Protecting Cloud-Based Home e-Healthcare with Cryptographic Scheme

Ndibanje Bruce[1], Hyun Ho Kim[1], Mangal Sain[2], and Hoon Jae Lee[2]

[1] Department of Ubiquitous IT, Graduate School of Dongseo University, Sasang-Gu, Busan 617-716, Korea
bruce.dongseo.korea@gmail.com, feei_@naver.com
[2] Division of Computer and Engineering Dongseo University, Sasang-Gu, Busan 617-716, Korea
mangalsain1@gmail.com, hjlee@dongseo.ac.kr

Abstract. The emergence of ubiquitous technologies gives rise to huge applications that enable the data accessibility anytime anywhere. Cloud-based home healthcare system is one of researching area of the cloud computing applications. As cloud computing allow the on-demand network to a shared pool of configurable computing resources, patients' data protection is the paramount requirement for the security and privacy to ensure the trustworthiness of the cloud-based home healthcare system. To this end, this paper proposes cryptographic scheme where a patient can encrypt his data before uploading the data to the cloud. To achieve this, we design and implement a healthcare monitoring system to collect patient data and send them to computer. In this experiment we use pulse sensor on arduino board for heart rate measurement. The data collected from the patient can be uploaded to cloud after encryption operations. Only the user with shared private key can decrypt the patient data. Thus, the patient would trust in the cloud infrastructure that supports critical applications for the healthcare system. In addition, the analysis of the proposed scheme ensure the honesty of the cloud provider, since the patient has the ability to control who has access to his data by issuing a cryptographic access credential to data users.

Keywords: cloud, healthcare, cryptographic, credential.

1 Introduction

The cloud offers the potential of easy access to electronic medical records in a medical setting. Quick access to a person‘s medical history could speed up treatment, help to avoid complications, and even saves lives. In addition, the cloud could make it easier for the patients to locate and keep track of their own medical history. However, on the other hand, patient also wants privacy and guarantees that their health information is secure. According to the Health insurance Portability and Accountability Act (HIPPA) regulation, the providers of IT services should first get the trust from consumers and minimize all areas of risks then eHealth cloud can be totally deployed [1].

Y.-S. Jeong et al. (eds.), *Ubiquitous Information Technologies and Applications*, Lecture Notes in Electrical Engineering 280,
DOI: 10.1007/978-3-642-41671-2_95,

Different suggestions to accomplish privacy and access control in eHealth have been published [2-4]. Moreover, assurance of privacy and address privacy issues must be provided by the eHealth systems at different system levels: architectural design, access control, communication protocols, etc. Thus, it is commonly achieved in practice by means of a form of access control or authentication [5-9]. However, typical eHealth systems, especially in future, will be highly distributed and require interoperability of many subsystems. Even if health-care data is well protected and access control is perfectly employed, improperly designed communication protocols for such interoperability will cause information leakage and hence breach users' privacy. So far, security and privacy of communication protocols in eHealth systems is seldom studied in the literature.

The problem addressed in this paper is the confidentiality or trust of cloud providers by the customer. This paper considers a case of patients who wants to upload his data to cloud but because of untrustworthiness, we propose a way where the patient can encrypt his data before uploading it to cloud. Hence, the patient would trust in the cloud infrastructure that supports critical applications for the healthcare system.

The remainder of this paper is organized as follow; Section 2 illustrates the related work while. We develop our method in Section 3 and security analysis is given in Section 4 before concluding in Section 5.

2 Related Work

In order to ensure the security of e-health systems, several different schemes have been proposed. In the following, we provide an overview of some existing security implementations for e-health systems. The patient centred access to secure systems online has been presented in [10]. The authors claim that, initially; it aims to permit patients and health care providers to access health information, even the sensitive data. Their access scheme combines role-based access control, mandatory access control and discretionary access control. The implementation is a patient-centred and centralized approach that stores all the data on a single server.

Different countries have developed and implemented their e-Healthcare System such as electronic Health Card (eHC) system [11-12] in German where each patient has an eHC smartcard as described in the compulsory health insurance system. The main function of eHC is to store the administrative data (for billing with the health insurance), with embedded encryption operations of patient’s records to be saved on HER servers and to give access rights when the data is needed.

Figure 1 shows an advanced model, which not only involves more parties (e.g., health insurances), but also includes some technical means to enforce data security and privacy of EHRs.

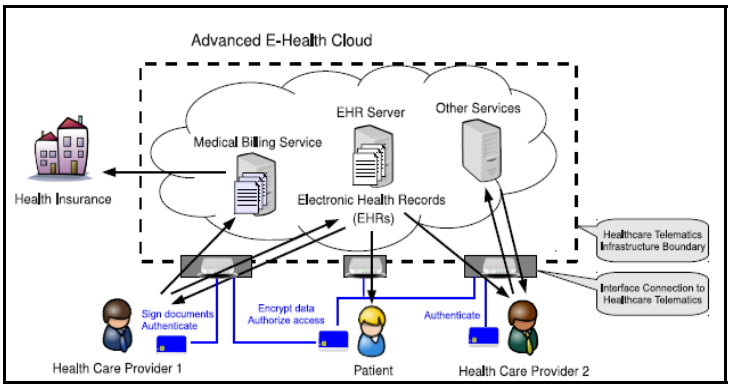


Fig. 1. Advanced E-Health Cloud model

3 Data Collection and Cryptographic Techniques

This section describes the main work of our paper. Details are sketched to show how we designed and implemented a system to collect data from patient and store the data to computer using sensor pulse, arduino board and wireless sensor node and finally how a patient can encrypt this data before upload it to cloud.

3.1 Data Collection Design for eHealthcare System

This subsection describes the architectural design and implementation of the healthcare data collection system using the sensor pulse to measure the heart rate, arduino sensor node to support the wireless technology. Figure 2 shows the process of the pulse sensor set up operations. Partially, we recall the work we did in our previous research [13] and incorporate the cryptographic scheme for the reason that we apply our Healthcare Monitoring Application to cloud computing area. To send the data

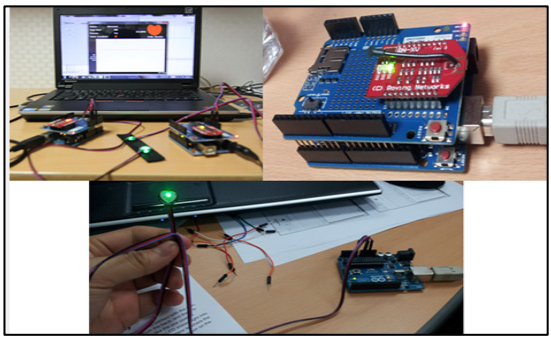


Fig. 2. Pulse sensor and Arduino set up operations

wirelessly, the sensor pulse is connected to the wireless sensor node which uses RN-XV module base on 802.11x protocol micro controller made by Roving Networks. The sensor pulse is first connected to the arduino and then all the set are connected to the computer via an usb cable. In this paper, we focus on the pulse sensor which collects raw data of the heart rate and transmits received data through Wi-Fi connection to the computer.

When the sensor is sensing the heart rate, it sends raw data without any operations of analyzing. To make the raw data understandable by doctors or nurses, we developed software which interpret the raw data to a graph platform. The description of the algorithm is given in Figure 3. It has been observed that changes in heart rate occur before, during, or following behavior such as posture changes, walking and running. Therefore, it is often very important to record heart rate along with posture and behavior, for continuously monitoring a patient's cardiovascular regulatory system during their daily life activity. The algorithm of HR analysis with activity monitoring is shown in Figure 3. Analysis of HR data is done on server for HR status and activity monitoring of patient. After calculating HR parameters, the algorithm goes for their classification for activities monitoring and HR status. If the heart rate is between 60 and 110 bpm and the patient is in rest position then can classify as a normal condition.

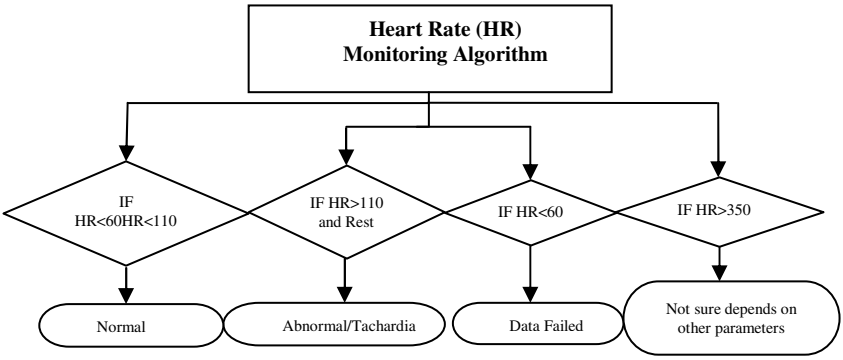


Fig. 3. Analysis of Heart Rate

If heart rate is greater than 110 bpm and patient position is rest then can classify for abnormal. For more precision, abnormal or regular HR, while resting if the HR is between 60 and 100 bpm the person is an adult otherwise if HR goes to 110 he is a baby. Therefore, it is necessary to know about the patient activities during measurement of HR parameter. During moving activity of the person, an HR analysis depends on other parameters also such as blood pressure, temp etc.

The measurement of the heart rate is done by a sensor pulse connected to Arduino as interface between computer and the sensor pulse. And the wireless communication is done by the wireless module connected to arduino wireless shield. The sensor pulse sends raw data and the HR algorithm translates the raw data using HR calculating the code. The result of the HR is given in a graph platform where the doctor or nurse can

easily ready it. Figure 4 gives the result of the HR with 2 scenarios where the HR is between 60 and 110 for the first and HR is below 60 for the second.

For the left graphic, the patient doesn't present any problem from the status which is normal we can see that the HR is 97, and then the alarm condition is green which means no disease. On the right side the status is "fail" because the HR is under 60 in this case the doctor should take further decision for the patient.

Fig. 4. HR result with normal and fail status

3.2 Cryptographic Design for Data Security and Privacy

This subsection presents the method to encrypt the patient's data before sending the data to cloud. We use the data obtained using the method to collect data illustrated in subsection A. Following the semi-trusted situation between consumer and cloud provider, we believe that the cloud providers are honest but curious. Thus any attacker can (un) intentionally initiates a misuse case. Considering those untrustworthily situation, in order to establish trust in the cloud infrastructure to support critical applications (such as healthcare systems), security and privacy should be built in to assure trustworthiness. To do so, cryptographic techniques to build in security and privacy are needed as regards the specific security and privacy challenges for the home healthcare system in the cloud. Figure 5 is an overview of an eHealthcare Information System where a patient can encrypts his HR result and then uploads the ciphertext to cloud, after an authorized person can decrypt the data after downloading.

The patient using his secret key K encrypts his HR result, let us call $<M>$ the data obtained. From his from his device he uploads the ciphertext to the cloud.

$$E_K(M) = C(M) \tag{1}$$

The content of the ciphertext $C(M)$ such as attributes, shared secrets keys and accessibility conditions will define the rights of the authorized person to decrypt the data. If any attacker can access the encrypted data from the cloud he will not be able to read the content because restrictions access embedded into the cipher. Furthermore, shared secret keys are required to access the data.

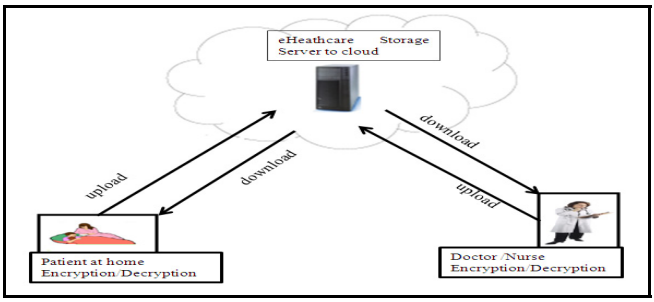


Fig. 5. Encryption and Decryption processes

Ciphertext contents: patient and Doctor attributes. The patient attributes are:Nonce_patient (*Np*), Patient_ID (*Idp*), and TimeValid_patient (*Tp*).The Doctor attributes are: Nonce_Doctor *(NDr)*, Doctor_ID *(IdDr)* and Time_Doctor *(TDr).Ciphertext contents: embedded conditions* OR-AND-NOT. The embedded conditions play the important role to dispatch the rights for viewing the information incorporated into the ciphertext. In addition, the ciphertext *C (M)* can be accessible by everyone. Decryption is only possible *iff* the attribute set of the secret key satisfies the access policy specified in the ciphertext. If the data is encrypted with embedded conditions such as "[Doctor Staff] OR [Practioner AND Family member]", then it can be decrypted with a key containing the attributes [Doctor, Nurse, Wife], but not by a key containing the attributes [Lab Personnel, Financial department]. The cases in the following illustrate the states among many cases.

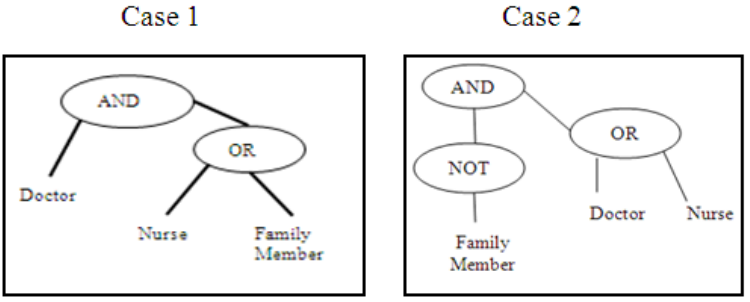


Fig. 6. Embedded Conditions with restricted rights to Family Member

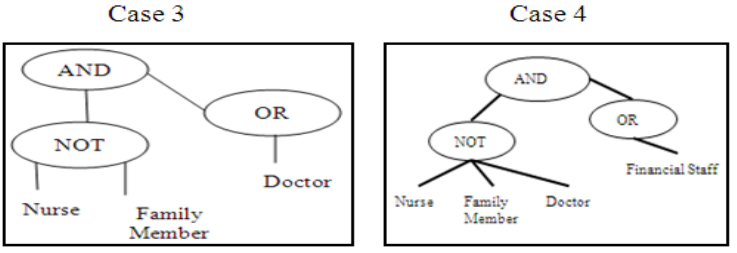
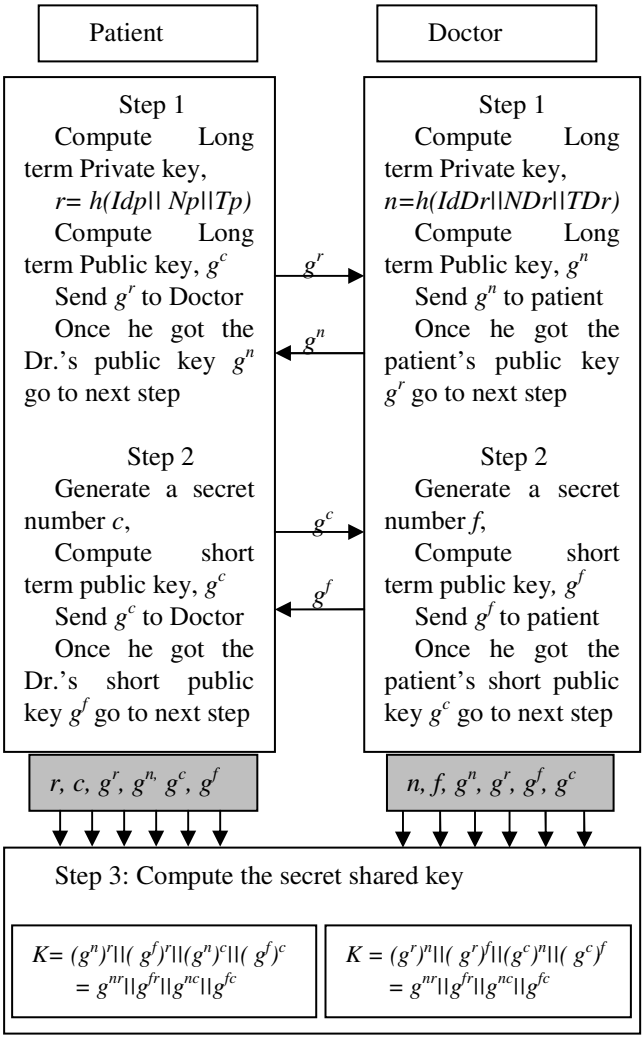


Fig. 7. Embedded Conditions with Access Rights to Doctor and F Staff

As abovementioned, the embedded conditions in the proposed cryptographic scheme define who has the rights to decrypt the patient's records data otherwise the file will be opened in encrypted form. In the system of eHealthcare, we assume that the ciphertext *C (M)* can be accessible by everyone and also the encryption/decryption operations are done into both ways. The accessibility rights from Figure 6 and Figure 7 can be explained like this:

- Case 1: The privileges are granted to all entities, once downloaded the patient's data, they can open it following the cipher embedded conditions
- Case 2: Doctor and Nurse have the rights to decipher the data while family member does not have.



- Case 3: The embedded condition *"NOT"* does not allow the Nurse and Family Member to read the patients' records data. Only Doctor can communicate with his patients.
- Case 4: The only Financial Staff can read the patients data(Data relating to the bills and payment process)

Key Exchange Computation Procedures. The ciphertext C (M) stored by data owner contains the keys and they are computed into the system. They play vital role in our proposed method such as: mutual authentication, data access rights, encryptions and decryption. This subsection describes the fundamental operations to compute the keys.

Once the shared keys computations between patient and Doctor are done, the encryption process of patient data can start whenever the user wants to upload it to the cloud. From the aforementioned operations, we can see that, the keys contain all IDs to identify each entity involved into the exchange and communication flow. In this paper we consider only those attributes and for the future work we will take in consideration others in case of experiment and implementation purposes.

3.3 Access Credential Architectural Principle

The keypoint architectural principle behind the proposed cryptographic scheme is the ability of patient to issue access credentials to Doctor and then he would be trust the cloud provider for his data security and privacy. A credential is a statement that specifies what access rights its holder has with respect to very specific data. The credential is cryptographically signed by its issuer. The possessor of the credential may present it to the issuer to gain access to the data. For the purpose of this work we are using the Key Note Trust Management system [14] which provides us with the necessary credential functionality. In this paper we describe two types of credentials where the patient issue the credentials according to the aforementioned cases (we take Case 1 and Case 3); the holder will have access to all of the data owner's patient records. The credential contains the public keys of the two parties along with the cryptographic signature (shared secret key) verifying the validity of the credential. The specific credential also has an expiration date, invalidating it past that date. Finally the credential has an extra field specifying the type of application the credential is supposed to be used for, in this case cloud computing. Example 1 is a sample credential for allowing the entities in case 1 to read patient records and Example 2 is a sample credential corresponding to case 3 where nurse and family member are not allowed to ready patient's data.

```
Authorizer: Patient_ID
    Local-Constants:
      Patient-ID_KEY="SecretKey||rsa-base64: MIGJb..."
      Doctor-ID_KEY= "SecretKey||rsa-base64: MIGJb..."
      Nurse-ID_Key= "SecretKey||rsa-base64: MIGJb... "
      Family Member-ID_Key= "SecretKey||rsa-base64: MIGJb... "
    Conditions:
    ((app_domain == "CLOUD_COMPUTING") &&
    (Medical Data == "Checkup_Results") &&
    (Permissions == "Access_Read_Only") &&
    (Timevalid <= "20130630")) -> "permit_if_not_Invalid";
    Licensees: Doctor-ID_OR_Nurse-ID_AND_Family member
Signature: "sig-shared-secret-key: QU6..."
```

Example 1: Credential for allowing the entities in case 1

```
Authorizer: Patient_ID
    Local-Constants:
      Patient-ID_KEY="SecretKey||rsa-base64: MIGJb... "
      Doctor-ID_KEY= "SecretKey||rsa-base64: MIGJb..."
      Nurse-ID_Key= "SecretKey||rsa-base64: KI&^%4... "
      Family Member-ID_Key= "SecretKey||rsa-base64: KI&^%4... "
    Conditions:
    ((app_domain == "CLOUD_COMPUTING") &&
    (Medical Data == "EGC-Glucose-Measurements") &&
    (Permissions == "Access_Read_Prescription") &&
    (Timevalid <= "20130625_26")) -> "permit_if_not_Invalid";
    Licensees: AND_Doctor-ID_NOT_Nurse-ID_OR_Family member-ID
Signature: "sig-shared-secret-key: QU6..."
```

Example 2: Credential for allowing the entities in case 3

4 Security Analysis

The scheme is secure to chosen ciphertext-only attack: Data transmissions from patient to cloud as well as from cloud to patient are done with proper encryption. The processes are the same under Chosen Ciphertext Attack (CCA) [15] based on the modification of stored ciphertext to cloud. Such adversaries are permitted to see the ciphertexts for messages of their choice, and (in the public-key setting) to generate ciphertexts on their own. However, the adversary never gets to see the decryptions of any messages. For the reason that the credentials contain hashed secrets parameters $r = h\ (Idp||\ Np||Tp)$ and $n=h\ (IdDr||NDr||TDr)$ to verify the authenticity of the attacker. Nonetheless, for some applications, the adversary will need a stronger definition in which he gets (limited) access to the decryption machinery as well.

The scheme is resistant to the eavesdropping attack: The aim of an eavesdropping attacker is to have the access to the private and sensitive patient's medical data. This attack may be happened between the involved entities during communication and exchange message. To access the data at the health cloud server, an attacker needs to have sufficient attributes to complete the access authentication protocol process *(step1, step2 and step 3)*. Here the shared secret key is made by multiple secrets parameters based on the attributes set. For the non-privacy dataset, he may get access and allowed in our scheme. But he cannot modify the data due to the verification bindings. However, for the patient sensitive data, a unique random number is embedded into the ciphertexts (*Np*) and *(NDr)*. Without knowing that secret number, it is impossible to access the data. Therefore, any attacker cannot successfully launch the eavesdropping even thought sophisticated applications can do that.

The scheme ensures message integrity, non-repudiation, and source authentication: We use the patient's secret key and the session identity to generate the signature playing the session key role $K = (g^r)^n || (g^r)^f || (g^c)^n || (g^c)^f$. The data receiver can verify the signature by using the public parameters of the sender "g^c". This verification ensures the corresponding source authentication. The scheme computes secrets keys "*n*" and "*r*" by computing their hash values of the concatenated message. Only the patient and Doctor know each other their secrets keys which include the same of their attributes such Ids. With others subkeys, the secret key are also used to generate the signature "*K*". Therefore the message integrity with non-repudiation can be provided by our proposed scheme.

5 Conclusion

In this paper, we presented a healthcare data collection system where we designed and implemented the system. We have shown the HR result obtained using the sensor node. In addition we described the cryptographic scheme for protecting the HR data where a patient can encrypt his data before uploading and storing to cloud provider. The aim of our proposed method it is to revoke the patients' semi-trusted assumption to cloud provider by giving the patient the ability to issue an access credential with embedded rights to the authorized person to decrypt the patient's record medical data.

First, we defined the attributes of the involved entities in this paper and we described the contents of the ciphertext *C (M)* uploaded to cloud. Moreover we presented the concept of credential based on the key note trust management which provides the credentials functions. By the end, we made a security analysis regarding known attack to cipher and cloud storage, hence the proposed scheme have been founded efficient and resilient to various kinds of attacks

Acknowledgments. 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. And it also supported by the BB21 project of Busan Metropolitan City.

References

1. Osterhaus, L.C.: Cloud Computing and Health Information. U of I SLIS Journal, Iowa Research, University of Iowa's Institutional Repository (November 2010)
2. Matyas, V.: Protecting doctors' identity in drug prescription analysis. Health Informatics Journal, 205–209 (1998)
3. Ateniese, G., de Medeiros, B.: Anonymous e-prescriptions. In: The Proceedings of the ACM Workshop on Privacy in the Electronic Society, pp. 19–31. ACM Press (2002)
4. De Decker, B., Layouni, M., Vangheluwe, H., Verslype, K.: A privacy-preserving eHealth protocol compliant with the Belgian healthcare system. In: Mjølsnes, S.F., Mauw, S., Katsikas, S.K. (eds.) EuroPKI 2008. LNCS, vol. 5057, pp. 118–133. Springer, Heidelberg (2008)
5. Anderson, R.: A security policy model for clinical information systems. In: The Proceedings of the 17th IEEE Symposium on Security and Privacy, pp. 30–44. IEEE CS (1996)
6. Reid, J., Cheong, I., Henricksen, M., Smith, J.: A novel use of rBAC to protect privacy in distributed health care information systems. In: Safavi-Naini, R., Seberry, J. (eds.) ACISP 2003. LNCS, vol. 2727, pp. 403–415. Springer, Heidelberg (2003)
7. Evered, M., Bögeholz, S.: A case study in access control requirements for a health information system. In: Proceedings of the. 2nd Australian Information Security Workshop. Conferences in Research and Practice in Information Technology, vol. 32, pp. 53–61. Australian Computer Society (2004)
8. Hung, P.C.K.: Towards a privacy access control model for e-healthcare services. In: Proceedings of the 3rd Annual Conference on Privacy, Security and Trust, October 12-14 (2005)
9. Masys, D.R., Baker, D.B.: Patient-Centered Access to Secure Systems Online (PCASSO): A Secure Approach to Clinical Data Access via the World Wide Web (1997)
10. Gematik. Einführung der Gesundheitskarte - Gesamtarchitektur, Version 1.7.0 (August 2009)
11. Gematik. Einfüuhrung der Gesundheitskarte - Netzwerkspezi_kation, Version 2.0.0 (August 2009)
12. Kemis, H., Bruce, N., Ping, W., Lee, H.J., Gook, L.B., Antonio, T.: Healthcare Monitoring Application for Ubiquitous Sensor Network: Design and Implementation based Pulse Sensor with Arduino. In: The 6th International Conference on New Trends in Information Science and Service Science (NISS 2012), Taipei, Taiwan, October 23-25 (2012)
13. Blaze, M., Feigenbaum, J., Ioannidis, J., Keromytis, A.: The role of trust management in distributed systems security. In: Vitek, J. (ed.) Secure Internet Programming. LNCS, vol. 1603, pp. 185–210. Springer, Heidelberg (1999)
14. Blaze, M., Feigenbaum, J., Ioannidis, J., Keromytis, A.D.: The Key Note Trust Management System Version 2. RFC 2704 (September 1999)