A Design of Security Framework for Data Privacy in e-Health System using Web Service

Non Thiranant*, Mangal Sain*, HoonJae Lee**
*Department of Ubiquitous IT, Graduate School of Dongseo University,
Sasang-Gu, Busan 617-716, Korea
**Division of Computer and Engineering Dongseo University
Sasang-Gu, Busan 617-716, Korea
thiranant.non@gmail.com , mangalsain1@gmail.com, hjlee@dongseo.ac.kr

Abstract— **E-Health is a common term used for electronic health, where the services and systems provided include electronic health records, prescriptions, consumer health information, healthcare information systems, and so on. In this period of time, several patients have started to use e-health, considering the convenience of services delivered and cost reduction. The popularity has abruptly been increasing due to a wide range of services. From the system administrator's perspectives, not only protecting privacy of patients is considered a difficult task, but also building trust of patients in e-health. In this paper, a design of security framework for data privacy in e-Health system based on web service architecture is proposed. It is interesting to note that the approach proposed in this paper is not limited to e-Health system.**

Keywords- **Privacy, E-health, Data Privacy, Web service, Data encryption**

I. INTRODUCTION

E-health has grown its success and popularity from time to time, due to a wide range of services provided. In practical, the system has to be secure, and e-health service provider is entrusted with the responsibility to handle the sensitive information [1]. E-health system has encountered many threats to the confidentiality of patient such as sensitive data are in wrong hands, unreliable authentication process. The above factors may cause a drastic impact directly or indirectly to the patients, as well as the reputation of the service providers. Data integrity and availability are also of great importance; as a patient's life could depend upon the e-health system. Patient's information should be conserved and ensured that it is always up to date, and is not altered by those who have no right [1] [2].

It is known that e-health involves a variety of users such as patients, doctors, nurses, etc. who would access electronic medical data. These various types of users have different assigned tasks and perhaps may not be allowed to access certain data. For example, doctors have right to check and modify the records of patients' diagnosis results, but this information shall not be accessed by patients [2].

In order to ensure the privacy of all patients, not all the information should be revealed to all types of users. It can be easily achieved by having a clear separation line between each of user type. The sensitive information is to be under control and permission to access and exchange data is based on their role. Authentication process is the first step that each system should be aware of. A weak authentication system may lead to information leakage, and it is a possibility that patients will be the victim as the information is altered.

In this paper, a design of security framework for data privacy in e-health system via web services is proposed. The procedure includes the use of simple web applications and web services, built along with the database as data storage. The technique proposed in this paper is to ensure the data stored in the web server are safe, and will still be safe in case they fall into wrong hand. This concept can be applied in various scenarios, not limited to e-health system. With the proposed approach, data in e-health system can be considered secure and the process is cost-effective.

II. BACKGROUND AND RELATED WORK

1. Web Application

A web-based application is an application that uses a web browser as a client. It refers to the computer software that is programmed in browser-supported programming languages; such as Java, ASP.NET. Web applications are commonly used due to the popularity of web browsers, and the convenience of using web browsers. There are no extra software installations required for consuming services provided. The main benefit is that it requires no upgrade procedure since all new features are implemented on the server and automatically delivered to the users.

2. Web Service

A Web service a method of communications between electronic devices over internet. It is a software function provided at a network address over the web or the cloud. It is considered a software system designed to support interoperable machine-to-machine interaction over a network. Systems interact with the Web service by its description using SOAP messages, typically conveyed using HTTP with an XLM serialization in conjunction with other Web-related standards [3].

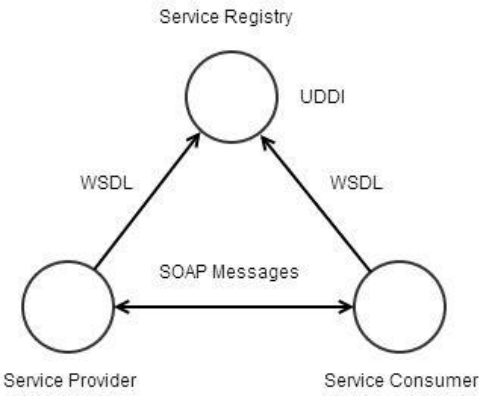

Figure 1: Web Service Architecture

3. Cloud Storage

Cloud storage is considered one of the primary use of cloud computing. With the cloud storage, data are stored on various third party servers. Cloud storage services are usually accessed via a web service, web application and desktop applications. It is considered cost-efficient for many corporations and small businesses for everyday use. In this paper, cloud storage is seen in the form of database, where data; such as file unique number, file name, file path are stored. The database is designed along with the web service, which is a medium between the web application and client [4] [5].

4. Data encryption and Data privacy

Data stored in the cloud being transferred through network in plaintext form is at risk. Data encryption ensures the security and privacy of data stored in cloud storage. In case files in the cloud storage are accessed from unauthorized users, they will still be safe from being read and altered. The common challenge in data privacy is to share while protecting the sensitive information. Therefore, data encryption is considered one of the necessities when performing any action to files such as storing, sending, sharing, etc.

5. Related Work

Kumar, A proposed a technique for authentication, encryption, and decryption is proposed. The files stored in the cloud storage are separated into two sections, which are private data section and shared data section. The approach used for data encryption is Elliptic Curve Cryptography, which is public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The proposed scheme still faces the problem of group sharing data in the shared data section. This is because it only allows one-to-one communication [6].

Löhr, H, the author proposed the security architecture for establishing privacy domains in e-health infrastructures. The solution provided in the paper includes client platform security and combines with network security concepts. The security and privacy issues in modern distributed e-health system are discussed [7].

III. Design and Implementation

The proposed scheme is essentially focused on the use and popularity of web service and cloud storage. As mentioned earlier, unencrypted data stored in the cloud are vulnerable and probably, due to poor security, getting accessed by many unauthorized users. The main concept of the proposed scheme is that data should be encrypted before getting warehoused in the cloud storage. Encryption algorithms are not discussed in this paper, since we are focused on the encryption and decryption process using web service.

1. System Requirements and System Overview

Web service is implemented along with the database as an intermediary consumed by the web application. Any Web-based programming language can be used to implement. A database is designed to store the information and details of each file such as file ID, file name, file path, etc.; not the files themselves. It is known that files from various sources are stored together in the same storage, the important thing that indicates the right of users is stored in the database. Figure 2 depicts the process of accessing files. Each file has its own unique ID, name, and storing path. When users make a request to read a file, the system will use the information in the database to retrieve the particular file that has the corresponding ID, name, and file path.

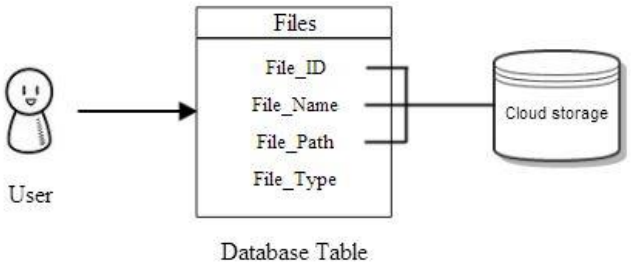

Figure 2: Files access process

With the use of web service, the system is designed in the way such that users are to interact with the application programming interface (API) in the form of web page. Once users make a request; says uploading files, the application will then call the web service in which database is attached. In case there are data-in and data-out, all the tasks will be handled by web service and the files will be stored in the cloud storage. Figure 3 depicts the system overview, showing how users interact with API and web service.

From the explanation above, it is seen that data stored in the cloud storage can be an easy target; since there is no encryption process involved. The proposed approach involves the files encryption and decryption steps. When users upload any type of file such as image, video, text files, the web application will request the encryption function from web services, by passing the files as parameter and consume the service. The function will return the encrypted file, once the encryption process is done. This approach does not have restriction with the algorithms. In addition, both symmetric and asymmetric key algorithms can be applied.

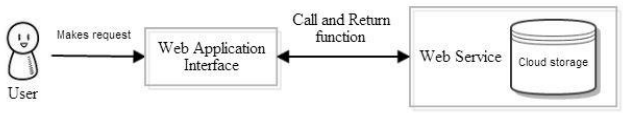

Figure 3: System overview

2. Encryption process

When a user wants to upload a file, the web application will make a request to the web service; where operations and messages are described abstractly. User has to choose a file to upload to the server via the web application interface. The web application will call the encryptFile function, which will encrypt with a system specified encryption algorithm. Once the file has been encrypted, it will be stored in the cloud storage at the specified path. Figure 4 depicts the encryption process showing step-by-step how the service is consumed and how files are safely stored in the cloud storage. The steps involved in the encryption process are listed as follow:

1) User chooses a file to upload via web application interface
2) Web application calls the encryptFile function implemented in the web service
3) The file chosen by user will be encrypted, regardless the type of file
4) The encrypted file is stored in the cloud storage and file information is stored in the database table

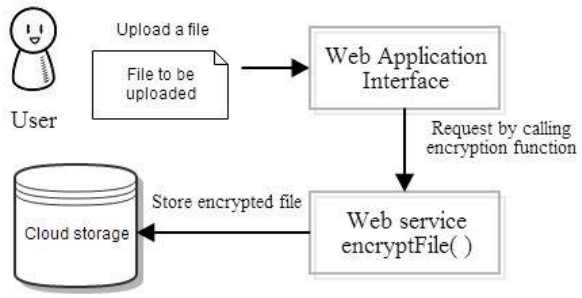

Figure 4: Encryption process

3. Decryption process

The same process goes for file decryption when a user wants to download a file. Firstly, user has to choose a file to download via the web application interface. Secondly, the web application will call the decryptFile function, which will decrypt the file and make it available for the user to download. In the back-end, the file ID, file name, and file path are needed to retrieve the corresponding file. This file information is to be taken from the database table. Figure 5 depicts the decryption process showing how the service is consumed, and how files are decrypted and downloaded from the cloud storage. The steps involved in the decryption process are listed as follow:

1) User chooses a file to download via web application interface
2) Web application calls the decryptFile function implemented in the web service
3) The file chosen by user is retrieved from the cloud storage according to the file ID, file name, and file path.

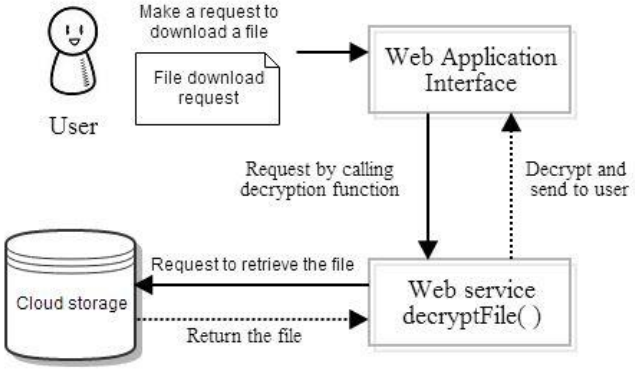

Figure 5: Decryption process

IV. Security Analysis and Problems

1. Man-in-the-middle attack

Assume an unauthorized user accesses the cloud storage (not via authentication system) and wants to read the file. In this case, the files stored in the cloud will be safe; since they are encrypted. It is interesting to note that all these files should only be allowed to delete or modify only by users who have right; says unique identification needed. To fulfil this, the system should check every session of each user starting from log-in. There must not be unauthorized users getting into the system in the intermediate state.

2. Application security

The application is basically delivered via the internet through a web browser. The problem may occur if there are flaws in the web application, and this may create vulnerabilities for the software as a service application (SaaS). It has always been a problem, because traditional security solutions are not protecting effectively against recent threats nowadays. In this case, the web application should be carefully implemented. The strong authentication process is required for the safety of data.

3. Data security and Accessibility

Data security is a common concern in the proposed scheme. From the proposed idea, it shows that the data are processed and stored in the proper encrypted form. Despite the fact above, it is still a big challenge because users have to rely on the service providers for the appropriate security. In addition, accessing the web application over the internet makes access from any device; information stealing in the intermediate state is still a problem when the file is being encrypted. The proposed scheme is still facing the data stealing problem, which may occur when a user's file is waiting to be encrypted.

V. CONCLUSION

In this paper, a design of security framework for data privacy in e-Health system is proposed. This approach can be applied to other systems as well for security purpose. The main idea of this paper is that files stored in the cloud storage should be properly encrypted. The reason why e-Health system is concerned is because most of the data stored in e-Health system are considered sensitive information; such as health records, prescriptions, etc. In this period of time, several patients have started to use e-health system, considering the convenience of services delivered and cost reduction. The popularity has abruptly been increasing due to a wide range of services. From the system administrator's perspectives, not only protecting privacy of patients is considered a difficult task, but also building trust of patients in e-health. In the future work, key management web service is to be studied and included in the proposed framework. The security breaches mentioned in the section IV are to be solved.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant number: 2013-071188. And it was also supported by the BB21 project of Busan Metropolitan City

REFERENCES

[1] R. Agrawal, A. Kini, K. LeFevre, A. Wang, Y. Xu, D. Zhou, "Managing Healthcare Data Hippocratically", Proc. Of ACM SIGMOD International Conference on Management of Data, Paris, France, June 2004

[2] Apaporn Boonyarattaphan, Yan Bai, Sam Chung, "A Security Framework for e-Health Service Authentication and e-Health Data Transmission", Institute of Technology, University of Washington, Tacoma 2009

[3] "Web Services Glossary". W3C. February 11, 2004. Retrieved 2011-04-22.

[4] S.Han, G. Skinner, V. Potdar, E. Chang, "A Framework of Authentication and Authorization for e-Health Services", Proc. Of the 3rd ACM workshop on secure web services, pp.105-106, November 2006

[5] Kamara, S., & Lauter, K. (2010). Cryptographic cloud storage. In Financial Cryptography and Data Security (pp. 136-149). Springer Berlin Heidelberg

[6] Kumar, A., Lee, B. G., Lee, H., & Kumari, A. (2012, October). Secure storage and access of data in cloud computing. In ICT Convergence (ICTC), 2012 International Conference on (pp. 336-339). IEEE

[7] Löhr, H., Sadeghi, A. R., & Winandy, M. (2010, November). Securing the e-health cloud. In Proceedings of the 1st ACM International Health Informatics Symposium (pp. 220-229). ACM

[8] Kandukuri, B. R., Paturi, V. R., & Rakshit, A. (2009, September). Cloud security issues. In Services Computing, 2009. SCC'09. IEEE International Conference on (pp. 517-520). IEEE

[9] Ramgovind, S., Eloff, M. M., & Smith, E. (2010, August). The management of security in cloud computing. In Information Security for South Africa (ISSA), 2010 (pp. 1-7). IEEE

[10] Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication, 800-144