INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 5, ISSUE 3, MARCH-2014
ISSN 2229-5518

Enhancing Security in Service Oriented Architecture driven EAI using Aspect Oriented Programming in healthcare IT

Neha Sharma, Usha Batra, Saurabh Mukherjee

Abstract— Information security and privacy in healthcare IT have been a longstanding challenge in recent years. Technologies like data mining, private database, Role based access control, encryption etc. attain the goal at some extent but don't provide a solution to resolve every aspect. Considering the extremely sensitive nature of medical records, in any attempt to transmit the data over the network; we need to make sure that any third party cryptanalyst can't be able to access, modify or even understand the encrypted document sent over the network. This growing privacy and security needs in electronic-health records is the motivation for our approach. In this paper, we propose an approach for integration and exchange of medical records over the network in a service oriented driven framework using HL7 standard that provides an end-to-end security.

Index Terms— Aspect oriented programming, Electronic Health Record, Enterprise Architecture Integration, Hash, HL7, Message Digest Code, and Service Oriented Architecture.

1 INTRODUCTION

Over the past few years, the development of technology has led most of the developers and vendors to change their approach to hetrogeneous environment. The main purpose is to achieve a single system that can interact with heterogeneous systems with different devices at different locations over different networks with varied quality-of-service requirements.

Healthcare is one of the most important matters in human societies, as the life quality of people depends on it directly making it a wide area for research. A literature survey reveals that medical data sent electronically i.e. electronic health records (EHR) are more efficient and cheaper than the classical paper-based Health records. However, as William J. Clinton implied in 1999, "As more of our medical data are stored electronically, the threats to all our privacy increase [1]". The three major ethical priorities for EHRs i.e. privacy, confidentiality and security [1] are the major concern for our research work and their need in e-health motivated us to apply different standards, protocols and technologies to create a Hospital Management System Framework that will provide security at different level of communication and cover as many security aspects per se privacy, authentication, integration, confidentiality etc. as possible. To achieve this goal, an algorithm is developed that transmit the medical data over the network while preserving the privacy of information with the help of Hashing with encryption/decryption instead of classical cryptosystem. To provide a standard vocabulary between two hospitals, HL7 standard is required. However, various issues like inappropriate incorporation with non-HL7 standards, use of complex tools and incompatibility with previous versions makes it sometimes inappropriate and difficult to adopt[2]. Therefore, Wrapped HL7 [3] will be used in our implementation to maintain communication security. Aspect Oriented Programming (AOP) will allow us to design a security agent which will be used for hashing and encryption/decryption as an aspect and enable it to be used as a plug-in for other systems and make it easier to design and use by providing modularity.

One of the largest challenges in using encryption based communication is the distribution of shared key. In our approach by using the hash generated secret key, we eliminate the need to share the key and instead generate it at both side with the help a hash function. However, for now, this paper only focuses on the algorithm that is proposed to achieve the intended goal. The rest of the paper is organized as follows: Section 2 describes the background and related work. In section 3, the problem statement is defined followed by proposed approach in section 4. Section 5 explains the framework architecture and algorithm along with the security analysis of the proposed work. Finally, section 6 contains the conclusion and future work of the research work.

2 RELATED WORK

This paper mainly focuses on enhancing security by analysing different aspects of security and proposes a framework model that will provide an end-to-end security during transmission of medical records. In 2006, Marci et al [4] proposed an explorative research on privacy and security implications of health care technologies. Since then, variant research work have been done in different security and privacy approach. Recently, many encryption-based techniques have been proposed for secure sharing of medical information.

Agrawal et al[5] proposed a set of protocols that disclosed minimal information during information sharing across private databases. A similar approach is proposed by Adam et al[6] for privacy preserving Integration of health care data. They proposed an approach for integration and querying of medical

- *Neha Sharma is currently pursuing master's degree program in computer science and engineering in ITM University, Gurgaon, Haryana, India, PH-9654038571. E-mail: neha.sh1991@gmail.com*
- *Usha Batra is currently working as assistant professor in department of computer science and engineering in ITM University, Gurgaon, Haryana, India, PH-9811973824. E-mail: batrausha@rediffmail.com.*
- *Dr. Saurabh Mukherjee is currently working as associate professor in department of computer science and engineering, Banasthali University, Rajasthan, India, PH-7742114404. E-mail: mukhejee.saurabh@rediffmail.com.*

data from multiple sources in a secure manner. Zhang et al [7] also proposed sharing and integration in healthcare clouds and analysing the arising security issues in management of electronic health records (EHR). They took a methodological step to investigate security requirements and proposed an EHR reference model for managing these issues in healthcare clouds. Therefore, focusing on different security aspects, various models and techniques have been proposed in healthcare IT.

3 PROBLEM DEFINITION

Security is a very important concern when information or data within organization is exchanged, especially when it comes to hospital information. We are considering a distributed environment with hetrogeneous distribution of data and aim to analyse the security in healthcare integration. The security in health integration is not a business concern but rather a cross cutting concern which spams over all business concerns so Aspect oriented programming is a good choice for effectively and efficiently dealing with such cross cutting concerns. Aspect oriented programming (AOP) includes programming methods and tools that aims to separate these cross cutting concerns [8] by increasing modularity. The hospital integration system for which we will be working to enhance security will be HL7 aware. Therefore, the problem identified is :"Enhancing Security in Service Oriented Architecture driven EAI using Aspect Oriented Programming". Due to certain flaws in HL7 standard that are already discussed in previous section, we will use wrapped HL7 (by securing HL7 lower layer protocols based on socket interface).

4 PROPOSED APPROACH

The general process of encryption/decryption for any secure communication between endpoints doesn't ensure the integrity and authentication of a message. In our approach we will employ a security agent that will ensure these two aspects of security by using a hash generated symmetric key to cipher the plain document which is to be sent over the network.

4.1 Input: The Hospital Id (Hid) is the unique id which is provided to every hospital during the registration for the first time. Once generated, the same id will be used by respective hospital for future communication. Whenever the patient requests for his/her medical information to be send over a network he/she will provide his/her Adhaar Card number which will act as the patient id (Puid) and will ensure that the hospital is using the patient's information by his/her permission. Along with these two variables, a special character will also be added on which both parties have already agreed upon.

4.2 Security Agent: The wrapped HL7 message will act as the plain input which needs to be encrypted and decrypted at respective sender and receiver side. Our main focus is to generate the key by using the hash method as follows:-

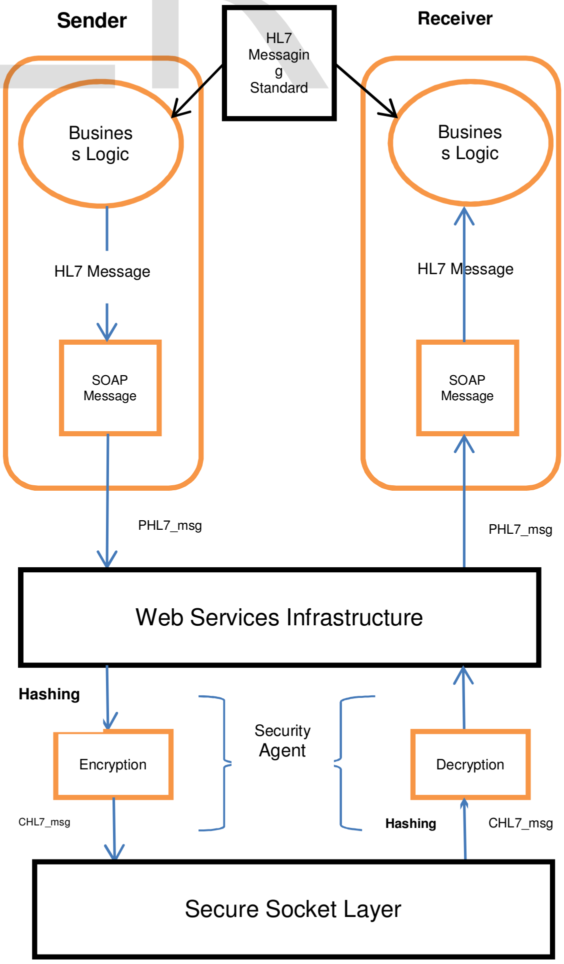
1. Take the Salt variable generated from input. This salt will be a combination of Hospital Id, Adhar number of Patient and a special character already decided between both parties. It will ensure that the hash code more complex than the classical method and will add an extra level of security i.e. Salt = Hid+Puid+SC.
2. Apply hash function to this Salt+HashData. A message digest code will be generated.
3. This Message Digest Code will act as a key to Encrypt and Decrypt the HL7 message and will ensure the integrity and authenticity of message by acting as a message digest code to be matched at other side.

4.3 Output: The message digest code which is created through hash function and the encrypted document are finally sent over the SSL [9] to the intended receiver hospital. At receiver side this cryptic document is decrypted to get the original message along with a new message digest code. If both MDCs matches, the document is accepted else it is rejected.

5 Proposed Algorithm

The Hash functions are fast to create and hard to reverse (due to how they are iterated internally) and therefore is a perfect candidate to obtain a secure symmetric key eliminating the problem for key distribution. Decoding a MD5 hash algorithm nearly require infinite amount of resources making the hashing code almost impossible to reverse. Therefore, by using this approach we are ensuring the validity and integrity of our medical information.

5.1 Framework Architecture and Pseudo code



Encryption at Client Side

```
Encryption(PHL7_msg,Hid, Puid)
{
Call Hms_hash(hid,puid)
CHL7_msg ← $E_{Hkey}$(PHL7_msg)
Return CHL7_msg
}
```

Decryption at Server Side

```
Decryption(CHL7_msg,hid,puid)
{
Call IsAuthentic()
Call Hms_hash(hid,puid)

PHL7_msg ← $D_{Hkey}$(CHL7_msg)
Return PHL7_msg
}
```

On both side two different functions are called

```
public class HmsHash
        {
  public static void main(String[] args)
         {
String userID = "testuser123";
String password = "pass1234";
String hashdata = HMS_hash (password);

If(IsAuthetic(hashdata, userID))
{
System.out.println("User Authenticated ");
}
Else
{
System.out.println("User Denied ");
}
}

public static String HMS_hash(String hashdata)
{
String hash = null;
String salt = Hid+Puid+"$SaltValue$*";
hashdata = hashdata + salt;
try {
MessageDigest objdigest = MessageDigest.getInstance("MD5");
objdigest.update(hashdata.getBytes(), 0, hashdata.length());
hash = objdigest.digest().toString();
}
catch (Exception e)
{ }
return hash;
 }
}

public static bool IsAuthetic(String hashdata , string userID)
{
Check if message digest code matches
If yes
Return true;
Else
Return false;
}
```

Class HmsHash is to authenticate the user and return Hash Value. This class will become part of authentication Webservice and will be called using web methods. HMS_hash() is static method which takes hashdata typically consisting of username and password along with any other information to identify the hospital. Hash of this string will be created in normal mode and returned back. In our implementation Salt will be added to this Hashdata string. Inauthentic() method will verify currently generated Hash from previous method and validate it with HASH value received from sender.

5.2 Encryption and Decryption

The document intended to be sent over the network is too large to be encrypted as whole. Therefore, the document will be divided in two segments according to the HL7 specification [10]:-

1. Patient Identification (PI) Segment
2. Details Segment

The PI segment is the only part that is encrypted using the secret key obtained by security agent and the same is decrypted at other side. The HL7 specification provides 30 different fields to provide identification information [11] of patient out of which only a few fields will be used in our approach (according to the requirement). As the PI segment is encrypted, the details segment needs not to be encrypted. The triple Data Encryption Standard/ Advance Encryption Standard will be used to complete the task.

5.3 Data Source

The data source used in our approach is XML-database. After a thorough survey, we believe that it can facilitate our research needs by providing a standard way. XML database is considered as a best choice if we need to export or transfer data between applications in a secure manner[12]. However, the proposed algorithm is made flexible enough to use another database if need arises.

As the framework is a service oriented architecture [13], XML-database is a good choice considering their compatibility. Also, perks like simplicity, extensibility, self-descriptive, multi lingual support and one-service-view presentation makes XML-database a good candidate according to our requirement. Most of the companies are adopting XML-database due these features and modern approach.

5.4 Security Analysis

As security being the focus of our research, through our approach we need to ensure that maximum level of security is provided. After analysing the algorithm, we can conclude that an end to end security has been achieved that can be justified by follows:-

1. The Service Oriented Architecture and use of web service standards like WS-Security, SAML, WS-Trust, XML gateway ensure and focus on the identification and security aspects during implementation.
2. Hashing creates the message digest code and key that focuses on integrity and Authentication aspects to ensure security of patient's medical data.
3. The crypt message generated after the cryptography process is sent over the network using Secure Socket Layer (SSL) which is initially and solely developed for transmitting private documents over the network providing the architecture another level of security.
4. Features like XML signature and XML encryption makes XML database a good choice for secure transfer and communication.[14]

Therefore, we can conclude that most of the aspects of security including privacy, integrity, confidentiality, authenticity, transmission etc. have been achieved by our approach.

6 Conclusion

In this paper, we propose an approach that allows an end-to-end security for transmission of a medical record among hospitals. The proposed approach employs a cryptography based solution that uses a secret key and message digest code generated through hash function to provide better results in contrast to the classical approach. This approach lessens key distribution overhead, ensures integrity, authenticity and confidentiality of the medical records and therefore qualifies. The encryption prevents any third party to access any sensitive data from extraction. As the key can't be generated without the Adhaar card number of patient, it ensures identification of intended client.

The successful demonstration of this approach could help achieve the primary goal to enhance security in a service oriented hospital management system. For future work, a framework is to be developed that will process this approach and after testing the results, a comparative analysis will be made with the existing system and based upon that we will examine if the proposed approach is efficient.

7 References

[1] Laurinda B. Harman, Cathy A. Flite, and Kesa Bond, "Electronic Health Records: Privacy, Confidentiality, and Security", State of the Art and Science, *Virtual Mentor.* September 2012, Volume 14, Number 9: 712-719.

[2] HL7, "Swot – To Provide Input For Roadmap", http://www.hl7.org/documentcenter, HL7 Meeting San Diego, September 2011.

[3] Bernd Blobel, "Standard Guide for EDI (HL7) communication Security", Otto-von-Guericke University Magdeburg, 2009.

[4] Marci Meingast, Tanya Roosta, Shankar Sastry, " Security and Privacy Issues with Health Care Information Technology", Proceedings of the 28th IEEE EMBS Annual International Conference New York City, USA, Sept. 2006.

[5] Rakesh Agrawal, Alexandre Evfimievski, Ramakrishnan Srikant, "Information Sharing Across Private Databases", IBM Almaden Research Center, proceeding of ACM SIGMOD international conference on management of data, pp. 86-97, 2003.

[6] Nabil Adam, Tom White, Basit Shafiq, Jaideep Vaidya, "Privacy Preserving Integration of Health Care Data", Rutgers University, 2NY Office of Mental Health & Columbia University, NYC.

[7] Rui Zhang, Ling Liu, "Security Models and Requirements for Healthcare Application Clouds", College of Computing, Georgia Institute of Technology, Atlanta, Beijing Jiaotong University, Beijing, China.

[8] Aspect-Oriented Programming for a Distributed Framework, Department of Computer Science, University of Pretoria, Pretoria 0002, South Africa.

[9] Pradeep Kumar Panwar, Mr. Devendra Kumar, "Security through SSL", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, issue 12, December 2012.

[10] HL7 ORU – HL7 Result Message, http://www.corepointhealth.com/resource-center/hl7-resources/hl7-oru-message.

[11] HL7 PID(Patient Identification) Segment, http://www.corepointhealth.com/resource-center/hl7-resources/hl7-pid-segment.

[12] Stephen B. Johnson, David A. Campbell, Michael Krathammer, "A Native XML database design for clinical document Research", AMIA Annu Symp Proc. 2003.

[13] Peter Classon, Jatinder Prem, "SOA: Integrating XML and Web Services, A primer in Web Services and XML (Extensible Markup Language)", www.liquidhub.com/docs/Horizons_WSXML_primer_v3.

[14] Claudio A. Ardagna, Ernesto Damiani, Sabrina De Capitani di Vimercati, and Pierangela Samarati, "XML Security", Security, Privacy and Trust in Modern data Management, Spinger XVIII, 2007.