

# Medical Data Security Model for Early Intervention Support System Based on HIPAA

EKO SUPRIYANTO, HAIKAL SATRIA, TAN KEAN SIONG

Faculty of Health Science and Biomedical Engineering

Universiti Teknologi Malaysia

UTM Skudai, 81310 Johor

MALAYSIA

[eko@utm.my](mailto:eko@utm.my), [tankeansiong@gmail.com](mailto:tankeansiong@gmail.com) <http://www.biomedical.utm.my>

*Abstract:* - Early Intervention Support System for Special Children (ELISSA) is an effective tool to improve the special children developmental ability. As the system stores sensitive personal data such as children medical data, it is crucial to have an adequate data security model for the system. The existing system however only uses conventional insecure login method, and this may cause information leakage. Hence, we propose a novel medical data security model that integrate security features based on Health Information Portability and Accountability Act (HIPAA) in a Universal Serial Bus (USB) dongle. Advanced Encryption Standard (AES)-256 has been implemented and new file format .els has been introduced. The model complies to the HIPAA Security Rule includes access control, audit control, person authorization, integrity and transmission security. It has been successfully integrated with the support system. Test result shows that the model is able to improve ELISSA security and compatible with Linux and Microsoft Windows operating system.

*Key-Words:* - medical data, security model, HIPAA, ELISSA, USB dongle, AES

## 1 Introduction

Early intervention support system has been developed as the Down Syndrome babies require an individual early intervention program, an appropriate medical care, and a positive learning attitude. The software, Early Intervention Support System for Special Children (ELISSA) has served the purpose of input, store, display, and update the user data; to generate the individual curriculum with optimal training duration; as well as to give duration and analyze the result as part of screening and training[1]. This Java-based system has however lack of secure authentication method in the system module. The system currently adopts the conventional insecure Username and Password authentication model. With the current model, the personnel information will be stored in the source code and database in clear text without any encryption. The malicious user may capture the authentication data easily thus obtain the administrative credential. The system is also lack of software protection mechanism which is important for the software ownership and copyright. The system has yet complied with law or acts that protect the health care information such as HIPAA.

In August 1998, the United State Department of Health and Human Services (HHS) published the Security and Electronic Signature Standards; Proposed Rule (Security Rule). The Security Rule covers all healthcare information that is electronically maintained or used in electronic transmissions. It is defined by HHS as a set of requirements with implementation features that providers, plans, and clearinghouses must include in their operations to assure that electronic health information remains secure[2].

The Security Rule is merely a set of common best practices that is intended to be comprehensive, technology neutral, and scalable for different-sized organizations. It is a high-level information security framework that documents what needs to be done to secure healthcare information systems. At the same time, and much to widespread chagrin, the Security Rule is not a set of how-to instructions outlining the exact steps for securing healthcare information systems.

To ensure the confidentiality, integrity and accessibility of healthcare information, the Security Rule outlines various technologies, policies that must be implemented. The policies and procedures for technology-based systems include:

- Logical access controls
- Physical access controls
- User authentication controls
- Authorization controls
- Audit controls
- Data encryption mechanisms

General medical security models fall short of what is needed. From the policies and from the environment where the information is kept, the requirements for the security model can be deduced [3]:

- Attribute and credential -based authorization
- Content-dependent authorization
- Context-dependent access modes
- Delegation of rights
- Administration of security

- Temporal restrictions
- Need for coordinated authentication and encryption
- Consideration of web standards
- Consideration of different architectural levels
- Compliance with laws protecting security and privacy of health care information
- Explicit audit.

It is clear that no single model can satisfy all these requirements. Thus it needs several related models at different abstraction levels to cover all the requirements.

In section 2, we describe the medical data security design which is based on HIPAA Security Rule. Result is discussed in Section 3 and we draw some discussions and conclusions in Section 4 and Section 5.

## 2 Design and Implementation

In this section, we describe the medical data security design in detail.

### 2.1 Design Specification

Three main functions have designed for ELISSA, which include User Authentication, User Authorization, and software protection mechanism. The model is compatible with the Linux operating system such as Ubuntu, Fedora Core and also the Microsoft Windows operating systems. The security features has been implemented with specific USB dongle. The automated specific USB dongle detection has been designed to serve as hardware token for authentication and data storage usage. AES-256 bit encryption method and data obfuscation method has been used in the model. New file format with extension .els has been introduced for the sensitive data security and secure storage. The configuration of the system is shown in Fig. 1.

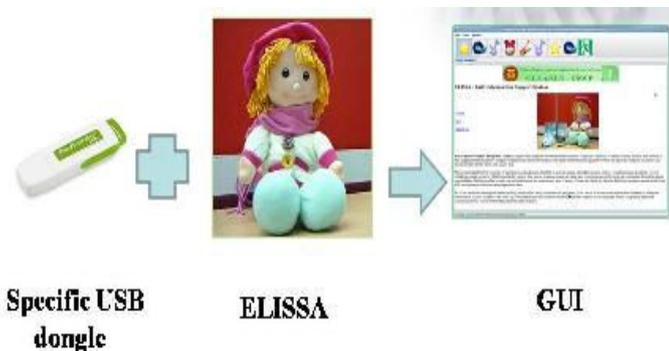


Fig. 1 System Configuration

The model has been designed and complied with the HIPAA Security Rule. Table 1 shows the features that follow the HIPPA Security Rule technical safeguards [4][5]:

Table 1  
Data Security Model Design

Technical Safeguard	Model Design
Access Control	Specific USB dongle
Audit Control	Security log audit
Integrity	Data backup, Data integrity
Person Authentication	User authentication
Transmission Security	AES-256 Encryption, Data obfuscation, .els file extension

#### 2.2.1 Specific USB dongle detection

Specific manufacturer and device identity number has assigned to every USB dongle during the production. The identity number is unique for each dongle. This characteristic has been adopted well in the model design and served as for authentication purpose.

#### 2.2.2 Data Encryption

The user credential is important for the authentication and authorization function. The data has been encrypted with AES-256 encryption. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits[6]. AES-256 has been chosen as TOP SECRET information that requires use of either the 192 or 256 key lengths, according to United States National Security Agency[7].

#### 2.2.3 Data Obfuscation

Unique data obfuscation technique has been introduced for the data hiding. The algorithm for data obfuscation is shown in Fig.2. The message input has been encoded with base64encoder and the message content has been translated to base64 representation. The textual result can be used to create the .els format binary. The encoded message has been appended with specific delimiter for the message differentiation. Each character in the message has been added with two random characters. The obfuscation process has been performed till the end of the message. With JAVA DataOutputRStream function[8], the output has been written to .els extension binary with the file segment structure as show in Fig.3. The magic number of the els extension is a three-bytes hex format combination “454c53” which stand for ELS. This specification has been used for binary verification during the deobfuscation process.

## 2.2 HIPAA compliance

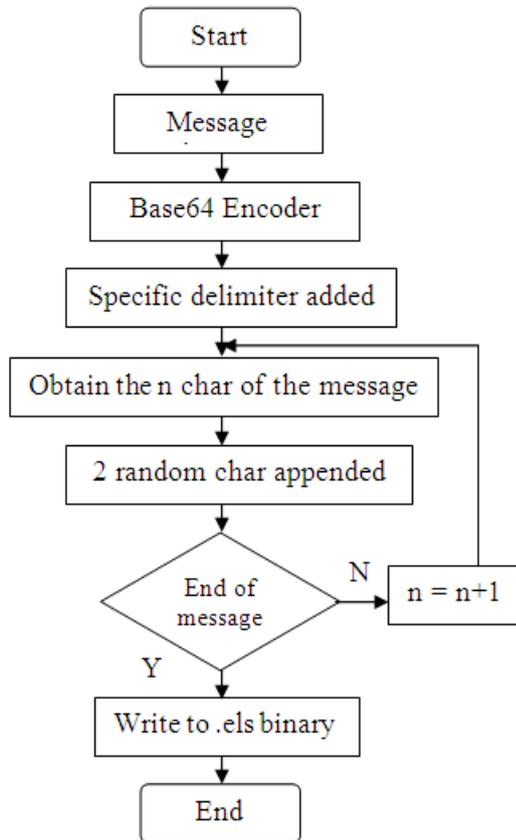


Fig. 2 Data Obfuscation Algorithm

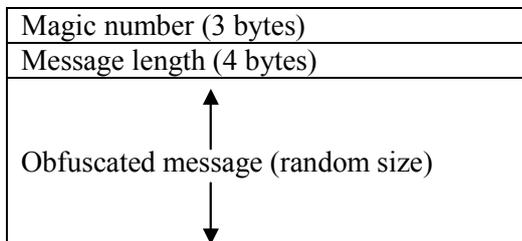


Fig. 3 The Structure of .els File Segment

### 2.3 Model implementation

For the model implementation, we use open source software for the cost-saving purpose. The model has been developed with JAVA language due to the ELISSA integration issues. We have implemented the model in LINUX and WINDOWS environment. Softwares and used tools are shown in Table 2.

Table 2  
Implementation Tool and Software

Function	Tool and Software
Programming Language	JAVA
USB Interfacing	Shell script
Operating System	Linux (Ubuntu, Fedora), Windows
USB Dongle	Kingston Traveler
JAVA tool	Eclipse

### 3 Result and Analysis

To ensure the quality and reliability of the software, the functionality and compatibility testing has been performed. The test results are listed in the Tables 3 and 4.

Table 3  
Functionality Test

Function	Parameter	Result
USB detection	Specific USB dongle	Passed
User Authentication	User password	Passed
User Authorization	Role : Trainer, Parent	Passed
Data Backup	Backup to USB dongle	Passed
Security log	Log record	Passed
Data Integrity	Integrity checking	Passed

Table 4  
Compatibility Test

Operating System	Result
Ubuntu 9.04	Passed (100%)
Ubuntu 9.10	Passed (100%)
Fedora 12	Passed (100%)
Windows XP	Passed (100%)
Windows Vista	Passed (100%)
Windows 7	Passed (100%)

The difference of security enhancement features between previous design and the model design based on HIPAA is shown Table 5. The new model has improved the overall support system security with the modification of the existing model and introduction of new features.

Table 5  
Comparison of Security Specification

Specification	Existing model	New model
Data Visibility	Clear text	Encrypted form, Obfuscated form
Data Storage	.txt	.els
Access Control	1 layer: password	2 layers: usb dongle, password
Audit Control	None	Security log
Integrity	None	Integrity checking
Transmission security	None	AES-256

### 4 Discussion

The model has focused on the three main functions : user authentication, user authorization and software protection mechanism. The input of user password has been served as the first layer of user authentication process. The

automated specific USB has been designed to be the second layer of the protection. Adequate user right is authorized to user according to their role as parent or trainer. The support system has been protected with new .els extension binary which contains encryption and unique data obfuscation technique.

In our study, we have compared the new model with the conventional user-password authentication method. We found that the model has improved the overall security issues of ELISSA. The sensitive data such as user credential has been stored well in encrypted format and this makes the effort of reverse engineering become nearly impossible. However, the limitation of present model is the authentication time has taken longer time than the original security method as it has involved USB dongle detection and verification. The model is subjected to JAVA virtual machine bytes code decompilation attack. But, the risk of data being decompiled is minimized due to the unique data obfuscation technique. To encounter the limitations mentioned above, we have investigated security enhancement techniques of USB hardware token and secure the bytes code.

## 5 Conclusion

We have proposed a medical data security model for Early Intervention Support System for Special Children. The model has features that comply to HIPAA Security Rule. AES-256 encryption and unique data obfuscation technique has been introduced and implemented in new .els extension file format. Findings showed that the model is able to improve and enhance the overall ELISSA security.

## ACKNOWLEDGMENTS

The authors are so indebted and would like to express our thankfulness to Universiti Teknologi Malaysia and Ministry of Science, Technology and Innovation (MOSTI), Malaysia for supporting and funding this study under Vote 79327. Our appreciation also goes to the Progressive Healthcare and Human Development Research Group members for their ideas and comments on this paper.

## References:

- [1]E. Supriyanto, S. C. Seow, *Java Based Automatic Curriculum Generator for Children with Trisomy 21*, International Journal of Humanities and Social Sciences, Volume 2, Number 1, 2007, pp. 24-27.
- [2]Kevin Beaver, *Healthcare Information System*, Second Edition, United State of America: Auerbach, 2003, pp. 173-180.
- [3]Eduardo B. Fernandez, María M. Larrondo Petrie, and Tami Sorgente, *Security Models for Medical and Genetic Information*, 2004.
- [4]Center of Medicare & Medicaid Services, *Security Standards: Technical Safeguards*, Vol. 2, Paper 4, 2007.
- [5]Center of Medicare & Medicaid Services, *Security 101 for Covered Entities*, vol.2, paper1, 2007.
- [6]J. Daemen and V. Rijmen, *AES Proposal*, AES Algorithm Submission, September 3, 1999.
- [7]L. Hathaway, *NSS Policy National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*, No. 15, Fact Sheet No. 1, 2003.
- [8]David. Hook, *Beginning Cryptography with Java*, Wrox Professional ,2005.