Enhancing Privacy Protection in Steppy Applications through Pseudonymization

Heri Arum Nugroho*, Ary Setijadi Prihatmanto** and Kyung Hyune Rhee*
* Dept. of IT Convergence and Application Engineering, Pukyong National University, Republic of Korea
** School of Electrical Engineering and Informatics, Bandung Institute of Technology, Indonesia
harumn01@gmail.com, asetijadi@lskk.ee.itb.ac.id, & khree@pknu.ac.kr

Abstract

Smart Healthcare System as an Open Platform (Shesop) is an integrated healthcare system and have several features, one of them is Steppy Application. Steppy does count your step and display on Shesop website. In this system security issues are not properly addressed, while Personal Health Record (PHR) patient stored in the cloud platform could be at risk. In fact, the huge electronic information available online, people needs reliable and effective technique for privacy preserving. In order to improve the security of data which are displayed on the Shesop website, so that anyone who access could not tamper without permission. Recently Xu et al. showed a pseudonym scheme using smart card as a solution in e-health systems which uses discrete logarithm problem with cyclic group. In this paper, we adopt their scheme and use it application into smartphone using Near Field Communication (NFC) to construct security in Steppy apps.

1. Introduction

Currently there are many health application based on cloud computing. These system are adopted from Ubiquitous healthcare (uhealthcare) also collect patient health information. These system can be obtain cute prices and have been adopted in many countries, like as USA, Canada, U.K, Korea, and European Union [1]. It has been witnessed that uhealthcare tied to portable devices with extraordinary advantages, mobile healthcare (mHealth) leverage in this systems. Using mHealth patient can periodically collect and upload their Personal Health Record (PHR) on sensor and health apps [2]. In initiatives on healthcare, both Apple and Google have capitalize on a shift toward their consumer in mobile apps. That is Apple Health Kit and Google Fit [3] to provide centralize health data user locations especially for simply tracking steps in following decade.

One of them is application named Shesop. This application is an ongoing research founded by LSKK [4] Institute Technology of Bandung, Indonesia. Shesop support a health society as a whole that begins from the examination of vital signs, data processing and health measurement which is monitored via the website [5] as well as integrated directly with doctors, the hospitals, the pharmacies, and the solutions in outcomes problem in healthcare through the monitoring system and a doctor's examination. Focus area of this research is in four segment, desktop apps, web apps, mobile apps, and wearable devices.

Although all the above system are not implemented yet; we avail downloadable application with improved security features. In this paper we review Steppy application, and propose enhanced security features.

2. Related Work

In this section we present the related work which consist of three important part:

Privacy preserving in the clouds: Several research such as in [6], [7], [8] proposed novel algorithm on the cloud for effective user privacy and authentication process. To support them, they give similar concept with providing security requirements, system model in the cloud using anonymous user then arranged a protocol as solution.

Privacy preserving in the mobile healthcare: Privacy preserving has been conducted for mobile healthcare emergency. In works [9] [10], they collected PHR patient using smartphone and multiple sensor. Moreover, in [11] Zhang et al. proposed security and privacy protection for mobile healthcare network from the perspective of quality of protection (QoP).

Pseudonymization in the healthcare: In [12], Aleman et al. investigated 13 articles with pseudo anonymity technique in electronic health record (EHR) systems. They describe that pseudonymization is conversion personal data then replacing using pseudonym. It cannot be associated with identification without knowing key secret. Furthermore in [13], Xu et al. propose pseudonym scheme for encryption and authentication EHR patient then store to the cloud. It is to secure privacy patients when they conduct an activities within healthcare systems, user and the cloud provider.

3. Motivation

It is evident that Satria et al. [14] did not discuss about privacy issues in Shesop. However security aspect is very important, particularly in healthcare that involves many parties. In [15] the author proposed several threats in the uhealthcare system, identity threats of patient, access threats to PHR or EHR patients, and disclosure threats of data at rest and transit. Therefore we also we also need to consider a wide range of crimes that may occur in this field, such as can be done by patient himself / herself, by people in the health network, and from outside the network. Based on that reasonable aspect we suggest a pseudonymization for enhancing security in the Steppy application.

With above motivation, we would prefer to increasing security between user and cloud and make the following contribution:

a. We review the existing Shesop system,

b. We present on details for Steppy communication,
c. We describe the security requirement for the architecture,
d. We present the approach to tackle the security requirement,
e. We present a pseudonym algorithm to preserve the identity of users.

4. Review of Current Steppy Application

4.1. Architecture Overview

Figure 1 shows architecture of Shesop system [14]. There are five main parts which are the hospital, the pharmacy, the vehicle, the portable and home (consist of smart watch, smart chair, smart mouse, steppy, and smart mirror), then the cloud server. For the user there are two categories, the professional is person who works in healthcare system and the normal user.

Steppy is an application for counting your steps that is integrated with Shesop. The application module aims the following:

Figure 1. Shesop Architecture

a. User can download apps in the Google play [16] and create an account on the website using Android downloaded applications.
b. For instance, the application is used for collecting steps and it's connected in the website and database. Thus, data collected by Steppy application can be displayed in the website [17] as shown in Figure 2.

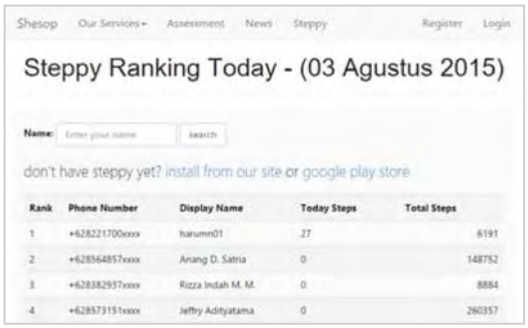

Figure 2. Steppy information in Shesop website

Looking at the current application, we make the following recommendation:

a. For example in Fig 2, the "Display Name" of any registered user is visible on the website, which might not preserve the privacy of every user.
b. The apps doesn't provide details on how to collect upload securely the data in the cloud server.

4.2. System Model of Steppy and Assumption

We introduce our proposed system model in Fig 3. This model consist of three entities, trusted authority (TA), cloud server (CS), and user. List of assumption and functionalities are listed.

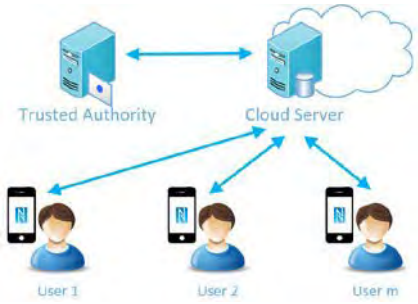

Fig. 3 Details of Steppy communication

- Trusted Authority (TA). It is neutral entity, which has responsible for system security on behalf of users. TA is fully trusted because of perform as government health administration.
- Cloud server (CS). It is a server which provide data storage or computing services. CS is an entity, managed by cloud service provider. The cloud server receives and stores user's PHRs. In this case we assume CS is trusted.
- User. An individual or group entity. They use NFC which is embedded in smartphone. It also included Steppy apps as monitoring devices to collect tracking step.

4.3. Security and Privacy Requirements

Security requirements needed to protect the user's true identity as follows:

- Identity privacy preserving: The real identity of user who registered should not be revealed and explicit seen.
- Unlinkability: The user session of uploading data information from Steppy should not be linked to his previous or later upload.
- Confidentiality: The Steppy data sent from the mobile to the cloud should be confidential. No attacker can reveal the information.

5. A Pseudonym Scheme

5.1. System Setup

Each user generates a major secret key (MSK) using their smartphone which is only known by the user himself. MSK is very important to the patients because it consists of private information such as email, phone number, display name, password, age, gender, height, and weight. This systems used NFC to store and protect the MSK. NFC is employed Secure Element (SE) in the NFC Card emulation mode for encrypting and decrypting private data. NFC behaves like a smart card [18] which is embedded in the NFC chip [19].

To use Steppy a user must register in sign up menu. It important to produce a strong password (is better if unique and memorable), if the password can be compromised by other person or being hacked, then your private information can be accessed.

A pseudonym scheme was proposed by Xu *et al.* [20] which is raised from Discrete Logarithm Problem (DLP) with cyclic group. Allowing DLP we need a prime number p, a generator α of Z_p^* (Z_p^* is a multiplicative group module p), an element β Z_p^* to find integer x, $0 \leq x \geq p - 2$, such that $\alpha^x = \beta \pmod p$. In this case user chooses k-bit prime integer q (k no less than 160 bits), another prime number p (the size around 512 bits), both of them can satisfy $q|\ (p-1)$. Then user produces g is a generator of subgroup G_q. Selecting a random element x G_q into the NFC, results into MSK= [x, g, p, and q]. Given g then select randomly h from G_q (h G_q), computing integer x is become not easy such that

$$g^x = h \pmod p$$

Sometimes we will drop the "mod p" arithmetic part of G_q to ease the notation. Furthermore to generating pseudonym, user can compute

$$PID = g^{MSK} \bmod p$$

The computation has been done at smartphone devices of patient's. The *PID* is sent to the systems and it will be used to authenticate if a user want to login in the Steppy.

In order to design this protocol, we used notation in the table 1.

Table 1. Notation used in our protocol

Notations	Descriptions
PID_i	Pseudonym for user
ID_i	The user identity
PW_i	Password
a, b	Default value of PID
MSK	Major Secret Key
EK	Encryption Key
‖	The concatenation operation

5.2. Algorithm for Generating PIDs

We define PID as (a_0, b_0) which (0, 0) for all as default. We assume user already can generate and use previously PID ($PID_1, PID_2, \ldots PID_i$), for $i + 1^{th}$ from PID_{i+1} which is generated from concatenation operation.

INPUT: $PID_0\ (a_0, b_0), i, IDi, PW_i, MSK$ (to be authenticated by Steppy apps)

OUTPUT: PID_{i+1}, EK_{i+1}

$EK_{i+1} = KHash, (i + 1 \parallel a_0 \parallel b_0, \text{x})$, where $KHash$ is a hash function by key x

$a_{i+1} = g^{EK_{i+1} + Hash\ (a_0 \parallel b_0)\ mod\ q}$, $b_{i+1} = a_{i+1}^x$

$PID_{i+1} = Hash(a_{i+1} \| b_{i+1})$

The user identity, password and major secret key used as input in apps as well as to authenticate those application. For output, last numbers PID_i that has been used should be stored in the Shesop system. Then we can use EK_{i+1} with hash function as an encryption key to secure private contents. Index of PID_{i+1} will be generate for a new pseudonym.

5.3. Algorithm for Reproducing PIDs

Reproducing pseudonym and encryption key is undertaken in accordance with this algorithm.

INPUT: $PID_0 = (a_0, b_0), i, IDi, PW_i, MSK, last$ (the order number of last used pseudonym PID_{last})

OUTPUT: $PID_1 \sim PID_{last}, EK_1 \sim EK_{last}$

for $i = 1\ To\ last\ Do\ EK_i = KHash, (i \parallel a_0 \parallel b_0, x)$,

$a_i = g^{EK_i + Hash\ (a_0 \parallel b_0)\ mod\ q}, b_i = a_i^x$

$PID_i = Hash(a_i \parallel b_i)$

Reproducing PID algorithm shows if the old PID_1 will be replace with the last PID_{last}, similarly in encryption key EK. Both can reproduced in a loop executes.

5.4. Protocol for Verifying the Ownership of Steppy

After generating and reproducing PID, we need to verify our protocol between users U to cloud server CS when Steppy data is uploaded. Arrow notations is to define the process of sending messages.

INPUT: a Steppy entry PID in cloud; p, q of the user's Password and SK are known by the cloud

OUTPUT: Yes or No

U → CS: User sends (a, b) as a defaut $PID = Hash\ (a \parallel b)$

C: checks PID? $= Hash\ (a \parallel b)$. If not equal, C returns No, otherwise $continues$.

U → CS: User randomly chooses s, then calculate and sends $(A = a,\ B = a^s\ mod\ p)$.

CS → U: choose cloud as random then sends c

U → CS: computes and send $y = s + cx\ mod\ q$

CS: cheks $a^y\ ? = Bb^c mod\ p$. If the result Yes, then C returns yes, if not CS returns No.

By using above protocol, users can give response to the server if they has secret x which is produced from G_q discrete logarithm problem.

6. Evaluation

According to basic requirements of Steppy review, we analyze proposed protocol.

- Identity privacy preserving

Users are advised to use strong password when registering application. Then they are generated his pseudonym which needs the patient's MSK. It is not impossible to generate PID in same time by knowing username from different users, because PID is only known by him/her. Besides that, PID encrypted using key hash function $KHash$ it will change independent input. This was made to create and then displays pseudonym on the site.

- Unlinkability

Before uploading user information, the user will get a pseudonym different from before PID_{last}, it's mean

no connection with the previous session. It is very difficult for user to generate similar input.

- Confidentiality

The protocol is designed to verify the authenticity personal evidence C: checks PID?. Cloud will check PID is equal or not with MSK that is known as input are known in the cloud. After this process, verifier can learn about information of patient. After that random value it is used as a guard in replay attacks from attackers.

7. Conclusion and Future Works

In this paper we endeavor to address the privacy issues in Shesop application. We reviewed the current application then we make recommendation to propose a pseudonym scheme for improving user privacy. We further discussed a pseudonym scheme to be apply on the Steppy apps based on the aforementioned security requirements. The security analysis confirms the enhanced security features of Shesop. Moreover, the proposed protocol ensures that true identity of user can be more secure than before, especially when data displays in website.

This protocol is small pieces of security part in Shesop system, so we will continue to review not only in Steppy but also in overall system. From this review we want to seek a landscape of practice to discover further solution in the systems. This system is still under construction by adding necessary features and implement current function. We hope in this implementation should give more practical advices and can be used to create a sample framework in to helping people based on healthcare.

Acknowledgment

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. NRF-2014R1A2A1A11052 981)

References

[1] A. Abbas and S. U. Khan, "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds," *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 4, pp. 1431 - 1441, 2014.

[2] L. Guo, Y. Fang, M. Li and P. Li, "Verifiable Privacy-Preserving Monitoring for Cloud-assisted mHealth Systems," in *IEEE Conference on Computer Communications (INFOCOM)*, Hongkong, 2015.

[3] C. d. Looper, "Google Fit vs. Apple HealthKit: Which Health Platform Is Best Choice?," Tech Times, 16 December 2014. [Online]. Available: http://www.techtimes.com/articles/22260/20141216/google-fit-vs-apple-healthkit-health-platform-better-draft.htm. [Accessed 30 July 2015].

[4] LSKK Group , "Grup LSKK - ITBCreative, Innovative, Competence, Professional," Institute Technology of bandung, [Online]. Available: http://www.lskk.ee.itb.ac.id/about-us. [Accessed 20 August 2015].

[5] LSKK ITB, "Shesop," [Online]. Available: shesop.org. [Accessed 15 August 2015].

[6] L. Malina, J. Hajny, P. Dzurenda and V. Zeman, "Privacy-preserving security solution for cloud services," *Journal of Applied Research and Technology*, vol. 13, no. 1, p. 20–31, 2015.

[7] B. Fabian, T. Ermakova and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Information Systems*, vol. 48, p. 132–150, 2015.

[8] A. Dubovitskaya, V. Urovi, M. Vasirani, K. Aberer and M. I. Schumacher, "A Cloud-Based eHealth Architecture for Privacy Preserving Data Integration," in *IFIP SEC 2015, ICT Systems Security and Privacy Protection*, Hamburg, Germany, 2015.

[9] R. Lu, X. Lin and X. (. Shen, "SPOC: A Secure and Privacy Preserving Opoturnistic Computing Framework for Mobile-Healthcare Emergency," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 3, pp. 614 - 624, 2013.

[10] J. Zhou, X. Lin, X. Dong and Z. Cao, "PSMPA: Patient Self-Controllable and Multi-Level Privacy-Preserving Cooperative Authentication in Distributed m-Heathcare Cloud Computing System," *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, vol. 26, no. 6, pp. 1693 - 1703, 2015.

[11] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen and H. Luo, "Security and privacy for mobile healthcare networks: from a quality of protection perspective," *Wireless Communications*, vol. 22, no. 4, pp. 104 - 112, 2015.

[12] L. Aleman, I. Senor, P. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541-562, 2013.

[13] J. Camenisch, M. Dubovitskaya, R. R. Enderlein, A. Lehmann, G. Neven, C. Paquin and . F. S. Preiss, "Concepts and languages for privacy-preserving attribute-based authentication," *Journal of Information Security and Applications*, vol. 19, no. 1, pp. 25-44, 2014.

[14] A. D. Satria, A. S. Prihatmanto and T. Mardiono, "Shesop Design and Implementation as a Smart Healthcare System Service," in *International Conference on Information Technology Systems and Innovation (ICITSI)*, Bali, 2014.

[15] S. Lee, H. Kim and S.-W. Lee, "Security Concerns of Identity Authentication and Context Privacy Preservation in uHealthcare System," in *International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2013 14th ACIS*, Honolulu, HI, 2013.

[16] ShesopTeam, "Google Play," [Online]. Available: http://play.google.com/store/apps/details?id=org.lskk.shesop.steppy. [Accessed 17 August 2015].

[17] Shesop LSKK ITB, "Step Ranking Today," [Online]. Available: http://shesop.org/steppy. [Accessed 03 August 2015].

[18] N. Elenkov, Android Security Internals: An In-Depth Guide to Android's Security Architecture, San Francisco: No Starch Press, Inc., 2015.

[19] V. Coskun, B. Ozdenizci and K. Ok, "The Survey on Near Field Communication," *Sensors* , vol. 15, no. 6, pp. 13348-13405, 2015.

[20] L. Xu, A. B. Cremers and T. Wilken, "Pseudonymization for Secondary Use of Cloud Based Electronic Health Records," in *The ASE International Conference on Information Privacy Security Risk and Trust*, United States Of America, 2014.