ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 8(21), DOI: 10.17485/ijst/2015/v8i21/60739, September 2015 ISSN (Online) : 0974-5645

Study of Cryptographic Algorithms to Protect Electronic Medical Records in Mobile Platforms

Jorge E. Camargo*, Diego F. Sierra and Yeison F. Torres

Faculty for Computing and Systems Engineering, Antonio Narino University, Bogota, Colombia;
jorgecamargo@uan.edu.co, diesierra@uan.edu.co, yeitorres@uan.edu.co

Abstract

Objectives: The aim of this paper is to analyze a set of cryptographic algorithms to protect medical records in the context of mobile applications. **Methods**: We analyzed the use of cryptography in a data set of medical health records taking into account the use of computing memory, processing and time in each studied algorithm. A system prototype was developed with the most efficient algorithm found after experimentation. **Findings**: Results show that health records are properly secured in a mobile scenario with good performance in terms of computational resources. **Applications**: This study will help mobile software developers to understand the importance of writing secure software in health systems.

Keywords: Cryptography in Health Systems, Electronic Medical Records, E-Health, HL7, Secure Mobile Applications

1. Introduction

With the increasing use of mobile devices, users want to access different types of services from tablets and smartphones. This phenomenon is known as ubiquitous computing[1] in which users want to access their information in any place, any time and from any device. Health services are not the exception. Doctors and patients want to access medical information to speed up processes and reduce workload by making information accessible. Although healthcare institutions have implemented electronic information systems, those systems are mainly focused on internal processes. However, mobility is a new need for users. For instance, a patient would like to access medical information to remember specific information of certain treatment or medics.

Doctors can access this information generally trough intranets, but it is not accessible to patients. An Electronic Medical Record (EMR) is a document of restricted use that contains important and sensible patient's information. Hospitals and health centers have to store and manage EMRs in physical and digital formats, therefore they have to guarantee that only patients and authorized personal can access them. Laws in countries generally regulate the access to medical information with the main goal to protect patient's confidentiality as a fundamental right.

Health institutions have been broadly using security mechanisms to protect sensible information in systems such as Picture Archiving and Communication Systems (PACS) and Electronic Medical Record systems (EMR). Those systems are mainly based on client/server architectures in which users access medical information through a desktop or browser client and secure networks protect sensitive information. However, in mobile environments security is a concern that has called attention of research community to develop mechanisms that allow protecting confidentiality of patients. Mobile devices are sensitive to be stolen and lost, and mobility makes they change regularly of networks (Telco operator, public wireless, enterprise networks, etc).

1.1 Background

HL7[2] is a set of standards internationally accepted by most of hospital and health centers to transfer clinical and administrative data. These standards focus on the layer 7 of the Open Systems Interconnection (OSI)

* Author for correspondence

mode and they are produced by the Health Level Seven International organization[3]. One of the standards of HL7 is the CDA standard[4], which defines an exchange model for clinical documents in Extensible Markup Language (XML)[5] format intended to specify the encoding, structure and semantics of clinical documents. A CDA[1] can contain any type of clinical content such as Electronic Medical Records (EMRs), in which medical information of patients is stored and transmitted between hospital systems[7].

Figure 1 illustrates an example of patient information according to the Electronic Health Record specification of the HL7 standards. The XML structure organizes patient information in a hierarchy of elements, attributes and values. The exchange of medical information requires of suitable mechanisms to digitally secure EMRs. Cryptography is an area that has developed strong mechanisms to secure digital information[8–10]. The use of cryptography prevents attacks that disclosure personal information[11].

There are two main families of encryption algorithms that are based on symmetric and asymmetric approaches[12,13]. In symmetric algorithms, a private key is used to encrypt and decrypt a message. In asymmetric algorithms, a pair of keys are used: private key is used to encrypt and public key to decrypt. In this paper we focused on symmetric algorithms, which are suitable to protect a EMRs when they are exchange through the network.

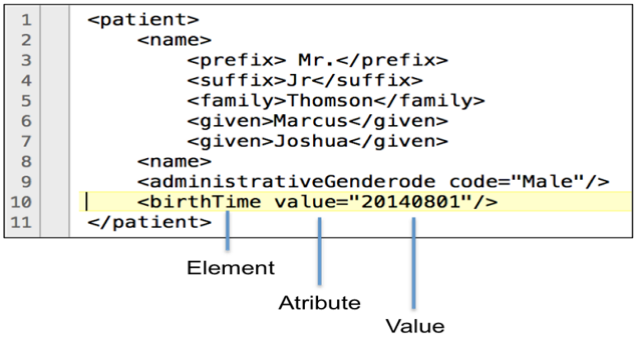

Figure 1. An XML example of an electronic medical record (Source: The authors).

1.2 Related Work

Four our surprise, there are not much works that address the problem of secure electronic medical records in a mobile scenario. Haque et al.[14] recently proposed a platform to secure communication between mobile devices and EMR systems. A web XML-based CDA prototype was proposed by Paterson et al.[15] to move discharge summaries from hospitals to family practice locations. Authors in[16] proposed an infrastructure to deliver health records to mobile phones in which security is not addressed. In such as infrastructure a web-mobile application was developed to display patient information. This proposal has the restriction of having an Internet connection. In[6] authors propose a cross-institutional implementation of a web service to interchange clinical data. Although this proposal takes into account HL7/CDA standards and addresses security concerns, the proposal applies only in non-mobile environments.

1.3 Contribution

In this paper we present an evaluation of asymmetric encryption algorithms to determine the efficiency and effectiveness in terms of memory, processor and execution time. We also developed a system prototype to evaluate the feasibility of securing electronic medical records when they are accessed from mobile devices.

This paper is organized as follows: Section 2 describes material and methods in which we describe the proposed system; In Section 3 we discuss results; and Section 4 concludes the paper.

2. Material and Methods

This work has two main objectives: the first one consists in evaluating the performance of a set of algorithms in terms of efficiency in order to determine which is the most suitable in a mobile environment; and the second one is focused on building a system prototype in which medical records are secured when they are interchanged between a mobile device (client) and a medical record system (server).

2.1 Experimental Design

In this section we present experimental design details, dataset used, encryption algorithms and prototype system developed.

2.1.1 Data Set

We used an anonymized data set of health records available at https://wiki.openmrs.org/display/RES/Demo+Data,which includes information of 5,000 patients and 500,000 observations provided by the Open MRS project. The software Open MRS is one of the most

popular open source medical record systems used in health centers of developing countries. This data set was pre-processed in order to build 50,000 CDA files in XML format.

2.1.2 Encryption Algoritms

We selected four symmetric algorithms to be evaluated in terms of performance based on the comparative study performed in a recent paper[17]. In the following paragraphs we briefly describe each of the selected algorithms[18].

2.1.2.1 Data Encryption Standard (DES)

Algorithm developed in the early 1970s at IBM based on an earlier design by Horst Feistel. This algorithm takes a fixed-length string of plaintext bits and transforms it through a series of operations into another cipher-text bit-string of the same length. The block size is 64 bits, form which 56 bits are used by the algorithm and 8 for checking party. The decryption process uses the same structure as encryption but the keys are used in reverse order. This algorithm was used for decades and it is considered one of the most influential in the advancement of modern cryptography.

2.1.2.2 Advanced Encryption Standard (AES)

Algorithm developed by Joan Daemen and Vincent Rijment in 2001 through a contest organized by the National Institute of Standards and Technology (NIST). It uses a combination of both, substitution and permutation operations in a sized block size of 128 bits, and a key size of 128, 192, or 256 bits.

2.1.2.3 RC4

It is the most widely used stream cipher algorithm and it is used in protocols such as Transport Layer Security (web browsers) and WEP (wireless networks). Ron Rivest at RSA Security designed it in 1987 and it is recognized for its simplicity and speed. The algorithm is based on generation of pseudorandom stream of bits to cipher the plaintext using bit-wise exclusive-or operations.

2.1.2.4 Triple DES

This algorithm consists in applying three times the DES algorithm to each data block using three keys. Those keys can be independent or identical. This algorithm appeared in 1998 as a more secure algorithm than DES.

2.2 Performance Measures

The 50,000 medical records were encrypted using selected algorithms. The following performance measures were evaluated in each algorithm:

2.2.1 Computing Time

Time in seconds spent by the computer to encrypt a set of electronic medical records using each encryption algorithm.

2.2.2 Computing Memory

Main memory in Kilobytes used by the computer to encrypt a set of electronic medical records using each encryption algorithm.

2.2.3 Processing Consumption

Percentage of processor used by the computer to encrypt a set of electronic medical records using each encryption algorithm.

These performance measures were calculated increasing by 5,000 the number of electronic medical records starting in 5,000 and ending in 50,000. For each performance measure a plot was generated including the four selected algorithms.

2.3 Execution Environment

Experiments were conducted in Linux machine with an Intel Core 2 Duo Processor 1.6 x 2 GHz and 2 GB of RAM.

3. Experimental Results

In this Section we present the obtained experimental results for each of the defined performance measures and some details of an Android system prototype.

3.1 Performance Evaluation

Figure 2 shows the obtained results for the computing time measure. In the first 30,000 the four algorithms show a linear trend. However, after this quantity, they show an exponential growth. Note that the AES algorithm in general obtained the lowest computing time, which is indicates that it is a candidate to be selected using computing time criteria.

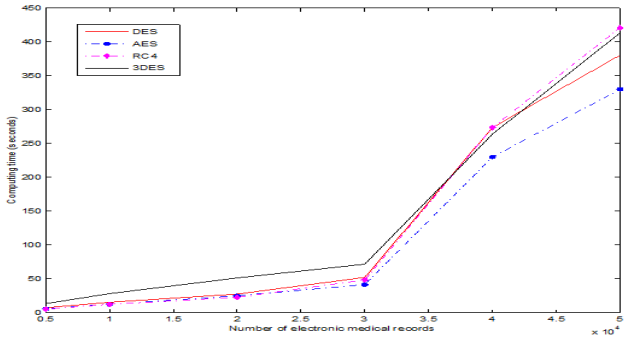

Figure 2. Computing time used for each algorithm to encrypt 50,000 electronic medical records (10 runs).

Figure 3 shows the obtained plots for the computing memory measure. Results show that all curves have linear trending. Until 2,000 electronic medical records RC4 has the lowest use of memory. After 3,000 EMRs, AES performs much better than the other algorithms.

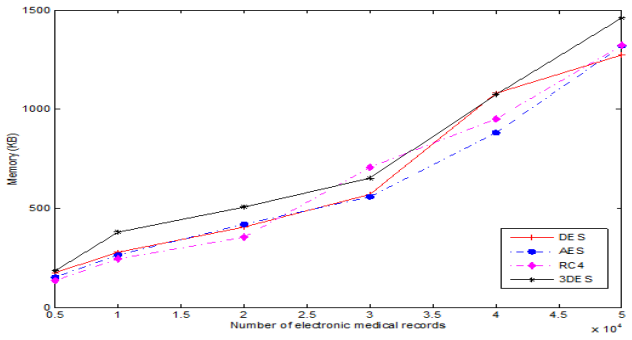

Figure 3. Computing memory used for each algorithm to encrypt 50,000 electronic medical records (10 runs).

Figure 4 shows the obtained results for the processor consumption measure. Results show that all curves have a linear trend. Until 1,500 electronic medical records RC4 has the lowest use of processor. In general AES performs much better than DES and 3DES and slightly better than RC4.

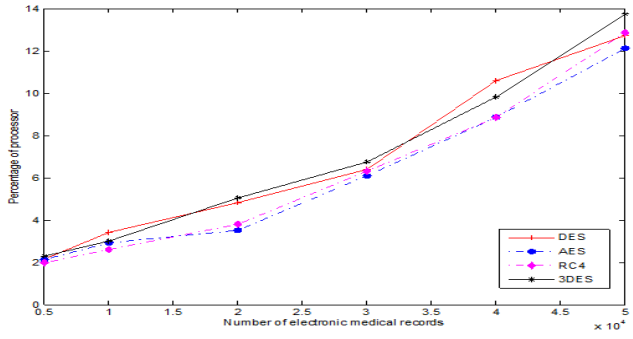

Figure 4. Processing consumption used for each algorithm to encrypt 50,000 electronic medical records (10 runs).

In general, the AES algorithm performs better than DES, 3DES and RC4, so this algorithm is the best in terms of efficiency. With respect to effectiveness, AES is the most secure algorithm according to the comparison performed by Hambdan et al[17].

3.2 System Prototype

We built a system prototype to evaluate the feasibility of implementing the AES algorithm in a mobile environment. To do that, we developed a system prototype composed of two components: mobile client and server. Figure 5 illustrates the general architecture of the system. Figure 6 presents a deployment diagram of the system. In the following Subsections we briefly describe functionalities of each component.

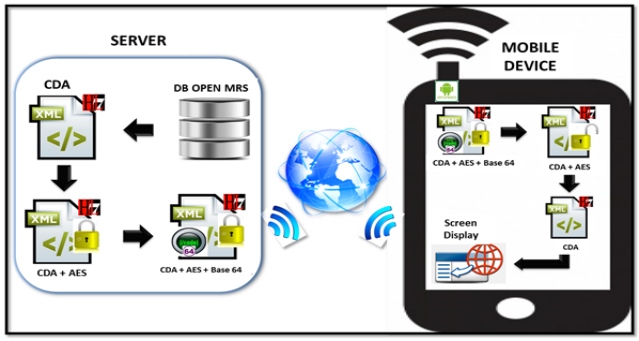

Figure 5. System overview. In the server component, electronic medical records are stored, encrypted, encoded and transmitted to mobile client. EMRs are decoded, decrypted and displayed to patients in the mobile component.

Figure 6 presents a deployment diagram of the system. In the following Subsections we briefly describe functionalities of each component.

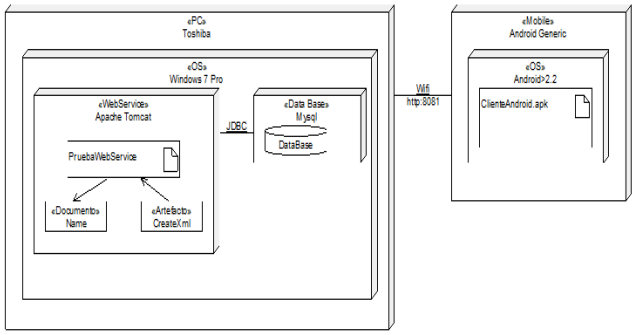

Figure 6. Deployment diagram of the two system nodes: mobile and server.

3.2.1 Server Component

The server component stores the collection of electronic medical records. The following are the functionalities that were implemented in Tomcat 7.0 as application server to bring access to clients to electronic medical records. The following are the steps performed by the server:

- Original electronic medical records are stored in MySQL database, so they are converted to files under the CDA standard.
- These CDA files are encrypted using the AES algorithm.
- After encryption process it is possible that special characters are generated, so it is necessary to encode them with the Base 64 encoding algorithm, which is commonly used after cipher streams to send them through network.
- Encoded records are exposed as a web service to be consumed by the mobile client.

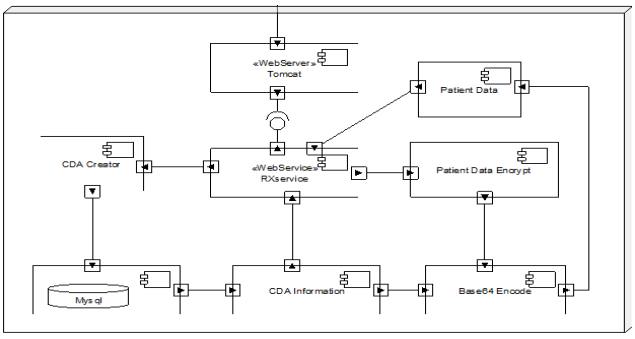

Figure 7. Component diagram of the system (server side).

Figure 7 shows a component diagram of the system at the server side, which is composed of software components specialized in each task performed by the server.

3.2.2 Mobile Component

The mobile client offers a Graphical User Interface (GUI) in which users can access electronic medical records through the Internet. Figure8 shows a software component diagram of the mobile client. The mobile application was developed natively for Android 2.x or superior. The following are the steps performed by the client to process data sent by the server:

- The user configures connection parameters to access the server (IP address and port).
- The GUI offers a text box to enter the identifier of a electronic medical record.
- The mobile device sends a request to the web service using the identifier.
- The server returns an encoded electronic medical record.
- The mobile processes the encoded electronic medical record returned by server using a REST Application Programming Interface (API).
- The mobile decodes the obtained record (decoding with Base64).
- A decryption process is performed using the AES algorithm.
- The electronic medical record is shown to the user in clear text.

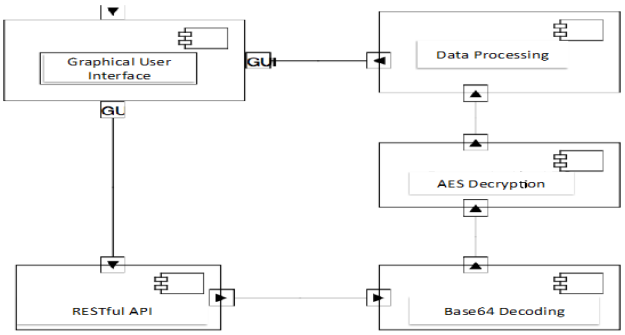

Figure 8. Component diagram of the system (mobile client).

Figure 9 illustrates the before mentioned sequence of steps that are performed by the system when a user requests a medical record. User, mobile client, web service and data base are the elements that participate to search and retrieve medical records.

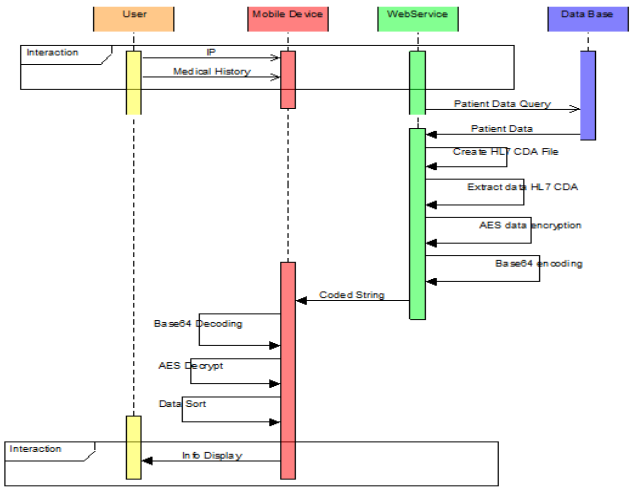

Figure 9. Sequence diagram of the interaction between user and system to retrieve a medical record.

Figure 10 shows a set of screen shots of the mobile component. This prototype allows configuring server connection parameters such as IP address and port, to search an electronic medical record and to visualize it in the screen. Android graphical user interface components are used to capture and display medical information.

Figure 10. Some screen shots of the mobile component: **(a)** Connection parameters and ID of the electronic medical record to be accessed; **(b)** and **(c)** Electronic medical record returned by the server corresponding to the ID provided by the user.

4. Discusion

Encryption algorithms are commonly replaced for other more secure algorithms. The security provided for a new algorithm is relative. Any algorithm can be broken using suitable computing resources and time, as it is described in vulnerability penetration tests[19]. One of the mechanisms to make an algorithm stronger consists in providing large encryption keys. However, this mechanism is not practical in scenarios in which computing resources are limited, as it is the case of mobile environments. Nowadays mobile devices have high memory, multiple cores, gigabytes of storage and broad bands such as 4G Long Term Evolution (LTE). Therefore, it is necessary to bring security to protect information possible atacksin mobile scenarios.

The evaluated algorithms in this paper have been reported by the industry as insecure because they have been broken in the past. However, when these algorithms are combined, the security is improved. They are being used today in multiple scenarios such as wireless routers, authentication protocols, network/transport protocols (TLS and SSL), among others.

5. Conclusion

With the increasing use of mobile devices, security is a concern that has to be addressed in the construction of new systems in order to guarantee patients confidentiality. In this paper, we presented a system to secure electronic medical records in a mobile scenario. We conducted an evaluation with four symmetric algorithms to determinate the most efficient of them in terms of memory, processing and computing time. Results showed that the AES algorithm was the most efficient according to some performance measures. We implemented a system prototype in which electronic medical records are securely exchanged between server and mobile client. A system prototype was developed for the Android platform, which offers a graphical user interface to access electronic medical records stored in an EMR. The proposed architecture can be implemented in other mobile platforms such as iOS. To the best of our knowledge, this paper is one of first initiatives to address security concerns to securely interchange electronic medical records under HL7/CDA in mobile scenarios.

6. References

1. Abraham C, Richard W, Boudreau M-C. Ubiquitous access: On the front lines of patient care and safety. Communications of the ACM. 2008 Jun; 51(6):95–9.
2. Health level seven international: HL7 CDA Release 2. 2005. Available from: http://www.hl7.org/implement/standards.
3. Murphy G, Brandt M. Health informatics standards and information transfer: exploring the HIM role (AHIMA Practice Brief). Journal of AHIMA. 2001; 72(1):68.
4. Dolin RH, Alschuler L, Boyer S, Beebe C, Behlen FM, Biron PV, Shabo (Shvo) A. HL7 clinical document architecture, Release 2. Journalof the American Medical Information Association. 2006; 13(1): 30–9.
5. Brewton J, Yuan X, Akowuah F. XML in health information systems. Greensboro, North Carolina USA: Department of Computer Science, North Carolina A and T State University. 2012.
6. Muller M, Uckert F, Burkle T, Prokosch HU. Cross-institutional data exchange using the clinical document architecture (CDA). International Journal of Medical Informatics. 2005 Mar; 74(2-4):245–56.
7. Hayrinen K. Definition, structure, content, use and impacts of electronic health records: a review of the research literature. International Journal of Medical Informatics. 2008 May; 77(5):291–304.
8. Patil A, Goudar R. A Comparative survey of symmetric encryption techniques for wireless devices. IJSTR. 2013 Aug; 2(8):61–5.
9. Lopez M. Criptografía UNAM, Facultad de Ingenieria. 2009.
10. Sklavos N. Wireless security and cryptography specifications and implementations. 2010.
11. Sridhar KP, Saravanan S, Vijay Sai R. Counter measure

against side channel power attacks in cryptography devices. Indian Journal of Science and Technology. 2014 April; 7(Suppl 4):15–20.
12. Gine F. Implementacion de un esquema criptografico para gestionar de forma segura las historias medicas de los pacientes a traves de una red de comunicaciones [Bachelor thesis]. Universitat Oberta de Catalunya. 2010.
13. Lombardo R. Sistema de historia clinica digital. Sociedad de Cardiologia de San Juan Federacion Argentina de Cardiologia. 2008.
14. Haque W, Horvat D, Verhelst L. A secure mobile platform integrated with electronic medical records. Prince George BC, Canada: University of Northern British Columbia. 2014.
15. Paterson G, Sheperd M, Wang X, Watters C, Zinter D. Using XML-based clinical document architecture for exchange of structured discharge summaries. In: Proceedings of the 35th Hawaii International on System Sciences; Maui. 2002. p. 1200–9.
16. Ghose A, Bhaumik C, Agrawal AK. Mobile healthcare infrastructure for home and small clinic.In: Proceedings of the 2nd ACM International Workshop on Pervasive Wireless Healthcare; New York. 2012. p. 15–20.
17. Hamdan O, Zaidan BB, Zaidan AA, Jalab HA, Shabbir M, Al-Nabhani Y. New comparative study between DES, 3DES and AES within nine factors. 2010.
18. Gomez A. Encyclopedia de la seguridad informatica. Mexico; 2007.
19. Daltabuit E. La seguridad de la informacion. Mexico, Limusa; 2007.