UACEE International Journal of Advances in Computer Science and its Applications – IJCSIA
Volume 3 : Issue 2 [ISSN 2250 – 3765]
Publication Date : 05 June 2013

Security Framework for eHealth Services: A Study

Shilpa Srivastava

***Abstract*— E-health services are subjected to same security threats as other online services. This paper emphasizes the requirement of a strong framework in e-health domain for reliable delivery of medical data over the internet. The paper recognizes current and future technological solutions in this regard. The solutions includes the authorization & authentication techniques and cryptography for the data transmission . Recent initiatives in Indian scenarios have also been analyzed. It further suggests the application of SOAP for building a secured framework.**

***Keywords—authorization and authentication,* cryptography,SOAP.**

I. Introduction

E-health - a web service oriented implementation of next generation information systems enables health care administrators members, medical professionals and patients to organize , share and access to medical services. due to the development of web technologies, security and privacy issues are rising over traditional medical services[1,2].These requirements can be met by providing health care security issues over web services. Web services should be used in such a way that timely and not too cumbersome access to health care records be provided without compromising patients privacy.

Application of information and communication technology (ICT) is a way to increase patient security. Although information security and protecting patient information has always been of high priority within the health care domain, the level of information security is still insufficient in this sector [3]. Information system security (ISS) is traditionally developed using the CIA-triad; confidentiality, integrity, and availability. These three objectives have guided the development of security measures to avoid different security threats in organizations[4].

Confidentiality means that information assets can not be accessible or revealed to unauthorized people. for example: in many cases as HIV treatment , anonymity of both the patient and the physician are required.

Shilpa Srivastava
Associate Professor ,RKGIT, Ghaziabad,
E-mail: Shri.Shilpa03@rediffmail.com

This includes anonymity of all pertinent documents and information. this is usually obtained by disassociating patient's names from the e-Health database by storing them in separate database. The data is also usually encrypted.

Confidentiality means that information assets can not be accessible or revealed to unauthorized people. for example: in many cases as HIV treatment , anonymity of both the patient and the physician are required. This includes anonymity of all pertinent documents and information. this is usually obtained by disassociating patient's names from the e-Health database by storing them in separate database. The data is also usually encrypted.

Integrity means that information assets are protected against undesired changes. An unauthorized or authorized user may deliberately or inadvertently change a patient's records. To ensure health information has not undergone any type of modification or undue delay in processing , cryptographic hash functions and hashed timestamps should be used.

The last concept, availability, means that information assets are accessible for the authorized users within the desired time. The attacker may launch a series of continual queries to flood the network which will prevent the legitimate users from having access to the system.

The purpose of identifying these issues is to create a secured architecture in the field of e-health. Section II of the paper describes the difference behavior of e-health over other online services .Section III discusses the security requirements and the existing solutions for handling the complex behavior of e-health. It shall examine the different mechanism like access control, authorization and authentication techniques, and cryptography. Section IV concludes the discussion by giving some suggestions for the further improvement .

II. Dynamic Nature Of Ehealth

The transformation of health care from human based to online services exposes e-health to the security threats as other online applications[5]. Healthcare services have different users like patients , doctors, nurses, official staff etc , and each of them have different roles to play. The confidentiality and sensitivity involved in the communication between a doctor and patient is different from the communication between a patient and pharmacist. Also while accessing that data paramedics, doctors and nurses need to access relative patients medical records, doctors who make diagnosis on patients or paramedics who prepare medical drugs would access different

medical records about a patient. To ensure the privacy of the medical data not all portions of medical data should be revealed to all the users. It is important to decide the level of sensitivity of the data. For example: a name, place and meeting time is less sensitive than the address and the type of disease the patients is suffering from which is more sensitive. According to the level of sensitivity we can categorize the different communication into different layers[6].

The whole communication has been divided into five different layers according to their sensitivity as depicted in table 1. the security requirement is different for different layers. The dynamic nature of e-health can also be explained by analyzing different situations like a patient visits his family doctor for a regular medical checkup.

TABLE1 Communication in e-Health

Layers	Sensitivity of the data	Requirement
1	Extremely Sensitive (personal information, medical history etc.) Doctor to Doctor Doctor to Patient Doctor to Nurse Nurse to Patient	Highest Security and fastest speed
2	Highly sensitive (medical information, allergy, BP etc) Paramedic to System Coordinator	second high security and second fast speed.
3	Medium sensitive (medication information) Doctor to Social Worker/NGO	high security and fast speed but less strict that layer 2.
4	low sensitive data (user account information, Non medical data) System Administrator to All users	security only, often speed is less concerned.
5	No sensitive data (general information) The Public	focus on speed more than security.

This can happen in doctor's clinic periodically ;but in emergency situation(like accident) the patient must be admitted for immediate action. In [7] these situations are categorized into normal, abnormal and critical situations:

Normal: A patient visits his/her family doc for regular check up.

Abnormal: A patient is expected to meet a substitute doctor when his/her family doc is out of town.

Critical: A patient is admitted to the emergency department of a hospital when he/she travels out of town and a hospital surgeon is needed to work immediately.

The two issues sensitivity in the communication and different situation existing in the way of e-health makes it different from the other online applications. For handling the dynamic behavior of e-Health some solutions have been analyzed in the next section.

III. Security Requirements

To provide sufficient security online two major aspects will be focused in this paper.

- E-health data transmission and
- E-health service authentication.

A. *E-health data transmission*

E-health data transmission can be divided into two parts: a)data security and b)channel security[7]. According to the different types of communication discussed above data or channel or both are required to secure the communication.

In our consideration[7] e-health is viewed as a web service. Web service is a method of communication between two devices over the web. It can also be defined as a software system designed to support interoperable machine to machine interaction over a network. It has an interface described in a machine process able format specifically WSDL. Other systems interact with the web service in a manner prescribed by its description using SOAP messages.[8].

Big web services use XML messages that follow SOAP standard.XML is a markup language that defines a set of rules for encoding documents in a format that is both human readable and machine readable. It is a textual data format with strong support via Unicode for the different languages. It can also be employed as a base language for communication protocol HTTPS(combination of HTTP and SSL/TLS protocol) for providing encrypted communication and secure identification of a network web server. So data security can be applied in the XML document by encrypting/decrypting and signing the document from the sender's machine , transmitting it over the network and decrypting it back at the recipient machine. In web services architecture data in XML document is sent as SOAP messages. SOAP is an application layer protocol, thus it naturally can work on top of any transport (network) layers below the application layer. In practice it is possible to lay SOAP directly on top of TCP/IP and open a direct socket connection between applications. However the problem lies in the fact that direct socket connection is platform dependent. By applying SOAP on top of HTTP ,language and platform both independencies can be achieved, which shall provide wide deployment of health services[7].

The advantages of using SOAP protocols are:

- SOAP is a versatile enough to allow for the use of different transport protocols. The standard stack use HTTP as a transport , but other protocols such as JMS and SMTP are also usable.
- SOAP model tunnels fine in HTTP get / response model , it can tunnel easily over existing firewalls and proxies, without modifications to the SOAP protocol and Can use existing infrastructure.

Channel security involves point to point encryption from a sender's point to recipient's end , such as SSL/TSL that uses HTTP protocol. HTTPS is a URI scheme which has identical syntax to the standard HTTP scheme. HTTPS signals the browser to use an added encryption layer of SSL/TSL to protect the traffic .SSL is especially suited for HTTP since it can provide some protection even if only one side of the communication is authenticated. This is the case with HTTP transactions over the internet, where typically only the server is authenticated(by the client examining the server's certificate). The fig 1 illustrates the framework for e-health service[7].

Web Service (Ehealth Service)	Application Layer
XML Message (Data Security)	
SOAP	
HTTPS(SSL+TSL) (Channel Security)	
TCP	Transport Layer
IP	Internet Layer

Fig 1: E-Health Service

The main idea of HTTPS is to create a secure channel over an insecure network. This ensures reasonable protection from eavesdroppers and man in the middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted[8].

B. *Cryptosystem Requirement*

Cryptography has been highlighted as a main factor in developing a system that share and transmit health information, besides access control and secure network protocols[9].For providing data security and channel security we require encryption algorithms suitable in the e-health environment. In literature many studies have been conducted to secure online communication in sharing medical data.

SECURE talk[10]was a system used secure the storing , processing and transmitting medical data using encryption, decryption and digital signature. In[11] medical data was classified at local level ,regional level or cross border level. Higher security measurements were given at the cross level compared to the local level and regional level. In this research all data were treated the same for all users in the particular level. In another research [12].The author has evaluated security mechanisms in three layers: application, transport and network layer of the OSI reference model. In application layer asymmetrical and symmetric cryptographic systems are used for data encryption ,digital signature and digital envelope . is used to establish secure channel between two nodes, and asymmetric cryptographic for authentications. The network layer includes security mechanisms in communication devices and firewalls and operating system such as Virtual Private Network and IPsec.

The researches stated above are providing security to the communication and data transmission, but they are not viewing the communication from the prospects of e-health. These approaches view all the communications between the users same and hence all communication will be secured by the same security processes. Different encryption algorithms are required for handling data with different level of importance.

C. *.Authorization and Authentication Techniques*

Health care services has a dynamic behavior. Access control mechanism are enabled at the OS level as well as higher levels. The level of granularity that applies at the OS level is aimed at the needs at that level for larger identified system components: data and executable programming files, input/output devices , network components, software processes, threads etc[13].The three most widely recognized models of access control are Discretionary Access control(DAC),Mandatory Access control(MAC and Role based access control(RBAC)

DAC is an access policy determined by the owner of an object. The owner decides who is allowed to access the object and what privileges they have.

Mandatory access control refers to allowing access to a resource if and only if rules exist that allow a given user to access the resource. It is difficult to manage but its use is usually justified when used to protect highly sensitive information. It was originally designed to meet confidentiality requirements of military systems, enforcing security policy as set out by the overall enterprise and not set up by definition provided by file/program "owners". For general applications, currently available products that support MAC principles of a trusted OS include "Red Hat enterprise Linux(RHEL) version 6","Fedora Core 18" and Sun Microsystems Solaris 10 with trusted Extensions Software".

RBAC refined the concept to allow for users to be grouped into defined functions or "roles" allowing for far easier management of overall security policy particularly in dynamic business environments.

These access control mechanism are too rigid for capturing the dynamic behavior of health care applications. Such mechanism fail in providing the appropriate flexibility that is necessary when dealing with unexpected situations. for example: a doctor that asks for the second opinion of another doctor who is in-charge of another ward , since the doctor is assigned to a different ward he may not be permitted to access the patient in order to provide an opinion.. The main drawback of current access control mechanism is that the granting of access rights require statically binding a subject (ie a doctor) to a target(i.e. a patient's medical record) where the subject and the target must be known in advance[14],in the exceptional conditions access to resources should be allowed to unauthorized entities. When an exceptional access is made ,

such an event must be logged for future analysis. Log analysis can be used for identifying whether the exceptional mechanism is misused. In a study[15] , in most cases the information provided in the logs is not sufficient for correctly identifying situations where the mechanism was misused.
From the above discussion we can say that access control includes two primary aspects
1. To deny access to health care data to those users who do not have the right of access.
2. They need to guarantee access to all relevant data to those database users who exercise their privilege properly.
Most of the existing research proposals that study authorization and authentication have separated the function of authorization and authentication in terms of access control and identify management, for example, in the security analysis of Microsoft .NET passort (Oppliger,2003) the authentication approach has been utilized as the main access control principle; while the others, for example. Zhang et al.(2003) studied authorization approach as the main access control principle. In some cases authorization is based on the result of authentication. if the result of authentication is negative/positive then the result of authorization is negative/positive. But this principle is not practical in e-health environment[16]. There is no consideration of mutual and sequential impact of authorization and authentication in terms of access control and identity management. In this regard some solutions have been suggested.
In [16] the authors have proposed an architecture for authorization and authentication for e-health services. This system integrated the role based method[17] and the attribute certificate(or privilege)based method[18,19] to better suit to the e-health service system. Although design and implementation has been not provided.
The authors of [7] have proposed two risk adaptive methodologies applicable for different situations(normal , abnormal & critical) discussed above.

1.Ehealth multifactor Authentication joint with RBAC to handle normal and abnormal situation. the doctors are required to provide a single piece of information to confirm their identity in normal situations, and multiple piece of information in abnormal situations, respectively.
2.Mutual Authentication to handle critical situations is a two way authentication where two parties authenticate each other in such a way that both parties authenticate each other in such a way that both parties are assured of the others' identity. The implementation has not been provided yet. Figure 2 defines different techniques to handle the situation in health.

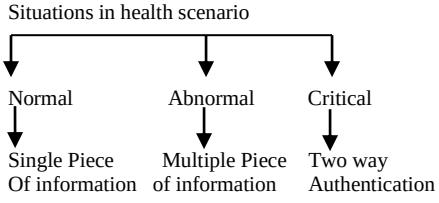

Fig 2

In another approach[14] a workflow access control framework is proposed to provide more flexibility in handling e-health dynamic behavior. The idea is to model each work task in the system as state machines. at each state , the data access permission is granted based on the resources required to move on to the next state. For any entities involved, the information of all states statuses are stored in the lookup table to improve processing speed. However this approach consumes a large amount of memory space since an entity must store a copy of the status of all states .

The goal of e-health services is to give a low cost and high quality system. If the access control mechanism is too restrictive then it could become a burden for the medical staff that have to use it whereas if access control is too loose protection of information and resources can cont guaranteed, so a precise access control mechanism is required that is able to deal with the level of unpredictability involved in healthcare applications.

IV. E-Health In Indian Context

India is a vast country with a population of more than 1.2 billion people, the second most populous country in the world, consisting of 29 states and six union territories. Health is the primary responsibility of each state and there is paucity of infrastructure and dearth of doctors in rural areas. Besides, there is no national health insurance policy for the country. Efforts are directed towards setting up standards and IT enabled healthcare infrastructure in the country but there are many challenges involved in its implementation. Out of many challenges like education, poverty, financial resources, secured data management is also of primary concern. Poor data management is one of the major problems in the developing countries which lead to breaches in data security and therefore it is considered as one of the major deterrents to the large scale adoption of e-health [3]. As a result government, administrative bodies and the different players in the health service system are looking for innovative solutions to make health services most efficient and secure. One of the most important initiative being taken is standardization of exchange of health information between different entities within the healthcare sector. In this regard the ministry of health & family welfare and the ministry of communication and information technology are jointly creating a national health information infrastructure for easy capture and dissemination of health information [20]. The center shall soon establish a national database for the medical records of all the citizens from birth to death that will come out with the launch of a National Health Portal [21]. Efforts are being made [22] to use “Aadhaar” card as authentication for electronic medical records. Some of the recent works show that hospitals like ‘Apollo’ [23] are in the process of implementing in their own chains of hospitals.

v .Conclusion And Future Work

The paper highlights the security related issues in the implementation of e-health. Because of the dynamic nature of e-health the traditional techniques of handling vulnerabilities in the online applications are just not sufficient. Some aspects of it have been discussed in this paper. The security framework for e-health data transmission has been analyzed. It is considered that the application of SOAP protocol preferable over the transport protocol HTTPS for creating a secure channel in the network. Further the paper investigated the various access control mechanism for data authentication since classical access control mechanism are so rigid to capture e-health environment. The security requirements for low cost and high quality e-health services have been examined. It includes

1. The use of platform and language independent application for the wide deployment of secured e-health services on top of SOAP.
2. The analysis of the relationship between authorization and authentication between authorization and authentication from e-health perspective, mutual and sequential impact of authorization and authentication in terms of access control and identity management have to be considered.
3. The analysis of different encryption algorithm at different communication levels according to the sensitivity involved in the communication.

In future it is proposed to build a prototype for delivering a secured e-health services which will be an improvement over the existing solutions.

References

[1]Smith E. Eloff JHP,1999," Security in health- care information systems-current trends", International Journal of Medical Informatics,54:39-54.

[2] Agarwal R.Kini A, LeFevre K,Wang A Xu Y and Zhou D,2004," Managing Healthcare Data Hippocratically". Proc. of ACM SIGMOD Intl. Conference on Management of Data.

[3] Dr. Anuradha Srivastava, May 2011,"E-Health in Developing countries: Pitfalls, Challenges and possibilities "http://www.ehealthmagazine.com.

[4] S. Dritas, L. Gymnopoulos, M.Karyda,T.Balopoulos,S.Kokolakis, C .L ambrinoudakis, S .K.Katsikas," A knowledge-based approach to security requirements for e-health applications", The electronic journal for E-Commerce Tools & Applications(eJETA), Special issue on Emerging Security Paradigms in the knowledge Era,October 2006.

[5]Apaporn Boonyarattaphan, Yan Bai, Sam Chung and Radha Poovendran,15-17 July 2010," Spatial - Temporal Access Control for e-Health Services." Fifth International Conference on Networking , Architecture and storage.pp.269 – 276.

[6]Apaporn Boonyarattaphan,Yan Bai, Sam Chung, 28-30 Sept.2009," A security framework for e-health service authentication and e-health data transmission",9th International Symposium on Communications and Information Technology.ISCIT 2009.pp1212-1218,

[7]R. Sulaiman, D. Sharma,W. Ma, D. Tran, February 2008, " A security Archtecture for ehealth services, " the 10th International conference on advanced communication Technology, Korea, Vol.2,pp.999 - 1004,

[8] http://www.w3.org/TR/2004/NOTE-ws-gloss-20040211/

[9]Bleumer, G.,1994, Security of decentralized health information systems.International Journal of Biomedical Computing, 139-145.

[10]Tulu, B., & Chatterjee, S.,2003, A new security frameworkfor hippa Compliant health information systems.Paper presented at the proceedings of Ninth Americas Conference on Information Systems, Tampa, FL.

[11]Gupta, V., & Gupta, S,2001, Kissl:Experiments in wireless internet security: TR-2001-103, Sun Microsystems laboratories, of Sun Microsystems, Inc.

[12]Doupi, P., & Ruotsalainen,P. Pohjonen, H ,2005," Implementing interoperable secure health information systems",Stud Health Technol Inform, 115,187-214.

[13]V. Liu, W. Caelli, L.May, P.Croll, January 2008,"Open Trusted Health Informatics Structure(OTHIS)," Proc. of the 2ndAustralasian Workshop on Health Data Knowledge Management, Vol. 80, pp.33-43.

[14]G. Russello C. Dong, N. Dulay, March 2008," A Workflow based control framework for ehealth applications," proc. of the 22nd International conference on advanced information networking and applications- workshops pp111-120.

[15] L. Rostad and O. Edsberg, December 2006, " A Study of Access Control Requirements for Healthcare Systems Based on Audit Trails from Access Logs." In Proc. of 22nd Annual Computer Security Applications Conference, Miami, Florida,

[16]Song Han, Geoff.Skinner,Vidyasagar.Potdar, Elizabeth.Chang,2004,"A Framework of Authentication and Authorization for e-Health Services", Proceedings of the UK e-Science All Hands Conference 2004 website: http://www.allhands.org.uk/2004/,pp934–937.

[17]Hitchens M, Varadharajan V,2000, Design and specification of role base access control policies. IEE proceedings in software, 47(4):117-129.

[18]Blobel B. Nerdberg R, Davis JM, Phraw P,2006, Modelling privilege management and access control, International Journal of Medical Informatics, 75:597-6231.

[19] Jajodia S, Kudo M, subrahmanian VS,2001 Provisional authorizations.In:Gosh A(ed) E-Commerce security and privacy,133-59.

[20]Dr.S.K. Mishra,"Ehealth initiatives in India", http://openmed.nic.in/1265/01/skm12.pdf

[21]http://ehealth.eletsonline.com/2011/06/national-health-portal-for-india/

[22]**GpCapt (Dr)Sanjeev Sood,2012,** http://ehealth.eletsonline.com/2012/01/aadhaar-opening-up-of-new-vistas-in-healthcare-gp-capt-dr-sanjeev-sood-hospital-administrator-and-nabh-empanelled-assessor/

[23]Shweta Kannan, February 2013, "http://www.thehindubusinessonline.com/companies/apollo-hospitals-working-on-linking-ehealth-records-with-Aadhaar

Shilpa Srivastava
Associate Professor,
RKGIT,
Ghaziabad

The goal of e-health services is to give a low cost and high quality system. The two issues sensitivity in the communication and different situation existing in the way of e-health makes it different from the other online applications. so a precise access control mechanism is required that is able to deal with the level of unpredictability involved in healthcare applications.