovation and applied studies, 3 (Mar, 2013), 262-270.

[2] Moen W. E. 2001. The metadata approach to accessing government information. Government Information Quarterly, 155-165.

[3] Heubusch K. 2006. Interoperability: What it means, why it matters. Journal of AHIMA, 26-30.

[4] Yum K.K. and Drogemuller R. 2002. How much interoperability can be achieved for the construction industry today. INCITE World IT for design and construction, Hong Kong.

[5] Trans Atlantic Consumer Dialogue, 2008. Resolution on software interoperability and open standards. Trans Atlantic Consumer Dialogue, 1-6.

[6] Institute of Electrical and Electronics Engineers Standard Computer Dictionary, 1999. A Compilation of IEEE Standard Computer Glossaries, Institute of Electrical and Electronics Engineers, USA.

[7] Semantic Health Report, 2007. Semantic interoperability deployment and research roadmap. European Commission of Information Society and Media, USA.

[8] Ai, J. and Ahlfors, L. 2012. Interoperability of electronic medical records, department of informatics. Lund University.

[9] McGovern, J., Sims , O., Jain A. and Little M. 2006. Enterprise service oriented architectures, concepts challenges, recommendations. Springer.

[10] Khan W. A., Hussain M., Latif K., Afzal M., Ahmad F. and Lee. S. 2013. Process interoperability in healthcare systems,. Springer-Verlag Wien, 1-26.

[11] Cooper T. and Collman J. 2006. Managing information security and privacy in healthcare data mining state of the art. Department of Ophthalmology, Stanford University Medical School, Palo Alto, California.

[12] Renner S.A. 2001. A community of interest approach to data interoperability. Federal Database Colloquium, San Diego, 1-7.

[13] Laurinda B. H., Flite C.A., and Bond K.. 2012. Electronic health records: privacy, confidentiality, and security. American Medical Association Journal of Ethics, USA, 712-719.

[14] Ingenix white paper, 2010. Security is not privacy: why current hit provisions may fail, http://www.ingenix.com/content/attachments/Ingenix_Security-is-Not-Privacy-WhtPaper%20June%202010.pdf,.

[15] Appari, A. and Johnson, M. E. 2008. Information Security and Privacy in Healthcare: Current State of Research Center for Digital Strategies Tuck School of Business Dartmouth College, Hanover.

[16] Keckley,P.H. 2010. Privacy And Security In Health Care: A Fresh Look. Deloitte Center for Health Solutions, USA.

[17] Ponemon Institute, 2010. Preventative care, proactive response. Mission College Boulevard Santa Clara, USA.

[18] HIMSS Analytics Report, 2009. Evaluating HITECH's impact on healthcare privacy and security," Retrieved from:http://www.himssanalytics.org/docs/ID_Experts_111509.pdf.

[19] US Department of Health and Human Services. 2011. "University of California settles HIPAA privacy and security case involving UCLA Health System facilities", Retrieved from: http://www.hhs.gov/news/press/2011pres/07/20110707a.html.

[20] Bolin J.N. and Clark L.S. 2011. Avoiding charges of fraud and abuse: developing and implementing an effective compliance program, JONA, 546-550.

[21] Connors,C. L., Malloy, M. A. and Masek E. V. 2006. Enabling secure interoperability among federated national entities:it's a matter of trust. The MITRE Corporation, USA.

[22] National Institute of Standards and Technology Computer Security Division. 2012. An Introduction to Computer Security. U.S. Department of Commerce. Gaithersburg, MD, USA.

[23] Wiederhold G., Bilello M., Sarathy V., Qian M.S. 1996. A Security Mediator for Health Care Information, Health Security.

[24] Petković M., Katzenbeisser S., and Kursawe K.. 2007. Rights Management Technologies: A good choice for securing electronic health records? Securing Electronic Business Processes, 178-187.

[25] Choi Y.B,.Capitan K.E,.Krause J.S, and Streepe M.M. 2007. Challenges associated with privacy in healthcare industry: implementation of HIPAA and security rules. Journal of Medical Systems, 57–64.

[26] Burgsteiner H. and Prietl J.A. 2008. Framework for secure communication of mobile e-health.application. Medical Informatics meets eHealth, 29-30.

[27] Cheng V.S.Y., and Hung P.C.K. 2005. Towards an integrated privacy framework for HIPAA-Compliant web services. In Proceedings of IEEE International Conference on E-Commerce Technology.

[28] Blobel B. 2004. Authorization and access control for electronic health record systems. International Journal of Medical Informatics, 251-257.

[29] Aramudhan, M and Mohan, K.. 2010. New Secure Communication Protocols for Mobile E-health System. International Journal of Computer Applications,8, (October, 2008), USA, 10-15.