

Towards a Secure Patient Information Access Control in Ubiquitous Healthcare Systems using Identity-based Signcryption

Giovanni Cagalaban *, Seoksoo Kim **

* Science in Computer Science, University of Western Visayas, Philippines

** Department of Multimedia, Hannam University, Daejeon-city, Korea

gcagalaban@yahoo.com, sskim0123@naver.com

Abstract — While ubiquitous healthcare applications over the Internet promise increasing efficiency, accuracy, and availability of medical treatment, security has received increasing attentions as one of the critical research challenges. In this paper, we consider security issues due to increasing access sharing of patient information resources in the networked environment. We propose a novel efficient access control in order to provide various security characteristics, such as authentication, confidentiality, integrity and non-repudiation for ubiquitous systems. In our communication environment, we deploy the recently developed concepts of identity-based signcryption in which the network effectively solves the problem of single point of failure in the traditional public-key infrastructure (PKI) supported system by providing key generation and key management services without any assumption of pre-fixed trust relationship between network devices.

Keywords — security, identity-based signcryption, patient information, access control, ubiquitous healthcare system

I. INTRODUCTION

With the advancement of medical technology for healthcare devices and health diagnosis, ubiquitous healthcare systems providing healthcare services anytime and anywhere has emerged as a new computing paradigm [1]. The rapid evolution of sensor technologies has spurred numerous healthcare researches and projects using body sensors as remote monitoring devices. These portable and cheap body sensors which can perform 24-7 monitoring enable remote diagnosis and treatment of patients giving them the comfort of not having to visit a hospital thus curtailing their expenses for healthcare services.

Existing healthcare information systems (HIS) use networked computing systems for recording and accessing medical records [2]. Additionally, ubiquitous healthcare extends the computerization of medical records to the domain of monitoring and diagnosis where monitored medical data will be recorded and the historical record used in subsequent analysis. The continuous recording of medical data taken by body and infrastructure sensors provides a life log of the patients. The healthcare environments composed of individuals such as doctors and nurses collaborate in order to

provide care to patients in a more efficient way. Also, healthcare institutions are increasingly interested in sharing access of their information resources over the networked environment. Other interested parties such as employers, insurance companies, drug companies, etc. might also be interested in these information resources. Healthcare applications over the Internet offer an attractive communication infrastructure at worldwide level but with a noticeably great factor of risk. Transmission of sensitive patient medical information over the networked computer systems increases the risk of security and privacy.

Security considerations are needed in order to deal efficiently with the communication security issues described above. In a large network, efficient access control with scalable rekeying is one of the most important requirements for secure data transmission and communication. Much research has been done into creating key management schemes to meet the notion of security, authentication, and privacy. The security scheme is established on the basis of a secret group key that is shared among the privileged users, but is unknown to non-group members. Generally, access control can be achieved by encrypting the group communication using the group key. However, the difficulty of managing cryptographic keys used for group communication arises from the dynamic membership change. Every time a member is added to or deleted from the group, the group controller must change the group key for backward or forward secrecy [3]. Thus, changing the group key for a large number of subscribers in a scalable and reliable manner is one of the most challenging issues in a secure group communication.

In this paper, we present a secure patient information access control mechanism in a networked environment. In a ubiquitous healthcare environment, we deploy the recently developed concepts of identity-based signcryption in which the network effectively solves the problem of single point of failure in the traditional public-key infrastructure (PKI) supported system by providing key generation and key management services without any assumption of pre-fixed trust relationship between network devices. We aim to resolve the data or sender authentication problem by using an identity-based signcryption scheme [4]. We implemented the proposed

scheme by combining identity-based one-way encryption with message integrity or signature verification. Only the intended group members determined by a sender can obtain the message with their own secret keys even if they are stateless, and can be convinced with the authenticity of the message with the public identity of the sender.

II. RELATED WORKS

The increasing access sharing of patient information resources in a networked environment has exposed a considerable number of security issues. In the early 90s, security threats to patient information were recorded. Few reports on security in electronic patient record (EPR) were released [5, 6]. Most security researches in healthcare systems [7, 8, 9] have been based on role based access control (RBAC) model.

Many researchers have worked on privacy in ubiquitous computing environments. Related to healthcare information systems are the researches on dependability issues of ubiquitous computing in a healthcare environment which were analyzed by Bohn, et. al. [10] and the perception of privacy based on the case study of a sensor-rich, eldercare facility discussed by Beckwith [11]. Various security issues on ubiquitous computing were discussed by Stajano [12]. In addition, security and privacy of RFID systems was introduced by Albrecht and McIntyre [13]. Some significant privacy-protecting solutions to security issues were the hash-based access control, randomized access control, and silent tree walking concepts invented by Weis, et. al. [14].

A fundamental issue regarding access control scheme in healthcare systems is their cooperative nature. A public-key infrastructure (PKI) supports the management of digital certificates suitable for identification and authentication purposes. In order to shield transport and sharing of medical data and protect healthcare applications over the Internet there is a need of a suitable security scheme with appropriate structure, compatibility with the PKI and PMI environments [15]. For secure communication services, an identity-based authenticated broadcast encryption scheme was proposed by Mu, et. al. [16]. This scheme allows each sender to dynamically broadcast messages to its group members using a polynomial function constructed with secret keys of the members. However, it does not provide the mechanism of verifying the signature or integrity of the message. Additionally, another identity-based ring signcryption scheme was proposed by Huang, et. al. [17] based on cryptographic primitives for preserving privacy and authenticity. However, the concept was designed for a general ubiquitous computing and not directly applicable to addressing security issues in ubiquitous healthcare systems such as authentication, confidentiality, integrity and non-repudiation.

III. SECURITY REQUIREMENTS FOR PATIENT INFORMATION ACCESS CONTROL

Ubiquitous healthcare systems provide functionalities of recording and accessing medical records of patients through networked computing systems. By adopting ubiquitous

computing as an enabling technology, ubiquitous healthcare systems allow the use of mobile sensors capable of monitoring the patient continuously. With the increased mobility of the patients and the changes in the structure of healthcare information systems, a patient's medical information is being accumulated in a variety of locations. Medical data are shared between different sources in order to provide information to internal users as well as external requests, payers, etc. as shown in Figure 1. Data may be accessed via remote workstations and complex networks supporting one or more organizations, and potentially within a national information infrastructure.

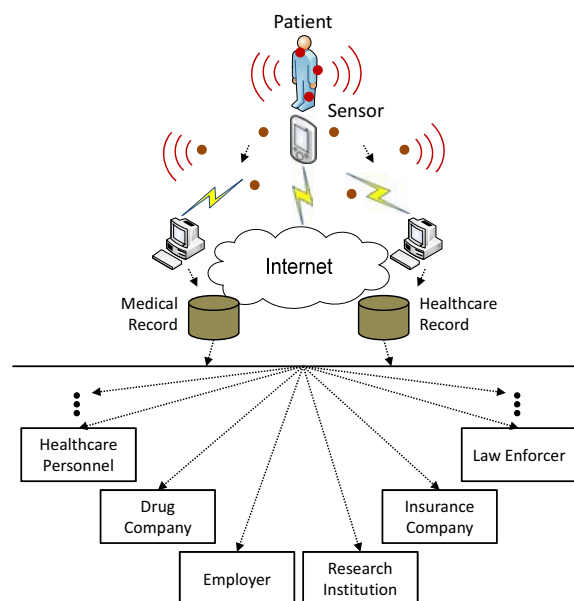


Figure 1. Ubiquitous Healthcare System

Healthcare systems that are geographically dispersed over wide-area networks to support data sharing in restricted collaborations give rise to a range of requirements for a secure access control. Despite promises of efficiency, accuracy and availability of medical treatment potential security problems may arise such as major privacy violations, discrimination, and even life-threatening attacks. Additionally, security problems presented by a ubiquitous healthcare system can be summarized into four areas:

- Ubiquitous monitoring. Monitoring and diagnosis will be done remotely and sensors will be mobile and goes wherever the patient goes, providing the caregivers or nurses with the ability to record, search and archive sensor data anywhere and anytime.
- Ubiquitous access. Remote access without adequate protection increases the vulnerability of medical records to unauthorized access.

- Ubiquitous care. Patients will receive tele-prescription and tele-infusion of drugs and receive professional advice remotely.
- Ubiquitous sensor data. The collection and recording of medical sensor data will be useful to researchers and related institutions.

TABLE 1. SECURITY REQUIREMENTS

Security Requirements	Description
Data confidentiality	Preventing non-group member from improper information modification.
Signature non-repudiation	Preventing the sender from rejecting its signature.
Ciphertext authentication	Guarantee of only authorized information access and disclosure.
Ciphertext anonymity	Hiding the fact that there was a data exchange.

The main security concerns of the ubiquitous healthcare system communication are secrecy and authenticity. Specifically, these security requirements are considered to be data confidentiality, signature non-repudiation, ciphertext authentication, and ciphertext anonymity. We describe systematically each of the security requirements in Table 1.

A. Data confidentiality

Data confidentiality is vital in preventing outsiders or non-group members from decrypting the data being transmitted. It allows the communicating parties to preserve the secrecy of their data being shared. Indistinguishability of encryption is considered the accepted notion of security with respect to confidentiality for public key encryption which occurs under adaptive chosen ciphertext attack.

B. Signature non-repudiation

Signature non-repudiation prevents the sender of a signcrypted data from rejecting its signature. It can be also verified by only the intended recipient of the signcryption. The accepted notion of security with respect to the non-repudiation is existential unforgeability under adaptive chosen message attack. This implies ciphertext authentication and integrity.

C. Ciphertext authentication

Ciphertext authentication is, in a sense, the complement to unlinkability. Authentication requires that the legitimate recipient be able to ascertain that the ciphertext did indeed come from the same person who signed the message it contains. Hence, an outsider cannot re-encrypt a signcrypted data of the sender throughout the transmission. This implies ciphertext integrity.

D. Ciphertext anonymity

Cipher anonymity makes the ciphertext appear anonymous and hiding both the sender and the recipient identities to anyone who does not possess the recipient decryption key.

This is to say that the ciphertext must contain no information in the clear that identifies the author or recipient of the data.

IV. IDENTITY-BASED SIGNCRYPTION SCHEME

The concept of identity-based cryptography was proposed by Shamir [18] in 1984 with the goal of simplifying certificate management in email system, thus avoiding the high cost of the public-key management and signature authentication in PKI supported cryptosystem. The basic idea is to find an approach wherein each entity's public key can be defined by an arbitrary string. In other words, users may use some well-known information, such as e-mail address, IP address, or identity as their public key, thus there is no need to propagate this common information through the network. The idea remains a theoretical concept until the first practical identity-based encryption scheme was proposed by Boneh and Franklin [19].

In identity-based signcryption, a digital signature scheme is used for the authentication of messages and an encryption algorithm is used for the confidentiality of messages. For a ubiquitous healthcare system to work, there is a private key generator (PKG), which generates system parameters, and master public/private key pair, and makes the master public key known to everyone. The master private key is only kept to itself. PKG is also responsible of generating private keys corresponding to the defined public keys for the network user, using the master private key and user's public key.

An identity-based signcryption scheme consists of the four algorithms: Setup, Extract, Signcrypt, and Unsigncrypt. Their functions are described below:

- Setup: This algorithm generates the global public parameters $globalparams$, the master secret key s , and the master public key on the given security parameter k .
- Extract: This algorithm generates a corresponding private secret key based on the given master secret key and the public key of the user.
- Signcrypt: Assuming that A wishes to send a message m to B , this algorithm works by generating a ciphertext σ given the message m with its own secret key.
- Unsigncrypt: Assuming that B receives a ciphertext σ from A , this algorithm is used to recover the message m from the ciphertext σ with its own secret key. This results in producing m , σ , and the identity of the sender A .

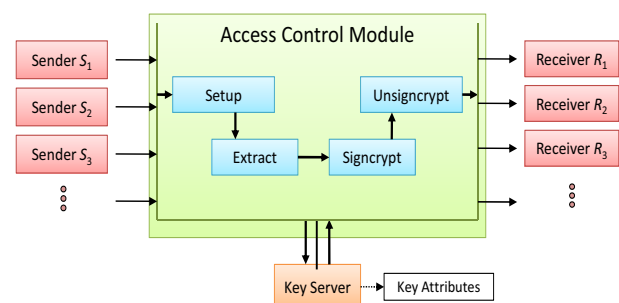


Figure 2. Access Control Operational Flow

The patient information access control scheme is aimed to provide a method for encrypting and signing data together in a way that is more efficient than using an encryption scheme combined with a signature scheme. Figure 2 shows the operational flow of the access control scheme.

A. Assumption

In this subsection, we describe our assumptions and overview of our efficient patient information access control scheme in a ubiquitous network environment. We describe the details of distributed key management and authentication mechanisms. Here, we consider the ubiquitous network environment where there are a centralized key server and multiple communication controllers. A sender of a group is in charge of managing the group as a communication controller. The key server generates public parameters for the system and the keys for the network group senders and users.

We assume that $C = \{ \zeta_1, \zeta_2, \dots, \zeta_n \}$ represents the set services in the network. Let $U = \{ \psi_1, \psi_2, \dots, \psi_n \}$ be the universe of users. Let S_j denote the sender of $\zeta_j \in C$, and $R_j \subseteq U$ denote the set of members who can access the service ζ_j transmitted from S_j . For example, a member $\psi_1 \in R_1 \cap R_2$ can access the broadcast services transmitted from S_1 and S_2 respectively. ID_U represents a public identity of U . For example, ID_{S_i} and ID_{R_j} represent the identities of S_i and R_j respectively.

The control access scheme in this paper does not rely on any assumption of underlying key management subsystem. There is no trusted authority to generate and distribute the public/private keys and there is no pre-built trust association between nodes in the network. All the keys used is generated and maintained in a self-organizing way within the network.

B. Construction

Based on the assumptions made above, we can now construct the secure access control scheme for each of the algorithms of the identity-based signcryption. The cryptography in the proposed scheme makes use of a bilinear map $\gamma : \zeta_1 \times \zeta_1 \rightarrow \zeta_2$ where ζ_1 , and ζ_2 are scalar services based on the order π .

For the Setup algorithm, the key server chooses a key generator PLK of ζ_1 and a random $s \in N_\pi^*$, and computes a master public key $PLK_p \leftarrow s_{PLK}$. The key server keeps s as a master secret key. Subsequently, the key server chooses cryptographic respective hash functions $H_1 : \{0,1\}^* \rightarrow \zeta_1$, $H_2 : \{0,1\}^* \rightarrow N_\pi^*$, $H_3 : \zeta_2 \rightarrow \{0,1\}^*$ and publishes parameters $globalparams = \{PLK, PLK_p, H_1, H_2, H_3\}$.

For the Extract algorithm, the key server extracts $T_{S_j} \leftarrow H_1(ID_{S_j})$ and computes the private key $PVK_{S_j} \leftarrow sT_{S_j}$, $\forall S_j$ of $\zeta_j \in C$. In the same manner, the key server extracts $T_{R_j} \leftarrow H_1(ID_{R_j})$ and computes the private key $PVK_{R_j} \leftarrow sT_{R_j}$, $\forall R_j$ of $\zeta_j \in C$. Subsequently, the key server sends the private keys PVK_{S_j} and PVK_{R_j} to S_j . Each sender S_j picks n qualified pairs (x'_i, x_i) for $i = 1, \dots, n$ where $n = |R_j|$, and computes $x = x'_1 x'_2 \dots x'_n$. Then, $\forall$

$\psi_i \in R_j$, the sender computes a secret key $PVK \psi_i \leftarrow x_i PVK_{R_j}$ for $i = 1, \dots, n$ and distributes PVK_{ψ_1} to ψ_1 .

In the Signcrypt algorithm, the sender S_j first signs m by choosing $r \in N_\pi^*$ and computes $U \leftarrow r_x T_{S_j}$, $\sigma \leftarrow (r_x + H_2(U \parallel m)) PVK_{S_j}$ which returns the signature (U, σ) . Then, the sender S_j encrypt m using (r, U, σ) for its group members in R_j to compute $T_{R_j} \leftarrow H_1(ID_{R_j})$, $X \leftarrow \gamma(PVK_{S_j}, xT_{R_j})$, and $W \leftarrow (\sigma \parallel ID_{S_j} \parallel m) \oplus H_3(X)$. Then, S_j sends ciphertext (U, W) to its corresponding group members.

For the Unsigncrypt, a member $\psi_1 \in R_j$ decrypts the received ciphertext (U, W) from S_j to compute $Y \leftarrow \gamma(U, PVK_{\psi_1})$, $\sigma \parallel ID_{S_j} \parallel m \leftarrow W \oplus H_3(Y)$. Then, ψ_1 computes $T_{S_j} \leftarrow H_1(ID_{S_j})$, $N \leftarrow H_2(U \parallel m)$ to verify the signature (U, σ) on message m .

C. Master Key Generation

Unlike other schemes, we designed our master key generation mechanism so that it would not need the support of the trusted third party to safely compute a master key, separate it into multiple parts and then distribute them to respective receivers. Instead, the master key pair is computed collaboratively by the initial network devices without constructing the master private key at any single node. The scheme we used is an extension to Shamir's secret sharing [18] without the support of a trust authority. In the scheme, each device S_j randomly chooses a secret $PVK_{S_j} \leftarrow sT_{S_j}$ over π . The device S_j computes $U \leftarrow r_x T_{S_j}$ and sends (U, W) securely to R_j . After sending it, S_j can compute its share of master private key.

D. Private Key Generation

The way to obtain a public/private key pair and register to the network is to contact with at least n neighbors, present its identity and request PKG service. The node that holds the master key share can be the PKG service node. In our scheme, all the network nodes share the master private key, thus each of them can be the PKG service node. The n nodes works together to issue the public/private key pair for the requesting node. Using identity-based cryptosystem, the public key can be any arbitrary string and usually it is decided by the sender's identity.

V. SIMULATIONS

In this study, we perform simulations to further evaluate the performance of our proposed secure patient access control scheme. We run the simulation on a Windows machine Intel Core 2 Duo 2.80 GHz with 1GB memory. We implement identity-based signcryption into ns-2 simulator. The transport protocol that we used for our simulations is TCP/IP (Transmission Control Protocol/Internet Protocol). The simulation time is set to 100 s. As we perform the simulation, we change the network size to (20, 40, 60, 80, 100) and measure the average time taken to jointly generate the maser private key, the ratio of successful PKG service, and the time taken by the PKG service.

Table 2 shows the time for master key generation in terms of different network size. When we increase the network size from 20 to 100, the master key generation time is also

increased. This observation can be easily explained as the result of more the transmission delay. To get a master key share, each device needs to get message from any of the $n-1$ device. As network size becomes larger, the number of transmitted message also became larger which results in a larger transmission delay.

TABLE 2. GENERATION TIME FOR MASTER KEY

Network Size	Time (in seconds)
20	2.6
40	25.89
60	75.21
80	104.63
100	197.04

VI. CONCLUSIONS

The ubiquitous computing environment extends the existing healthcare services provided in medical institutions to the individual and the home. While ubiquitous healthcare introduces great convenience, it also poses at the same time equally great risk. The shift to 24-7 patient monitoring via body sensors is not just an incremental improvement over the existing practice: it is a qualitative step change.

This paper presents a rethinking of the security and privacy aspects of ubiquitous healthcare where solutions that were appropriate for yesterday's situation are insufficient for tomorrow goals. To address this issue, we propose a secure identity-based signcryption scheme in a network environment. The proposed scheme resolves the sender and data authentication problem by using identity-based signcryption. It also guarantees chosen cipher text security while requiring less performance overhead with regard to the communication, computation, and storage. The group members can be stateless receivers in their group communications. The identity-based signcryption mechanism is applied here not only to provide end-to-end authenticity and confidentiality in a single step, but also to save network bandwidth and computational power of wireless devices.

CORRESPONDING AUTHOR

Seoksoo Kim (sskim0123@naver.com)

REFERENCES

- [1] A. Berler, S. Pavlopoulos, and D. Koutsouris, "Design of an interoperability framework in a regional healthcare system," in *Proceedings of Engineering in Medicine and Biology Society*, 2004, vol. 2, pp. 3093-3096.
- [2] S. K. Katsikas, "Health care management and information systems security: awareness, training or education," *International Journal of Medical Informatics*, vol. 60, pp. 129-135, Nov. 2000.
- [3] S. Rafaeli, D. Hutchison, "A survey of key management for secure group communication," *ACM Computing Surveys*, vol. 35, pp. 309-329, Sept. 2003.
- [4] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," *Lecture Notes in Computer Science*, vol. 3386, pp. 362-379, 2005.

- [5] W. Lowrance, "Privacy and health research a report to the U.S. Secretary of Health and Human Services," U.S. Department of Health and Human Services, 1997.
- [6] T. Rindfleisch, "Privacy, information technology, and health care," *Communications of the ACM*, vol. 40, pp. 92-100, August 1997.
- [7] J. Reid, I. Cheong, M. Henriksen, and J. Smith, "A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems," in *8th Australasian Conference on Information Security and Privacy (ACISP 2003)*, July 2003.
- [8] L. Zhang, G. Ahn, and B. Chu, "A role-based delegation framework for healthcare information systems," in *Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT 2002)*, 2002, pp. 125-134.
- [9] I. Mavridis, G. Pangalos, and M. Khair, "eMEDAC: role-based access control supporting discretionary and mandatory features," in *Proceedings of 13th IFIP WG 11.3 Working Conference on Database Security*, 1999, pp. 55-63.
- [10] J. Bohn, F. Gartner, and H. Vogt, "Dependability Issues of Pervasive Computing in a Healthcare Environment," *Lecture Notes in Computer Science*, vol. 2802, pp. 160-169, 2004.
- [11] R. Beckwith, "Designing for Ubiquity: The Perception of Privacy," *IEEE Pervasive Computing*, vol. 2, pp. 40-46, April-June 2003.
- [12] F. Stajano, "Security Issues in Ubiquitous Computing," *Handbook of Ambient Intelligence and Smart Environments*, pp. 1-34, 2009.
- [13] K. Albrecht and L. McIntyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID*, 1st ed., Thomas Nelson, 2005.
- [14] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," *Lecture Notes in Computer Science*, vol. 2802, pp 201-212, 2004.
- [15] I. Mavridis, C. Georgiadis, G. Pangalos, and M. Khair, "Using Digital Certificates for Access Control in Clinical Intranet Applications," *Technology and Health Care*, vol. 8, pp. 173-174, 2000.
- [16] Y. Mu, W. Susilo, W. Lin, and C. Ruan, "Identity-based authenticated broadcast encryption and distributed authenticated encryption," *Lecture Notes in Computer Science*, vol. 3321, pp. 169-181, 2004.
- [17] X. Huang, W., Susilo, Y. Mu, and F. Zhang, "Identity-Based Ring Signcryption Schemes: Cryptographic Primitives for Preserving Privacy and Authenticity in the Ubiquitous World," in *19th International Conference on Advanced Information Networking and Applications (AINA'05)*, 2005, vol. 2, pp. 649-654.
- [18] A. Shamir, "Identity based cryptosystems and signatures Schemes," in *Proceedings of CRYPTO 84 on Advances in Cryptology*, 1985, pp. 47-53.
- [19] D. Boneh and M. Franklin, "Identity-based encryption from Weil pairing," *Lecture Notes in Computer Science*, vol. 2139, Springer, Berlin, pp. 213-229, 2001.