Secure E-Health: Managing Risks to Patient Personal Identity

Haryadi Amran D.
Mike Yuliana
Reni Soelistijorini
Amang Sudarsono
Electronic Engineering Polytechnic Institute of Surabaya, Indonesia

doi: 10.19044/esj.2017.v13n24p377 URL:http://dx.doi.org/10.19044/esj.2017.v13n24p377

Abstract

As we are becoming a digital society, it is very important for us to protect the security of personal identity in any transactions. One of the efforts to maintain the security of personal identity is by unrevealed our data more than necessary. Anonymous credential allows an organization to give a credential to a user. This credential consists of user attribute such as address and date of birth. By using this credential, the user can prove the ownership to the third party without revealing the information that contained in credential information more than necessary. This paper proposes secure e-health system that focuses on proving protocol to reveal and prove some of the patient attributes while others remain hidden, so the security of personal identity more awake. The experimental results showed that the computational time of each proving protocol less than 1 second.

Keywords: Identity, anonymous, credential, attribute, e-health

Introduction

Currently, there are many using the Internet to access a variety of information about e-commerce, e-banking, and e-health, so the number of electronic transactions is increasing. One of the efforts to secure transactions is authentication by a variety of media including mobile phone, RFID tags, and also electronic identity card. The authentication mechanism requires the information of user's personal identity, and this leads to reduced privacy of users because the transactions can be linked. Lack of privacy is a big problem in the case of trust of the user.

Anonymous credential is a technology that allows an organization to give a credential to a user (Bichsel *et.al*, 2009). This credential consists of user attribute such as address and date of birth. By using this credential, the user can prove the ownership to the third party without revealing the information that contained in credential information more than necessary (Yuliana *et.al*, 2014). For instance, the user can prove the ownership of a credential that contains the user aged over 21 by using an ID card, by not revealing other data unnecessary. This is the reason why anonymous credential becoming very popular because the system can minimize the misuse of data by parties who are not responsible.

There are many types of research about anonymous credential with various methods or algorithms (Yuliana *et.al*, 2015). In addition to the basic functions of an anonymous credential, there is some research on the development of anonymous credentials such as enhancement of proving attributes (Belenky *et al*, 2009), an efficiency of coding attributes (Sudarsono *et al*, 2011), and implementation on Java card (Camenisch *et al*, 2008). However, that research only focuses on the computational complexity of each scheme, rarely that focus on the implementation and performance of the system.

In this research, it will be proposed secure e-health system that can improve the security of personal identity using anonymous credential. This system allows the user to reveal and prove some of the attributes while others remain hidden not only using CL signature but also by logical relations proof that includes AND, OR, NOT relations on several attributes, so the security of personal identity more awake.

We structure the remainder of this paper as follows. In section 2, related works of personal identity are described, and logic relation proof will be explained. In section 3, we describe secure e-health system design. The proposed secure e-health system will be discussed in section 4. A prototype implementation and performance measurement will be tested at section 5. Finally, we conclude our paper at section 6.

Related Works

Some research discusses the authentication system to secure personal data (Maji *et al*, 2011), and also anonymous authentication in e-health system which satisfies patient's personal information protection (i.e., health status information) from other patients, doctors, or pharmacists using Anonymous Credential System based CL signature and construct the system by Java programming language (Yuliana *et.al*, 2014).

The other authors extend the anonymous credential such that selection of attributes disclosure becomes more efficient by encoding attributes as prime numbers (Guo *et al*, 2013). This method provides significant advantages for a device that has limited computing capabilities such as smart card. Some other research also discusses the efficiency of attributes, thereby reducing computational complexity (Guo *et al*, 2014).

Anonymous credential system allows users to prove the ownership of the credential, by minimizing the disclosure of information. Some research extends proving protocol of anonymous credential based CL-signature with logic relation proof that includes AND, OR and NOT (Guo *et al*, 2014). The results show the complexity of computational is constantly based on the amount of exponentiation and pairing. Other researchers discuss security in e-health systems that focused on the security of e commerce, not personal identity (Androulaki *et al*, 2011).

Logic Relations Proof

Anonymous system consists of several rules for issuers, recipients, users, and verifiers. On issuing protocol, credential created by the issuers, and recipients will prove the ownership of credential by using proving protocol to the verifiers. Assumed users obtain CL credential that consists of E, for example, signature(A, e, v) on the message m_0 and m_1 where $m_1 = E$.

<u>AND Relation</u>

Users convince the verifier that credential contains an attribute with a specific value by using AND relation. Assumed attribute encode with prime e_j, proving that can be done to convince the verifier that e_j part of E is:

$$\begin{aligned} &PK\{(\varepsilon, v', \mu_0, \mu_1'): \\ &\qquad Z \equiv \pm R_0^{\mu_0}\left(R_1^{e_j}\right)^{\mu_1'} A'^{\varepsilon} S^{v'} (mod\ n) \wedge \\ &\qquad \mu_0 \epsilon \pm \{0,1\}^{l_m} \wedge \mu_1' \epsilon \pm \{0,1\}^{l_m - l_t} \wedge \\ &\qquad \varepsilon \in [2^{l_e - 1} + 1, 2^{l_e} - 1]\} \end{aligned} \tag{1}$$

n is 2 primes and t to be worth ± 1. If $Z \equiv \pm R_0^{\mu_0} R_1^{E} A'^{\varepsilon} S^{v'}$ then $R_1^E = \left(R_1^{e_j}\right)^{\mu_1'}$ and $E = e_1 \mu_1' (mod\ p'q')$, so $E = e_j \mu_1'$ to be worth integer and e_j is a factor of E.

If there are some attributes that encode with primes e_i, e_j, e_l then proving that can be done to convince the verifier e_i, e_j, e_l part of E is :

$$\begin{aligned} &PK\{(\varepsilon, v', \mu_0, \mu_1'): \\ &\qquad Z \equiv \pm R_0^{\mu_0}\left(R_1^{e_i e_j e_l}\right)^{\mu_1'} A'^{\varepsilon} S^{v'} (mod\ n) \wedge \\ &\qquad \mu_0 \epsilon \pm \{0,1\}^{l_m} \wedge \mu_1' \epsilon \pm \{0,1\}^{l_m - 3l_t} \wedge \\ &\qquad \varepsilon \in [2^{l_e - 1} + 1, 2^{l_e} - 1]\} \end{aligned} \tag{2}$$

<u>NOT Relation</u>

Users convince the verifier that credential does not contain an attribute with a specific value by using NOT relation. Proving that $e_j \nmid E$ can be done by showing that $aE + be_j = 1$, where a and b would not exist if

$e_j|E$. After getting a value of a and b, users generate random number r and compute commitment $D = g^E h^r mod\ n$ to be sent to the verifier.

$$\begin{aligned} &PK\{(\varepsilon, v', \mu_0, \mu_1, \alpha, \beta, \rho, \rho'): \\ &\quad Z \equiv \pm R_0^{\mu_0} R_1^{\mu_1} A'^{\varepsilon} S^{v'} (mod\ n) \wedge \\ &\quad D \equiv \pm g^{\mu_1} h^{\rho} mod\ n\ \wedge g \equiv \pm D^{\alpha} (g^{c_j})^{\beta} h^{\rho'} mod\ n\ \wedge \\ &\quad \mu_{0,}\mu_1 \epsilon \pm \{0,1\}^{l_m} \wedge \varepsilon\epsilon[2^{l_e-1}+1, 2^{l_e}-1] \end{aligned} \qquad (3)$$

From $D \equiv \pm g^{\mu_1} h^{\rho} mod\ n$ and $g \equiv \pm D^{\alpha} (g^{e_j})^{\beta} h^{\rho'} mod\ n$, it could be calculated $g \equiv \pm g^{\mu_1 \alpha} h^{\rho\alpha} (g^{e_j})^{\beta} h^{\rho'}$. If user calculates $log_g h$ then $\mu_1 \alpha + e_j \beta = 1$. α and β will exist if e_j and μ_1 are co-prime so $e_j|\mu_1$. Because μ_1 contained in CL signature, then it can be concluded that e_j is not one of the attribute that encodes in μ_1.

OR Relation

Users convince the verifier that credential contains one of the attributes with a specific value by using OR relation. Proving that credential contains one of the attributes $\{e_1, \ldots, e_l\}$ could be done by sending Commitment *D* to verifier using this protocol:

$$\begin{aligned} &PK\{(\varepsilon, v', \mu_0, \mu_1, \alpha, \rho, \rho'): \\ &\quad Z \equiv \pm R_0^{\mu_0} R_1^{\mu_1} A'^{\varepsilon} S^{v'} (mod\ n) \wedge \\ &\quad D \equiv \pm g^{\mu_1} h^{\rho} mod\ n\ \wedge g^{\prod_i^l e_i} \equiv \pm D^{\alpha} h^{\rho'} mod\ n\ \wedge \\ &\quad \mu_{0,}\mu_1 \epsilon \pm \{0,1\}^{l_m} \wedge \varepsilon\epsilon[2^{l_e-1}+1, 2^{l_e}-1] \end{aligned} \qquad (4)$$

Credential contained an attribute *e*, so we get the value of *a* where $ae = \prod_i^l e_i$. If e is not in the list *a* then *e* does not divide the product.

The Proposed Secure E-Health System Design

In this section will be proposed a system that can improve the security of personal identity by using anonymous credential system.. This system allows the user to reveal and prove some of the attributes while others remain hidden, so the security of personal identity more awake.

Privacy Requirements

The ability of the existing system in the hospital to maintain the privacy of personal identity of patients will increase the trust. Doctors only know partial information of the patient's personal identity.

Security Requirements

There are two types of attributes, namely strong and weak attributes. Strong attributes are unique for each user such as address, and phone number while weak attributes could be the same for each user such as name, and blood type. In this system, the strong attributes contain sensitive information that remained hidden when proving while weak attributes will be revealed. Disclosure of weak attributes must fulfill the security requirements where the user can select the attributes that will be revealed to prevent the disclosure of more information than required.

Proof of Attributes Protocol

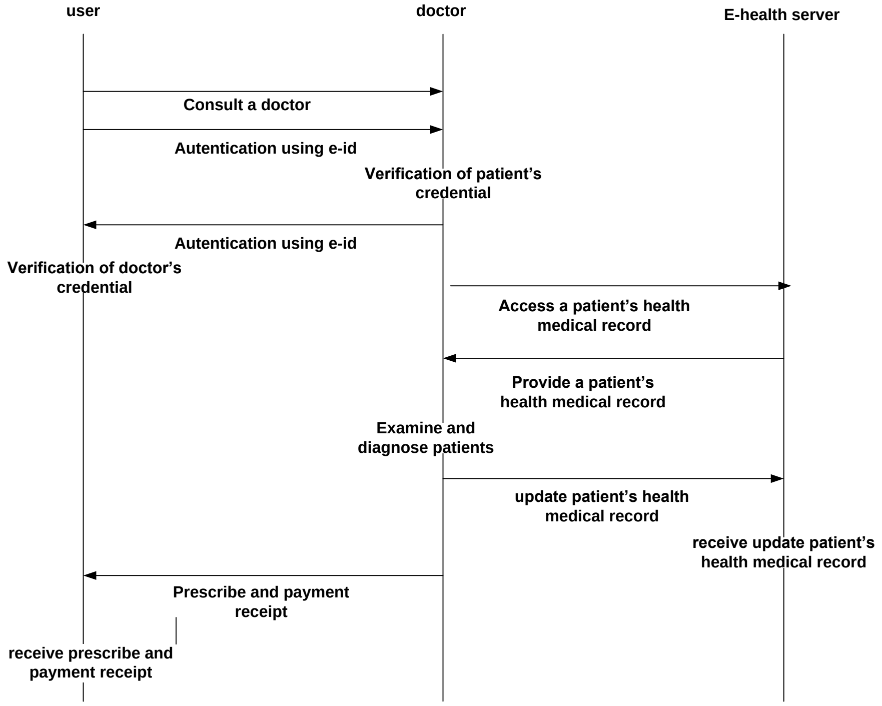

user
doctor
E-health server
Consult a doctor
Autentication using e-id
Verification of patient's credential
Autentication using e-id
Verification of doctor's credential
Access a patient's health medical record
Provide a patient's health medical record
Examine and diagnose patients
update patient's health medical record
receive update patient's health medical record
Prescribe and payment receipt
receive prescribe and payment receipt

Figure 1. Protocol of consult a doctor.

In this research, a credential from several attributes loaded into e-id, where e-id is obtained during the process of registration and used for the authentication process. Fig. 1 shows the protocol when consulting a doctor. It can be seen that the doctor can see the patient's health medical record if the authentication success performed by doctors and patients.

Prototype Implementation and proof of attributes testing

In this section will be explained the implementation of the prototype system, the results of testing proving algorithms and system performance. Specifications of Personal Computer can be seen in Table 1 and RFID reader and tag can be seen in Fig. 2.

Table 1. Specification of Personal Computer

Specifications	Remarks
Operation System	Microsoft Windows 7 Professional 64-Bit (Build 7601)
Processor	Intel Core i5-2450M (2.50 GHz, 3MB L3 Cache) (4 CPUs)
Memory	8 GB RAM

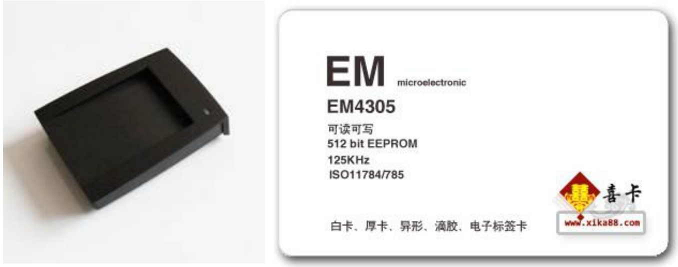
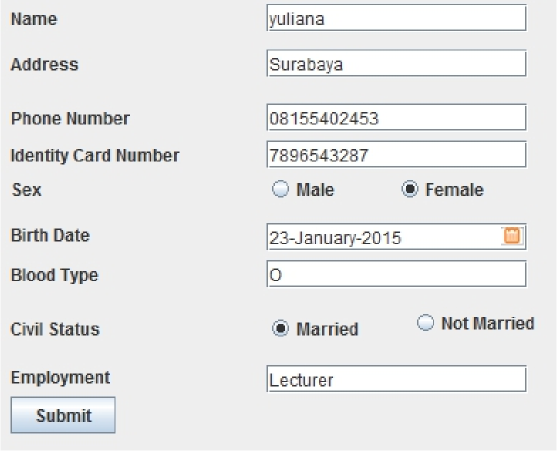


Figure 2. RFID reader and tag

Attributes are information that used during the registration process, in which the attributes information consists of name, issuance modes (known, hidden) and type (int, String, enumeration). Figure 3 shows the registration form, in which the attributes that are used include name, address, phone number, identity card number, sex, birth date, blood type, civil status, and employment. Address, phone number, and identity card number are strong attributes and the others are weak attributes. the issuance mode of strong attributes are hidden and weak attributes are known, so the user that acts as prover knows all the attribute values but the verifier only knows weak attributes.



Name	yuliana	
Address	Surabaya	
Phone Number	08155402453	
Identity Card Number	7896543287	
Sex	○ Male	● Female
Birth Date	23-January-2015	
Blood Type	O	
Civil Status	● Married	○ Not Married
Employment	Lecturer	

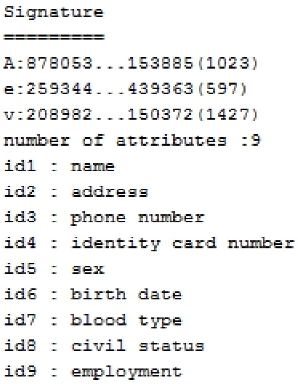
Figure 3. Registration form.

Proof of Attributes Testing

In this section will be performed some testing which includes proof of CL signature, proof of AND, OR and NOT relations.

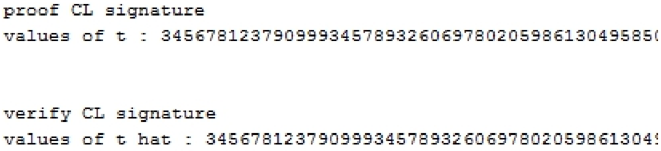
Proof of CL Signature

In this experimental test, it will be proved that the value of A, e, v are the signature of attributes. Fig. 3 show the example of signature from 9 attributes. The value that will be obtained when authentication and verification process is the success are t (proof process) and $\hat{t}$ (verify process) can be seen in Fig. 5. The test results showed that the proof is not rejected.



```
Signature
=========
A:878053...153885(1023)
e:259344...439363(597)
v:208982...150372(1427)
number of attributes :9
id1 : name
id2 : address
id3 : phone number
id4 : identity card number
id5 : sex
id6 : birth date
id7 : blood type
id8 : civil status
id9 : employment
```

Figure 4. Example of signature



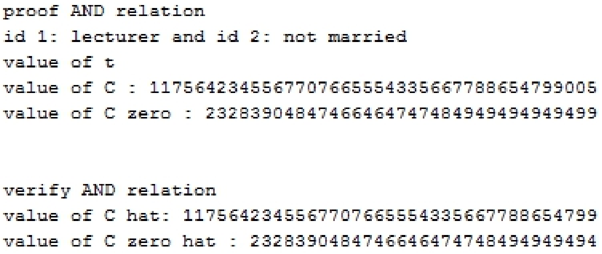
```
proof CL signature
values of t : 34567812379099934578932606978020598613049585


verify CL signature
values of t hat : 3456781237909993457893260697802059861304
```

Figure 5. Proof and verify CL Signature

Proof of AND Relation

In this experimental test, it will be proved that the patient will get medical check fee discount if the patient was a lecturer and not married. The value that will be obtained when authentication and verification process is the success are $\tilde{C}$, $\tilde{C}_0$ (proof process) and $\hat{C}$, $\hat{C}_0$ (verify process) that can be seen in Fig. 6. The test results showed that the proof is not rejected and the patient can get medical check fee discount.



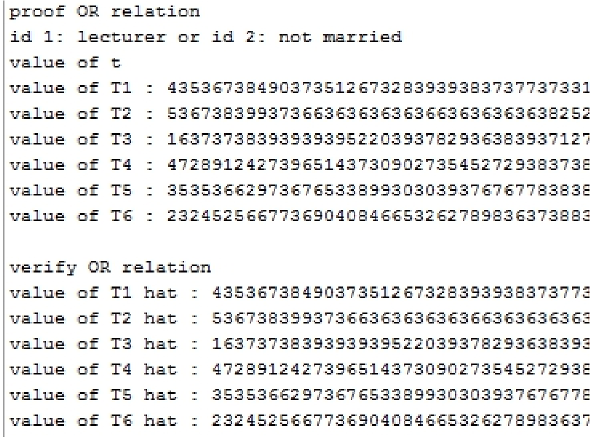
```
proof AND relation
id 1: lecturer and id 2: not married
value of t
value of C : 1175642345567707665554335667788654799005
value of C zero : 23283904847466464747484949494949499


verify AND relation
value of C hat: 1175642345567707665554335667788654799
value of C zero hat : 2328390484746646474748494949494
```

Figure 6. Proof and verify AND relation

Proof of OR Relation

In this experimental test, it will be proved that the patient will get medical check fee discount if the patient was a lecturer or not married. The value that will be obtained when authentication and verification process success is $\tilde{T}_1, \tilde{T}_2, \tilde{T}_3, \tilde{T}_4, \tilde{T}_5, \tilde{T}_6$ (proof process) and $\hat{T}_1, \hat{T}_2, \hat{T}_3, \hat{T}_4, \hat{T}_5, \hat{T}_6$ (verify process) that can be seen in Fig. 7. The test results showed that the proof is not rejected and the patient can get medical check fee discount.



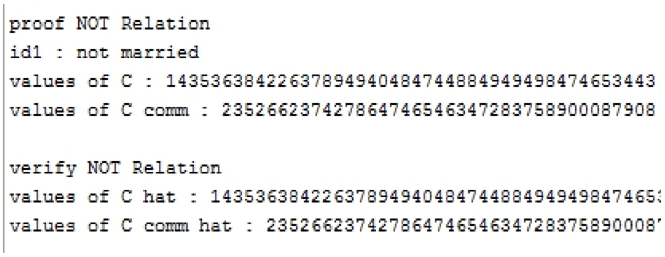
```
proof OR relation
id 1: lecturer or id 2: not married
value of t
value of T1 : 43536738490373512673283939383737737331
value of T2 : 536738399373663636363636636363638252
value of T3 : 16373738393939395220393782936383937127
value of T4 : 47289124273965143730902735452729383738
value of T5 : 35353662973676533899303039376767783838
value of T6 : 23245256677369040846653262789836373883

verify OR relation
value of T1 hat : 4353673849037351267328393938373773
value of T2 hat : 5367383993736636363636366363636363
value of T3 hat : 1637373839393939522039378293638393
value of T4 hat : 4728912427396514373090273545272938
value of T5 hat : 3535366297367653389930303937676778
value of T6 hat : 2324525667736904084665326278983637
```

Figure 7. Proof and verify OR relation

Proof of NOT Relation

In this experimental test, it will be proved that the patient will get medical check fee discount if the patient's civil status not married. The value that will be obtained when authentication and verification process is the success are $\tilde{C}, \tilde{C}_c$ (proof process) and $\hat{C}, \hat{C}_c$ (verify process) that can be seen in Fig. 8. The test results showed that the proof is not rejected and the patient can get medical check fee discount.



```
proof NOT Relation
id1 : not married
values of C : 14353638422637894940484744884949498474653443
values of C comm : 235266237427864746546347283758900087908

verify NOT Relation
values of C hat : 1435363842263789494048474488494949847465
values of C comm hat : 23526623742786474654634728375890008
```

Figure 8. Proof and verify NOT relation

E-Health System Performance

In this section will be tested computational time for proving protocol. There are 3 kinds of schemes, namely testing for revealed, unrevealed and combination. For proving protocol with all attributes revealed, the attributes have issuance mode known, so when authentication process all of these attributes will be revealed to the verifier. Fig. 9 shows the computational time of proving protocol for 2 through 9 attributes. The test results show that the computational time from 2 through 9 attributes do not have a lot of time difference. The highest computational time is 0.8866 seconds occurs when the number of attributes 9.

For proving protocol with attributes unrevealed, the attributes have issuance mode hidden, so when authentication process all of these attributes will not be revealed to the verifier. Fig. 10 shows the computational time of proving protocol for 2 through 9 attributes. The test results show that the computational time from 2 through 9 attributes do not have a lot of time difference. The highest computational time is 0.91 seconds occurs when the number of attributes 7.

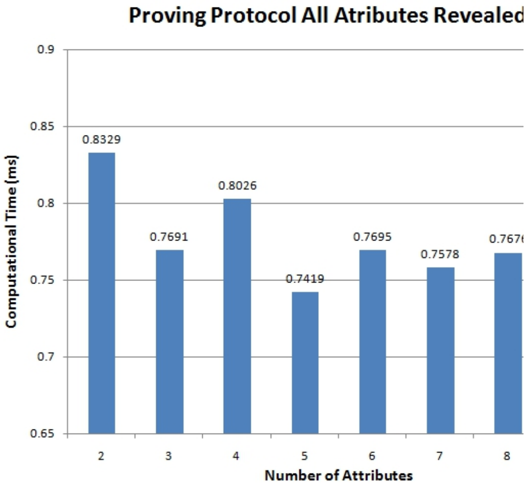


Figure 9. Proving protocol with all attributes revealed

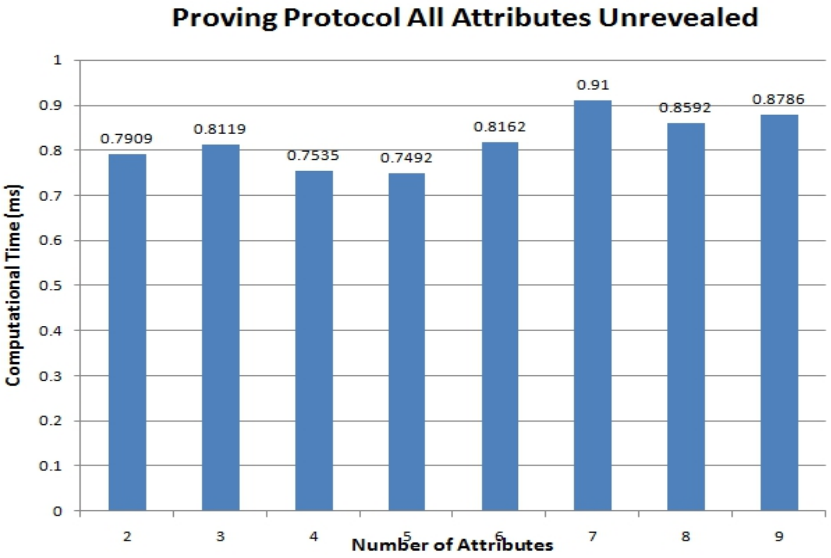


Figure 10. Proving protocol with all attributes unrevealed

For proving protocol with a combination of both attribute, the attributes have issuance mode known and hidden, so when authentication process some of these attributes will be revealed to the verifier and the others remain hidden. Fig. 11 shows the computational time of proving protocol for 2 through 9 attributes. The test results show that the computational time from 2 through 9 attributes do not have a lot of time difference. The highest computational time is 0.8426 seconds occurs when the number of attributes 3.

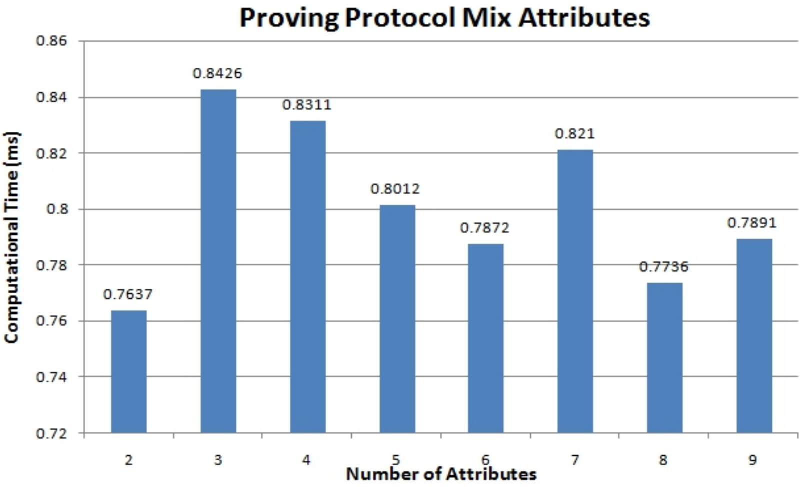


Figure 11. Proving Protocol with mix attributes

Fig. 12 shows the comparison of computational time from 3 kinds of proving protocol, where the results showed that no significant difference in computational time for different number and types of attributes. The computational time of proving protocol is less than 1 second.

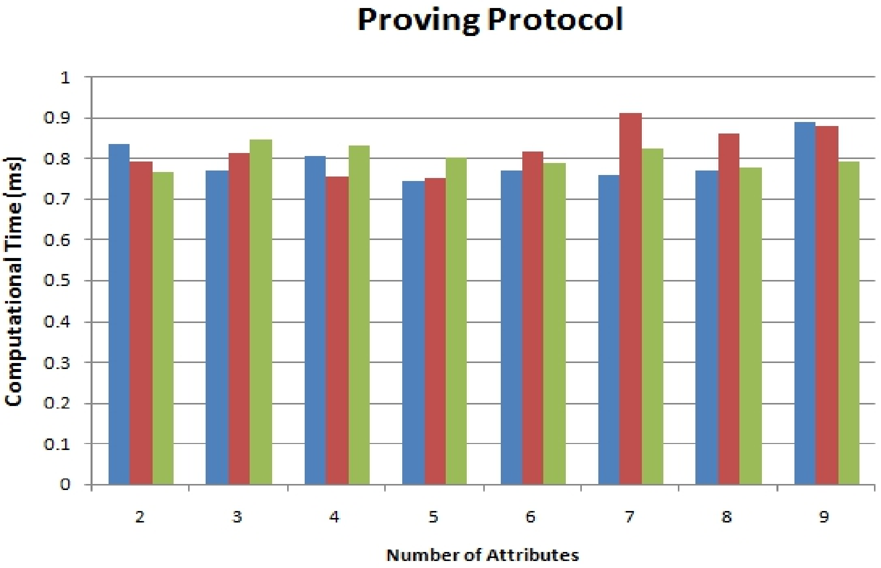


Figure 12. Comparison of 3 kinds of proving protocol.

Conclusion

We proposed secure e-health system design that can be fulfilled the privacy and security requirements. The system allows the user to reveal and prove some of the attributes while others remain hidden, so the security of personal identity will be more secure. Proof attributes testing includes the selection of attributes disclosure, proof of CL signature, proof of AND, OR and NOT relations. The computational time for each proving protocol is less than 1 second. Overall it can be said that the system designed was able to increase the security of personal identity, thereby reducing the misuse of personal identity by unauthorized parties.

Acknowledgment

This research was supported by Ministry of Research, Technology, and Higher Education through Penelitian Produk Terapan Scheme 2017.

References:

1. Bichsel, P., Camenisch,J., Gro, T., & Shoup,V., *Anonymous credentials on a standard java card*, in Proc. ACM Conference on

Computer and Communications Security 2009 (ACM-CCS'09), pp. 600–610, 2009.

2. Yuliana, M., Sudarsono, A. & Nadhori, U.I, *Protection system of client's privacy on e-health services,* In Proc. Of the 8th International Conference on Information and Communication Technology and System (ICTS), pp.291-296 , 2014.
3. Yuliana, M., Pratiarso, A. & Sudarsono, A., *Proof of Attributes Based CL Signature Scheme on E-Health Applications,* in Proc. Of International Conference on Science in Information Technology (ICSITech), pp. 253-258, 2015.
4. Belenky, M., Camenisch, J. & Chase, M., *Randomizable proofs and delegetable anonymous credentials,* in. Proc. Of Crypto, 2009.
5. Sudarsono, A., Nakanishi & T. & Funabiki, N., *Efficient Attribute-based signatures for non-monotone predicates in the standard model*, In Proc. Of the 11th International Symposium Privacy Enhancing Technologies (PETS'11),pp.246-263,2011.
6. Camenisch, J. & Grob, T. *Efficient Attributes for Anonymous Credential*, in Proc. Of ACM Conference on Computer and Communications Security, pp.345-356, 2008.
7. Maji, H.K.,Prabhakaran &Rosulek, M., *Attribute-based signatures,* in Proc.of Cryptographers'Track at the RSA Conference 2011 Topics in Cryptology (CT-RSA'11), pp. 376-392, 2011.
8. Guo, N., Cheng, J., Zhang, B. & Yim, K., *Aggregate signature-based efficient attributes proof with pairing-based anonymous credential,* in Proc. Of Network-based Information System (NBiS), pp.276-281, 2013.
9. Guo, N., Wang, J.,Gao, T. & Yim, K., *Privacy-preserving proof af attributes with CL-Anonymous Credential*, Journal of Internet Services and Information Security (JISIS), volume:4,number:1,pp. 37-46, 2014.
10. Androulaki, E., *A privacy preserving e commerce oriented identity management architecture,* PhD Dissertation, Columbia University, New York, 2011.