A Privacy-Preserving System based on Format-Preserving Encryption in Mobile Healthcare Environments

Kim Hyung-Uk, Kim Mansik, Chung Hyunsoo and Moon-Seog Jun*
School of Computer Science & Engineering, Soongsil University, Republic of Korea; ddarajaengi@gmail.com, mansik@ssu.ac.kr, hsj6553@ssu.ac.kr, mjun@ssu.ac.kr

Abstract

Background/Objectives: The healthcare industry has been greatly grown based on the system such as EMR and HER. The objective is to prevent the privacy invasion in mobile EMR and HER healthcare environments. Methods: Token system is suggested to prevent the information used in healthcare mobile devices and it communicates with each mobile phone which operates as gateway as well as EHR and EMR. Findings: In this paper, healthcare device information token system is suggested based on the Format-Preserving Encryption (FPE) in the mobile healthcare environment for preventing personal information from being infringed while preserving availability in order to solve an aforementioned issue. Application/Improvements: Format-Preserving Encryption techniques have applications in Fintech, EMR, HER, bank, and credit card company

Keywords: Electronic Health Records, Format-Preserving Encryption, Mobile Health Care, Privacy

1. Introduction

Healthcare industry has been rapidly growing in the global market. According to the report from Gartner in 2013, it was expected for healthcare industry to create added-value worth 285 billion dollar to all over the world by 2020. Especially, it became feasible to effectively proceed the medical research and diagnose by integrating all the medical information in the digital form through Electronic Medical Records (EMR) and Electronic Health Records (EHR). Various types of convenience are currently provided to patients and those in the relevant field in the mobile digital healthcare environment and hence are in a limelight among many of the countries and companies. In fact, America has released ‘draft guidance on mobile medical applications’. In 2013, guideline that more specifically summarized criteria for objects of permission in FDA has been released. In addition, Apple has released open healthcare platform and health kit in connection with apple watches, healthcare-related applications, devices, and hospitals in 2014. Google has presented healthcare platform Google-fit in the Google development competition held in San Francisco, America, in 2014. Furthermore, Samsung Electronics has released healthcare platform SAMI and wearable device SimBand in the form of wrist-band at the VOTB (Voice of the Body) event. However, there have been increasing security threats in various forms including the existing security threat as mobile digital healthcare environment was grown. Especially, malicious hackers or those in related fields approach digitalized system and cause an issue of infringing personal information of users. This paper suggest healthcare device information token system based on Format-Preserving Encryption (FPE) for protecting personal information of users while preserving availability of the system in order to solve aforementioned issues.
2. Related Work

2.1 Mobile Healthcare

In the mobile healthcare environment, mobile phones of a user become a gateway for connecting healthcare devices while communicating with server as shown in Figure 1 unlike existing healthcare environment. Sensitive personal and medical information of a user is collected from various sensor devices and delivered to the server via mobile phones, and server digitalizes delivered information and conveys it to EMR and EHR serves to preserve and use them. Information collected hereof is delivered to the doctor of a user either prescribing for users or being conveyed to those in the related fields for the purpose of research and development. However, identity of each of the devices or personal information of a user is bounded to users. Therefore, there is a chance to infringe privacy as personal information of a user is exposed to malicious hackers or third parties who read the information or even to cause fatal influence such as a threat on the life. There is a need to establish a measure for doctors or those in the related fields to utilize digitalized sensor information while not infringing privacy of a user.

2.2 Format-Preserving Encryption (FPE)

Format-Preserving Encryption (FPE) is a technique that guarantees the cryptographic randomness while producing the token with features identical with characteristics of personal information. In addition, FPE uses encryption key depending on the personal information to improve safety and also encrypts personal information from token and key. Therefore, FPE is appropriate as a protective technique that preserves personal information on the DB.

For example, credit card, Tax ID, and bank account as shown in Figure 2 have various methods in expressing information. However, if encrypting them with a method such as AES not to expose information, it ends up obtaining a value in the form that cannot be related to the original information at all. Therefore, a new system is required to distinguish and identify values from DB in the new format to preserve encrypted data. However, if encrypting them by using FPE method, encrypted data follow the existing format that there is no need to modify existing system or add a new system.

3. Proposed Scheme

In the suggested system, token is produced based on FPE from token-data server in the provisioning stage through safe channel for identity of each of the healthcare devices or personal information as shown in Figure 3. First of all, when mobile gateway delivers medical information of a user to token-data server either from a user or a device, token-data server sets up policies for objects on identification of personal information according to the delivered information such as device ID or personal information.
of a user in the Setting Policy for Personally Identifiable Information Module from Privacy Detection Engine. In the Classification and Rating Settings Module, personal ID information is classified, and grade is setup in each type of information. Hereupon, information becomes available to either EMR or EHR with appropriate authority in the future. In addition, PEP is utilized as shown in the table 1 through Anonymization of Personally Identifiable Information module from Anonymize and Token Engine not privacy of a user to be exposed when EMR or EHR reads the information while making personal ID information anonymous.

### Table 1. Token-Data Server DB

| Device          | Data      | Encrypted data |
|-----------------|-----------|----------------|
| Sphygmomanometer| 8d520-54477 | 5a247-45523    |
| Thermometer     | retbksdf  | sderlkej       |
| Scale           | 76        | 23             |

Anonymous personal ID information is encrypted as shown in the table 2 for them to be safely read by EMR or EHR with authority depending on types and grades of persona ID information and preserved in token-data server DB and also made as token. Authorized EMR and EHR are granted with token from token-data server and are able to read encrypted data. In addition, encrypted DB is updated by lifecycle management depending on the expiration of token granted to EMR or EHR. In addition, only the token value are newly produced without having to newly encrypt data upon necessity while reading new EMR and EHR. Therefore, it is possible to safely protect personal information of a user while preserving availability from EMR or EHR.

### Table 2. Token-Data Server DB

| Token   | Key     | Encrypted data |
|---------|---------|----------------|
| Fslkdhfsd | ****   | Klh3r,sdfns90(Ysk |
| Rkjehekrtd | ****  | AW#$%w,fnas908k |
| bnsbfyw   | ****   | Fgskj3a5r8()OO)@ |

Lastly, Active Control Engine Management module monitors data produced in the Anonymization of Personally Identifiable Information module to prevent a user from being identified and also verify how a user is not identified from token and encrypted data. In the Using Identification and Control module, ID information is classified and controlled to encrypt and preserve data as well as produce token with user identification information in the Token Generation, Storage, and Encryption module. In addition, Privacy Destruction makes sure to destroy user information that is no longer read and have it not to expose in the future when token granted to EMR and EHR is expired, and it becomes the date for destroying information.

### 3. Experimental Results

Suggested FPE-based personal information protection system is designed to utilize PEP and also the existing system for personal information of a use that can be exposed from healthcare device information without infringing privacy when exchanging data in the safe channel and is also token in a manner that only safely authorized EMR and EHR are able to access to. In addition, encrypted token information is produced based on healthcare device information while mapping token with personal information and also decrypted depending on the policies for authorized users as a function of availability.

### 4. Conclusions

Healthcare environment is currently receiving much attention from various countries and companies in all over the world as the growth of ICT and is growing more rapidly according to the emergence of EMR and EHR that can be shared by digitalizing personal medical information. In addition, mobile healthcare environment that can provide healthcare service at any place and time is providing much convenience to users and those in the field of medicine. However, digitalized personal information and healthcare device information make it feasible for malicious hackers or those in the related fields to access to personal information for causing an issue of infringing personal information. Especially, it infringes privacy of a user through exposed medical information or mobile device identification information and also causes a serious threat on lives according to circumstances. This paper has suggested personal information token system based on FPE for preventing personal information from being disclosed while maintaining availability in the mobile healthcare environment to solve an aforementioned issue. It is anticipated to provide safe service in the mobile
healthcare environment in the future through the system suggested in this paper.

5. References

1. Middleton P, Kjeldsen P and Tully J. Forecast: The internet of things, worldwide, 2013. Gartner Research, 2013.
2. Kavitha R, Kannan E and Kotteswaran S. Implementation of Cloud based Electronic Health Record (EHR) for Indian Healthcare Needs. Indian Journal of Science and Technology. 2016; 9.3.
3. Fernandez-Aleman JL, Senor IC, Lozoya PAO and Toval A. Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics. 2013; 46(3):541-62.
4. Kumari P Senthil and Nadira Banu Kamal AR. Optimal Integrity policy for encrypted data in secure storage using cloud computing. Indian Journal of Science and Technology. 2016; 9.8.
5. Paschou M, Nodarakis N, Tsakalidis A and Sakkopoulos E. Mobile Healthcare Systems: Generating Dynamic Smartphone Apps to Serve Multiple Medical Specializations. Future. 2013; 10(2).
6. Pathak J, Kho AN and Denny JC. Electronic health record-driven phenotyping: challenges, recent advances, and perspectives. Journal of the American Medical Informatics Association. 2013; 20(e2):206-11.
7. Lu R, Lin X and Shen X. SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency. IEEE Transactions on Parallel and Distributed Systems. 2013; 24(3):614-24.
8. Bellare M, Ristenpart T, Rogaway P and Stegers T. Format-preserving encryption. Berlin Heidelberg, Springer: Selected Areas in Cryptography, 2009; p. 295-312.
9. Lee JK, Koo B, Roh D, Kim WH and Kwon D. Format-Preserving Encryption Algorithms Using Families of Tweakable Blockciphers. Springer International Publishing: Information Security and Cryptology-ICISC. 2014; p. 132-59.