System Architecture and Economic Value-Chain Models for Healthcare Privacy and Security Control in Large-Scale Wireless Sensor Networks

Won Jay Song[1], Im Sook Ha[2], and Mun Kee Choi[2]

[1] Department of Computer Science, University of Virginia, VA 22904-4740, USA
[2] School of IT Business, Information and Communications University, 305-732, Korea
wjsong@cs.virginia.edu

Abstract. In this paper, we have designed and modeled the ubiquitous RFID healthcare system architecture and framework workflow, which are described by six classified core players or subsystems, and have also analyzed by an economic value-chain model. They consist of the patient and wearable ECG sensor, network service, healthcare service, emergency service, and PKI service providers. To enhance the security level control for the patient's medical privacy, individual private and public keys should be stored on smart cards. All the patient and service providers in the proposed security control architecture should have suitable secure private and public keys to access medical data and diagnosis results with RFID/GPS tracking information for emergency service. By enforcing the requirements of necessary keys among the patient and service providers, the patient's ECG data can be protected and effectively controlled over the open medical directory service. Consequently, the proposed architecture for ubiquitous RFID healthcare system using the smart card terminal is appropriate to build up medical privacy policies in future ubiquitous sensor networking and home networking environments. In addition, we have analyzed an economic value-chain model based on the proposed architecture consisting of RFID, GPS, PDA, ECG sensor, and smart card systems in large-scale wireless sensor networks and have also derived customer needs in the proposed service architecture using the value-chain model. Therefore, we also conclude that the business and technology issues for the service providers should exist in the networks.

1 Introduction

Recently, electronic healthcare systems have extended to ubiquitous healthcare systems such as personal home networking healthcare. They enable medical professionals to remotely make real-time monitoring, early diagnosis, and treatment for potential risky disease, and to provide the medical diagnosis and consulting results to the patient via wired/wireless communication channels. In addition to new ubiquitous medical equipments for patients (e.g., wearable healthcare sensor systems), smart home/sensor networks, radio frequency identification (RFID), public-key infrastructure (PKI), and Grid computing technology for large-scale physiologic and electrocardiogram (ECG) signal analysis have been studied and developed [1]-[8].

In spite of all the research and development in ubiquitous healthcare systems for a variety of applications, the system should still have to address both access control and

L.T. Yang et al. (Eds.): ATC 2006, LNCS 4158, pp. 511–520, 2006.

privacy protection issues for the patient's individual medical data. These problems are serious when unauthorized persons or groups trying to monitor and access to the systems, remotely and stealthily. The problem can be complicated since it is possible to collect the patient's medical data from a wide variety of ubiquitous sensor nodes and to track an individual patient's location in ubiquitous networking world. To address those issues systematically, advanced study of privacy and security control architecture is critical. We have designed and modeled an architecture based on RFID and smart card technologies for ubiquitous healthcare in wireless sensor networks. Our novel architecture can effectively protect personal medical data and diagnosis results [4],[9]-[11].

Additionally, a need for an efficient method of storing personalized medical data, while providing security, reliability and portability, has arisen for ubiquitous RFID healthcare system in large-scale wireless sensor networks. The current PC-based smart card terminal should not only be designed to interface with smart cards and to control the retrieval or storage of data on the card but should also consist of several hardware components [12]. The microprocessor, memory, and the other hardware components needed for data encryption are embedded in the IC chip of the smart card. Therefore, smart cards are usually used in the area of wireless sensor networks. There is a need for smart card terminal-based systems with technical specifications for specific IC card operations [13],[14].

Finally, most research for new system architectures has only focused on technical aspects. In this paper, however, we have described not only the technical approach but also performed economic evaluation of the architecture using a value chain model. The value chain is a systematic approach to examining the development of competitive advantage and it was introduced by M.E.Porter [16]. The chain consists of a series of activities that create and build value. Moreover, it serves a useful analytical tool of emerging new system or service, particularly under rapidly changing telecommunications environments [17]. Thus, this paper describes that a value chain of the healthcare system and core players of each stage exist for value creation of RFID wearable sensor healthcare systems.

2 Architectural Design Process

2.1 Ubiquitous RFID Healthcare System

In the proposed security control architecture for ubiquitous healthcare system, we use radio frequency identification (RFID) tag, wearable electrocardiogram (ECG) sensor, smart card, Grid computing, PhysioNet, wired/wireless networks, and public-key infrastructure (PKI) technologies. The system architecture and framework are described by six classified core players or subsystems as shown in Figure 1.

They consist of the patient (PAT) and wearable ECG sensor provider (WSP), network service provider (NSP) with encrypted medical database and Grid computing, healthcare service provider (HSP) with PhysioNet database, emergency service provider (ESP), and PKI service provider (PSP) with certificate and directory databases. The individual private and public keys should be stored on the smart card and be used to enhance security level control for the patient's medical privacy.

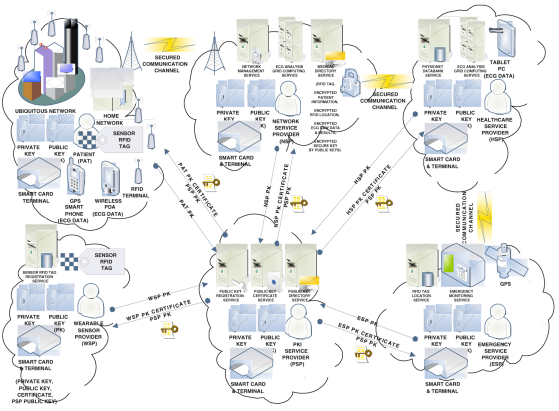

Fig. 1. The schematic diagram consisting of six core player or subsystems with their individual components and functions at privacy and security control architecture for ubiquitous RFID healthcare system

The WSP supplies its wearable ECG sensor system with RFID tag to the PAT, whose tag has unique identification information for the wearable sensor node. In order to protect the patient's privacy, all of the providers only recognize and use the tag information, instead of directly accessing to the patient's personal data. In addition, unique RFID tag information can be also used to track a patient in wearable RFID sensor system for emergency service by the ESP under ubiquitous RFID terminal network environments.

All individual public keys with correspondence to each private key should be stored on the PKI key server at the PSP. To verify the unique identification of each player or subsystem, the certificate of each public key should be issued by using the private key of the PSP and be stored on the PKI directory server. Then, both the certificates and the public key with correspondence to the private key of the PSP should be in service to all of the patient and providers via wired/wireless secure communication channels.

2.2 Security Features of Healthcare Smart Card

Digital Signature. A smart card can carry all the data needed to generate the holder's digital signature in sensor networks. The main components are encryption and decryption keys (private/public key pair) and a signed digital certificate. Digital signatures use a method of encryption and decryption known as 'asymmetric.' This method uses two keys, one to encrypt and the other to decrypt. If a message is encrypted using one key, it can only be decrypted using the other. These key pairs need not both be secret.

In 'public-key encryption' systems, one key is private, the users, and the other is the public domain. Note that in these cases, key distribution is trivial since the private key is never conveyed to anyone and the public key is available to everyone. An electronic signature cannot be forged. It is a computed digest of some text that is encrypted and sent with the text message. A digital signature ensures that the document originated with the person signing it and that it was not tampered with after the signature was applied.

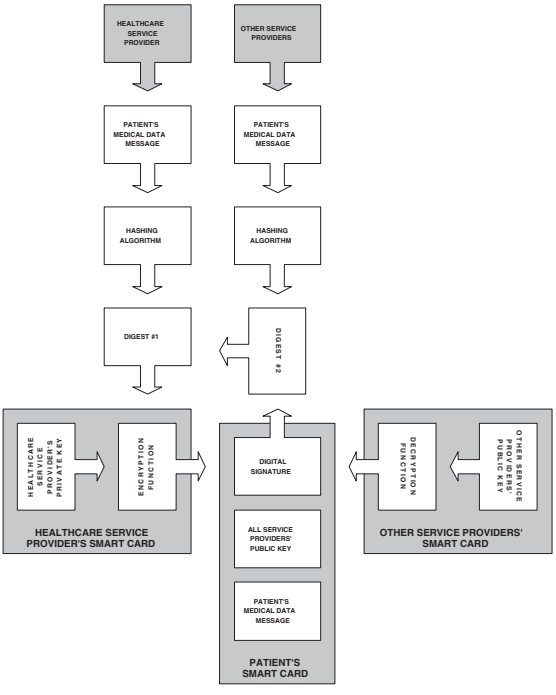

Fig. 2. The first processing sequence required to generate a digital signature for authentication purposes in ubiquitous RFID healthcare systems

Smart Card Authentication. As shown in Figure 2, you have to have access to that public key. Not only do you need that access, but you also need to be sure that the public key you obtain really is the public key for the person in question. One way to verify the validity of a public key is to sign it with yet another key, whose public key you know to be valid. Thus, it belongs to a trusted third party and a patient's smart card. This is the 'signed' digital certificate [15].

Public-Key Infrastructure. A Public-Key Infrastructure (PKI) is a collection of services that enables the use of public-key encryption techniques. The functions of a PKI include creating digital certificates, storing public keys, and tracking expiration dates of certificates. A public key obtained through a PKI is trustworthy. By managing these keys and certificates, an organization, such as the National Health Service (NHS), establishes and maintains a trustworthy networking environment. The existence of a PKI is therefore a critical factor in the use of the HPC in the NHS.

As commonly used, a digital certificate contains: (1) an expiration date, (2) the name of the certifying authority that issued the certificate, (3) a serial number, (4) the digital signature of the certificate issuer and the Certification Authority (CA), (5) the identity of the registered holder, and (6) the holder's public key. Using smart cards in conjunction with a PKI implies that the CA issues the card with certificates and key pairs already

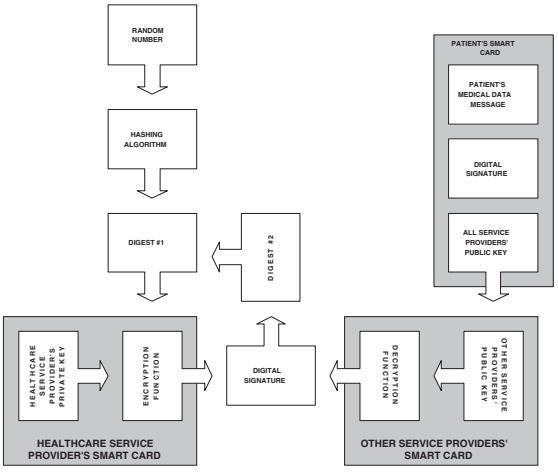

Fig. 3. The second processing sequence required to generate a digital signature for authentication purposes in ubiquitous RFID healthcare systems

written on it. This would apply both to the healthcare professional card and the patient's data card. Signed public keys are stored in a public directory. In the NHS, this would be the managed directory service [15].

2.3 Functions of Healthcare Smart Card

Login Process. The Healthcare Professional Card (HPC) is the core of the login process, which involves verification of the user and authentication of the HPC. Authentication is the process that identifies and validates either the principal(s) involved in a transaction, or the origin of a message. We assume for the sake of illustration that the HPC holder wishes to use a healthcare application. We also assume that the application is a client/server system with a wireless PDA acting as the user terminal and that it is fitted with a smart card terminal.

The first part of the login process will comprise the user inserting the HPC into the terminal. The application will request the HPC to generate the holder's digital signature. At the same time, the application will request the user to enter identification details. This will enable the application to verify that the user is the authorized holder of the HPC and that the card is genuine, and then start the session. The user identification might include the use of a Personal Identification Number (PIN) or password. This method has often been dismissed as 'weak' security and easily compromised. However, this is not necessarily the case, and the weaknesses often lie in sending clear text to the authentication server [15].

Request and Response Procedures. The authentication process performed by the application is achieved using a request and response procedure employing the cryptographic algorithm recorded on the HPC. To authenticate the HPC, the system requests

the card by sending a random number. Figure 2 shows the first part of the request process. i.e., the 'message' sent to the card being the random number. The card uses this number and its own secret (private) key as input to its cryptographic algorithm [15].

The output of the calculation is then transmitted to the application as a digital signature. The application decrypts the signature using the public key obtained through the Public-Key Infrastructure (PKI). It compares the result with the original. If the two match, the card is considered to be genuine. Figure 3 shows the authentication process, the second part of the request-response. The application obtains the public key for the user from the PKI, using the identification details supplied.

Authentication and Access Control. For security purposes it is necessary for the healthcare application to check that the card is genuine. This means that the card must be issued by the National Health Service (NHS) Certification Authority (CA) for the holder's GP and initialized with signed security data. For the Healthcare Professional Card (HPC) and Patient's Data Card (PDC) interaction, two services are required as the PDC has to prove its authenticity and the healthcare professional has to prove access rights [15]. When proving access rights, an authentication procedure has to be performed. If after successful authentication a read or update command is performed on a smart card file, the application has to verify that the respective security condition described in the security attributes of this PDC file is fulfilled. Access rights can be expressed in terms of either individual professionals or identifiable groups, or both. The problems with the application can therefore be complicated by the need to recognize the HPC holder as a member of an access group [15].

The PDC authentication procedure assumes that the professional has already logged into the healthcare application using an HPC. The patient holds a healthcare smart card, which is plugged into the auxiliary card terminal. The PDC is authenticated by the challenge-response method. This entails the professional entering the patient's NHS number at the user terminal.

Authentication proves that the PDC belongs to the NHS number supplied and was created by an authorized professional. When the application reads data from the card, it checks that the professional currently in session has the right to access that data. If not, the application will inform the professional that access has been denied, but provide an override facility for emergency purposes. If the professional makes a decision that affects the card's data, the application will check that the professional has the right to amend the data. If the professional is not authorized, an emergency override facility will be offered [15]. Any data written will have the professional's digital signature attached. Referring to Figure 2, the 'message' represents the data to be written to the card. The digital signature is a function of the data written. Therefore any later unauthorized attempt to alter the data written will result in the digital signature not matching the data.

3 Architectural Integration Process

In the proposed architecture combined with wearable and wireless sensor network environments, the patient's ECG signals should be automatically measured and periodically stored on the internal flash memory of the wearable ECG sensor system. The stored

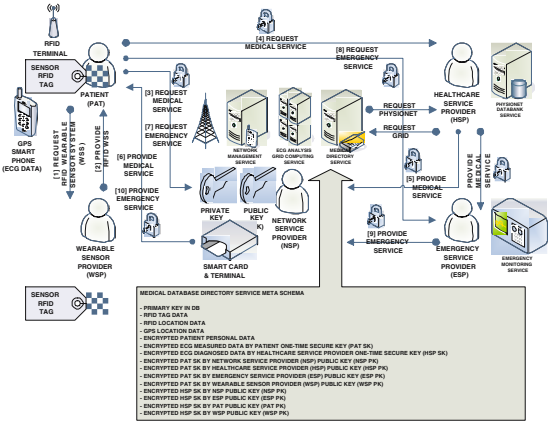

Fig. 4. The schematic diagram consisting of five core player or subsystems without public-key service provider

medical raw data will be transferred to the patient's or medical professional's wireless PDA with a 2-way double-type smart card terminal or GPS smart phone. For the data transfer, near-field wireless communications such as the Bluetooth wireless technology is used. The transferred data should be encrypted by using the patient's one-time secure key at the handheld devices.

As illustrated in Figure 4, all the data in wearable ECG sensors as well as analyzed data in Grid computing with PhysioNet should be encrypted by using an individually generated one-time secure key with expire-time by the PAT's and HSP's private keys, respectively. Additionally, the issued one-time secure keys are also encrypted by using public keys of the patient and pre-approved service providers. These encrypted medical data and encrypted secure keys will be also transferred to the network service provider via secured communication channels in wired/wireless networks. The encrypted data and keys with unique RFID tag information should be stored on the secured database directory of network service provider. The database meta-schema has decrypted and encrypted fields, that are used to make access control among the patient and providers.

4 Economic Value-Chain Modeling Process

The value chain is the full range of activities that are required to bring a product from its conception to its end use. This consists of activities such as design, production, marketing, distribution, and support to the final consumer [16]. In the value chain of ubiquitous system, however, subsystems of the existing value chains are regrouped in response to major function of system's players. Table 1 shows the reconfigured value chain. The reconfiguration value chain of the system consists of four parts; sensing, networking, diagnosis, and acting stages. Each stage has its own customer demands, technical issue, and business issue [18]. The proposed six classified core players in large-scale wireless sensor networks should match with four stages in value chain corresponding to common function.

Table 1. The economic value-chain model of RFID wearable healthcare systems in large-scale wireless sensor networks

Value Chain	Sensing Stage	Networking Stage	Diagnosis Stage	Acting Stage
Customer Needs	Precision awareness and convenience	Promptness and safety	High Quality service and professionalism	Quick response
Technical Issues	RFID technology (e.g. tag, reader, and server) and smart card terminal with easy of use	Cryptography (PKI) and high-bandwidth infrastructure for huge data handling	Grid computing, data warehouse, and medical equipment	Location based sensor and sensing (RFID/GPS)
Business Issues	Cost reduction, standardization for the market domination, and partnership between network provider and PKI service provider		Service pricing, CRM (data mining), and advertising and subscription model	
Player	Patient and wearable ECG	Network service provider and PKI service provider	Healthcare service provider	Emergency service provider

Sensing Stage. In the sensing stage, it is essential to have a precise awareness and convenient sensing technology. Through the ubiquitous RFID/GPS technology, the patients can be diagnosed in any place at any time so that the importance characteristics of this stage is sensor and sensing technology such as wearable ECG sensor. Additionally patients can feel comfortable to attach senor without any trouble. The technology issues are RFID technology in terms of weight and easy of use (e.g., tag, reader, and server). The main player of sensing stage is patient and wearable ECG sensor.

Networking Stage. The following stage is networking. Privacy and security are critical for the customer, especially in this stage. Network service provider provides wireless sensor networks, and PKI service provider supports high-level encryption and decryption algorithm for the protection of patients' medical data. Thus, the two players carry out important technical issues. Moreover, high-bandwidth infrastructure for huge data handling is also essential.

Diagnosis Stage. The third stage is a diagnosis stage. The correct and high-quality diagnosis service of a medical specialist is major customer needs based on the collected patients' medical data. The major technical issue of this stage is grid computing technology. It also provides the ability to perform computations on large medical data sets and to accomplish more computations at once with accuracy. From the accumulating patient's medical data, healthcare service provider analyzes the symptom and prescribes the medicine or treatment.

Acting Stage. Finally, last stage is an acting stage which is the reaction and control of hospital or pharmacy for the diagnosed patients. Emergency service provider (ESP) can be a core player of this stage. When any alerts from the diagnosis is announced, the ESP can track him through location-based system and then it gives

expediency and bring the patients to the proper hospital or organization within a short time. The technology issue of this stage is location-based sensor and sensing, for example, RFID and GPS.

The former two stages (sensing and networking) are based on the technology. To have comparative advantage in those business cost reduction, standardization for the market domination, and partnership between network provider and PKI service provider are necessary. The latter two stages (diagnosis and acting) are for the service from hospital or pharmacy. ESP can be a good business model for these stages. What we have to consider in terms of business is service pricing, customer relation management (CRM), advertising, and subscription model.

5 Conclusion

In the proposed privacy and security control architecture for ubiquitous RFID healthcare systems in large-scale wireless sensor networks, all of the patient and providers need suitable secure private and public keys in order to access to ECG medical raw data and diagnosis results with RFID and GPS tracking information for emergency service. By enforcing the requirements of necessary keys among the patient and providers, the patient's ECG data can be protected and effectively controlled over the open medical directory service of network service providers. Consequently, the proposed architecture for ubiquitous RFID healthcare system is appropriate to build up medical privacy policies. The architecture can provide a new business model to wired/wireless network service providers. In the future, the system architecture workflow and protocols will be modeled and verified using Petri nets.

The new emerging system and service have only been considered customer requirements analysis, systems design, integration, implementation, and verification passing over economic aspects. However, this paper analyzes not only the verification of proposed system architecture in technical aspect but also evaluating economic value creation through developing an economic value-chain model. The value chain model developed in this paper is also reconfigured in response to common function of classified six players. The reconfiguration value chain of the system describes four activities: the (1)sensing, (2)networking, (3)diagnosis, and (4)acting stages. The results show that sensing stage contains patient and wearable ECG sensor, the networking stage has network service provider and PKI service provider, the diagnosis stage has healthcare service provider, and the acting stage contains emergency service provider. In addition, it should be proposed technical and business issues for four service providers. Therefore, this new value-chain should be contributed to a better understanding of RFID wearable healthcare system in large-scale wireless sensor networks and economic implications for each player. It will be expanded by examining six players considering the evolution of networks

Acknowledgement. This research work has been supported in part by the Korea Research Foundation Grant (KRF-2005-M01-2005-000-10434-0) and the Information Technology Research Center program supervised by the Institute of Information Technology Assessment in Republic of Korea.

References

1. W.J.Song, S.H.Son, M.K.Choi, and M.H.Kang, "Privacy and Security Control Architecture for Ubiquitous RFID Healthcare System in Wireless Sensor Networks," *Proceedings in the IEEE ICCE 2006*, January 2006.
2. S.S.Choi, W.J.Song, M.K.Choi, and S.H.Son, "Ubiquitous RFID Healthcare Systems Analysis on PhysioNet Grid Portal Services Using Petri Nets," *Proceedings in the IEEE ICICS 2005*, December 2005.
3. G.B.Moody, R.G.Mark, and A.L.Goldberger, "PhysioNet: A Web-Based Resource for the Study of Physiologic Signals," *IEEE Engineering in Medicine and Biology*, vol.20, no.3, pp.70-75, May/June 2001.
4. K.Finkenzeller, *RFID Handbook*, 2nd Edition, Wiley & Sons, April 2003.
5. D.S.Nam, C.H.Youn, B.H.Lee, G.Clifford, and J.Healey, "QoS-Constrained Resource Allocation for a Grid-Based Multiple Source Electrocardiogram Application," *Lecture Notes in Computer Science*, vol.3043, pp.352-359, 2004.
6. G.Eysenbach, "What is e-healthcare?" *Journal of Medical Internet Research*, vol.3, no.2, 2001.
7. J.Marconi, "E-Health: Navigating the Internet for Health Information Healthcare," *Advocacy White Paper*, Healthcare Information and Management Systems Society, May 2002.
8. J.Joseph and C.Fellenstein, *Grid Computing*, Prentice Hall, 2004.
9. H.Chan and A.Perrig, "Security and Privacy in Sensor Networks," *IEEE Computer*, vo.36, no.10, pp103-105, October 2003.
10. C.H.Fancher, "In Your Pocket: Smartcards," *IEEE Spectrum*, vol.34, no.2, pp.47-53, February 1997.
11. R.W.Baldwin and C.V.Chang, "Locking the e-safe," *IEEE Spectrum*, vol.34, no.2, pp.40-46, February 1997.
12. W.Rankl and W.Effing, *Smart Card Handbook*, 2nd Edition, New York, John Wiley & Sons, 2000.
13. ISO/IEC 7816-1:1998, *Identification Cards – Integrated Circuit(s) Cards with Contacts - Part 1: Physical Characteristics*, International Organization for Standardization, 1998.
14. W.J.Song, W.H.Kim, B.G.Kim, B.H.Ahn, M.K.Choi, and M.H.Kang, "Smart Card Terminal Systems Using ISO/IEC 7816-3 Interface and 8051 Microprocessor Based on the System-on-Chip," *Lecture Notes in Computer Science*, vol.2860, pp.364-371, November 2003.
15. NHS, *NHS IT Standards Handbook*, National Health Service (NHS) Information Authority, June 2001.
16. M.E.Porter, *Competitive Strategy: Techniques for Analyzing Industries and Competitors*, New York: Free Press, 1980.
17. P.Olla and N.V.Patel, "A Value Chain Model for Mobile Data Service Providers," *Telecommunications Policy*, vol.26, no.9-10, pp.551-571, 2002.
18. Y.H.Lee, H.W.Kim, Y.J.Kim, and H.Sohn, "A New Conceptual Framework for Designing Ubiquitous Business Model," *IE Interfaces*, vol.19, no.1, pp.9-18, March 2006.