u-Healthcare System Protecting Privacy based on Cloaker

Seungjin Son, Kwangwoo Lee, Dongho Won, Seungjoo Kim*
Dept. of Information and Communication Engineering
Sungkyunkwan University
Suwon, Republic of Korea
{sjson, kwlee, dhwon, skim}@security.re.kr

***Abstract*—Recently, u-healthcare system has been widely used. Therefore many people are able to manage their health at anytime and anywhere. Especially, implantable device is used to care untreatable diseases. In u-healthcare environment with implantable device, privacy protection and secure access control mechanism support are important. When a patient wants to care at another hospital, implantable devices have to be accessed by doctor easily. However, these objectives are difficult to reconcile. To solve this problem, we propose u-healthcare system which provides a secure access control and protects the privacy of patient who uses implantable device.**

Keywords-u-healthcare security, IMD security, Cloaker

I. INTRODUCTION

Recently, there are many researches on u-healthcare system in overall area - security, network, medical science, and so on. Therefore, many patients are allowed to check and manage their health at anytime and anywhere. Especially, IMD (Implantable Medical Device) is developed and used to cure untreatable diseases such as diabetes, cardiac disorder and so on. Since IMD is directly related to person's life and personal information of patient, it is important to control the access and protect the privacy [1]. Moreover, IMD has a limited battery capacity and is implanted in human's body. Therefore, battery should be replaced in a timely manner and the attacker can attempt to consume the battery intentionally. If the access control is not provided, the attacker can threaten the patient's life by malicious operation. In this paper, we propose a system, which provides a secure access control to IMD and protects the privacy of patient who uses IMD in the u-healthcare environment.

The rest of paper is organized as follows. In section 2, we describe u-healthcare system equipped with IMD access control method and Cloaker based IMD system suggested by Tarnara Denning et al. [2]. In section 3, we derive possible risks and security requirements of IMD system. In section 4, we propose Cloaker based u-healthcare system which protects the privacy of patient and provides secure access control. In section 5, we analyze the performance and security of proposed scheme. Finally, we summarize and conclude in section 5.

* Corresponding author: Seungjoo Kim (skim@security.re.kr)

II. RELATED WORK

A. u-healthcare system with IMD

IMD is a device which is implanted in a patient's body to collect vital information (respiration, pulse, body temperature, blood pressure, etc). IMD such as defibrillator, cardiac pacemaker can treat patients remotely. Therefore, IMD provides solution for untreatable diseases such as cardiac disorder, diabetes, and so on. Since a doctor can check patient's condition in real time, IMD makes patients easier to manage their body [3]. In Unite States, about 25 million patents receive a medical service with IMD. The u-healthcare system provides that a patient can send his condition to a doctor, treat at anytime and anywhere. The u-healthcare system monitors 24 hours of patents status with IMD and enables first aid, if any problem is detected. Figure 1 shows a Construction of u-health care system with IMD [1][2][3][4].

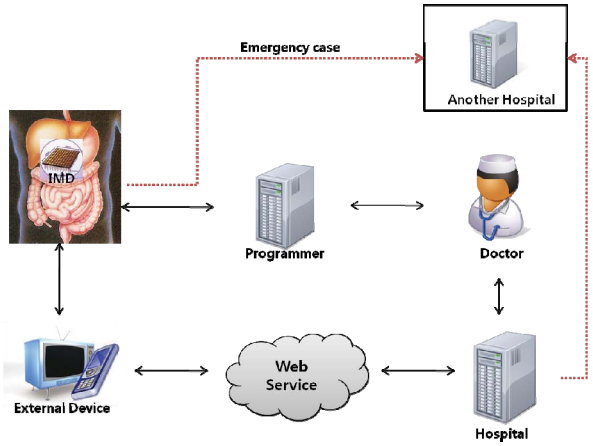

Figure 1. Construction of u-healthcare system

The u-healthcare system consists of IMD, programmer, doctor, an external device and web service. IMD is implanted in patient's body, measures the physical information and sends it to programmer and the external device. The doctor uses programmer to check the patient's vital information from IMD and adjust the function of IMD. The patient can check his condition in real time using the external device and get a diagnosis through web service

provided by the hospital. In case that a patient has an emergency and he is out of area that his doctor or hospital is in charge, a local hospital receives the medical record of patient from relevant hospital, and controls IMD and performs a treatment.

B. *Previous works for access control of IMD*

If IMD does not provide access control and only a person with doctor's approval can access IMD, it could make a patient in danger. Suppose that he has to get medical treatment from other hospital during his doctor is out of office, his life could be in danger. D.Halperin et al. [3][6] suggested a scheme which sounded an alarm or vibrated if any malicious access to IMD was detected. Although, it may detect the attack and take a measure afterward, it has a problem that it cannot provide radical prevention of attack.

C.Israel et al. [7] proposed a scheme that allowed access to IMD only within the close distance. This method measures communication time of message and denies the access, if measured time exceeds a certain period of time. However, this method has a problem that the attacker can get the access to IMD from a long distant using the device, which enables telecommunication [8]. To solve this problem, Kasper B. Rasmussen et al. [9] proposed a scheme verifying proximity with differences of the sound signal transferred. However, this method still has a problem that the attacker can try to access, and get permission by setting the device close enough to access.

To solve the problem of D.Halperin et al.'s scheme and C.Israel et al.'s scheme, Tamara Denning et al. [2] suggested IMD system, which used Cloaker. Cloaker is the external device, which controls access to IMD and protects IMD from the attacker.

C. *IMD System based on Cloaker*

Tamara Denning et al. proposed IMD access control using the external device which the patient keeps on him. Since Cloaker mediates the communication between IMD and programmer, IMD can be protected from external attack. Moreover, limitation of computational cost and power-consuming problem can be mitigated. This system consists of IMD, Cloaker and programmer as following Table 1.

TABLE I. DEVICE DESCRIPTION OF CLOAKER BASED SYSTEM

Device	Description
IMD	- measures patient's vital information implanted in body - treat following programmed firmware - has restrictions of battery consumption and replacement, and computational cost - communication range within 5 meters
Programmer	- collects patient's vital information from IMD - sends firmware update messages to change treatment functions of IMD
Cloaker	- has wireless communication ability, then mediates between IMD and programmer - has high computation ability and capacity. It can store various information (keys, log data, etc.) - can replace battery. It does not have restriction of battery consumption

In emergency case, Cloaker allows programmer to access directly when a doctor removes patient's Cloaker. Then, a patient can be treated, although he is away from his hospital. However, this case has problems shown in Figure 2.

In case Cloaker is stolen, attacker can access IMD directly regardless of patient's will. When IMD and programmer communicate, Cloaker writes the audit log. Therefore, the personal information of patient stored in Cloaker can be exposed to attackers.

When hospitals share the medical data, the data is classified according to the authority for protection of patient's privacy and studies on this subject is on-going. However, any study on privacy protection between programmer and IMD has never been done. For these reasons, in this paper we propose Cloaker based scheme that protects the patient's privacy and allows programmer and IMD to communicate securely in emergency case.

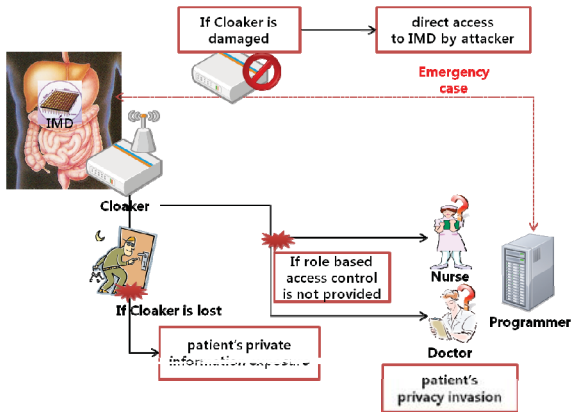

Figure 2. The problems of existing IMD Access Control based on Clocker

III. SECURITY REQUIREMENTS OF IMD SYSTEM

A. *Types of Treat and Attacker*

When the attacker manipulates IMD system, the patient can be in danger and the privacy can be exposed. Types of IMD attacker can be classified as shown in Table 2.

TABLE II. TYPES OF ATTACKER

Attacker	Description
Passive Attacker	eavesdrop messages from communicating devices
Active Attacker	malicious attacker as an interface communicating external or internal devices
Inner Attacker	healthcare specialist, software developer, hardware designer, or patient

The attacker can perform eavesdropping and replay attack to get the personal information and permission. Moreover, in case that the attacker repeats permission requests, the attacker can make the patient in danger. The attacker can tap the patient's information and try to get access from the outside and even the insiders.

In case of using Cloaker, when a patient loses his Cloaker, it is possible for the attacker to disguise himself as proper

programmer and get the information of patient or stored key. In addition, the attacker can get patient's information including his physical condition in audit log.

B. Security Requiments

IMD security requirements suggested by Daniel Halperin et al. [1] are stated in table 3.

When the patient is treated using IMD, only specific groups (doctor, nurse, and receptionist) should be able to access IMD. And IMD should be protected against DoS attack. In addition, remote wiping technique is required to prevent the loss of patient's privacy in case of losing a reader device.

Moreover, when IMD and the reader device are communicating, data access should be restricted for the protection of patient's privacy. When a patient needs to get treatment from other hospital, IMD should provide a secure access control method in emergency. If IMD is damaged or does not work because the battery is used up, status information should be sent quickly to both patient and doctor. Additional security requirements derived in this paper are stated in table 4.

TABLE III. SECURITY REQUIMENTS OF IMD

Security Requirement	Description
Authoization	Specific group of people can perform tasks accessing IMD
Availability	An adversary should not be able to perform successful DoS (Denial of Service) against an IMD
Device Software and Setting	Unauthorized people should not be able to modify IMDs or trigger specific device
Device-existence Privacy	Unauthorized people should not be able to determine remotely that a patient has IMDs
Measurement and Log Privacy	Unauthorized people should not be able to extract patient's measurement record, log data
Bearer Privacy	An attacker should not be able to extract patient's personal information such as name, medical record, so on.
Data Integrity	An attacker should not be able to modify measurement data, log data.

TABLE IV. ADDITIONAL SECURITY REQUIREMENTS

Security Requirement	Description
Privacy Protection against device lost	A patient's privacy should be protected although medical devices are lost.
Secure Device Authentication	When unregistered Programmer attempts to communicate with IMD, IMD should recognize whether the programmer is intended device.
secure Emergency Access	In emergency case, IMD should be accessed securely only by authorized people.

IV. PROPOSED SCHEMES

A. Notations

Notations used in proposed schemes are as following Table 5.

TABLE V. NOTATIONS OF PROPOSED SCHEME

Notation	Description	Notation	Description
K_{IC}	shared key between IMD and Cloaker	K_{CP}	shared key between Cloaker and programmer
K_{CE}	shared key between Cloaker and external device	PUK_P	programmer's public key
PUK_{CA}	public key of superior medical institution	PRK_{CA}	private key of superior medical institution
seq_p	sequence number of previous step	seq	sequence number
ID_P	identity of programmer	ID_C	identity of Cloaker
ID_E	identity of external device	M_{Status}	message containing vital information
M_{Status}'	vital information message containing accessible data by programmer	n, n', x, y	random number
$sign_K(m)$	signature of message m with private key k	$E_K(m)$	encrypt message m with key K
$D_K(m)$	decrypt message m with key K	$h(m)$	hash function of message m
T, T'	time stamp	$CHKS_M$	message M's checksum value
K_{CW}	shared key between Cloaker and web service	K_{EW}	shared key between external device and web service
$M_{IMD-status}$	message containing IMD status	$M_{Cloaker-status}$	message containing Cloaker status
$level$	permission level to access healthcare data	$permission$	positive or negative permission to access

B. System Components

Proposed system consists of IMD, programmer, Cloaker, external device and web service as shown in Table 6.

TABLE VI. SYSTEM COMPONENTS

Component	Description
IMD	- measures patient's vital information implanted in body. - send measured vital information and IMD status to Cloaker.
Programmer	- collects patient's vital information from registered IMD - requests authentication to unregistered IMD in emergency case. - sends firmware update messages, then change treatment functions of IMD.
Cloaker	- mediates between IMD and programmer in normal case. - performs device authentication, key exchange with unregistered programmer in emergency case. - has role based access list, extracts information that such programmer is able to access.
External Device	- receives IMD and Cloaker status information from Cloaker, show them to doctor and patient recognizably.
Web Service	- supports patient and doctor to check patient's condition on web site. - send remote wiping message to Cloaker when Cloaker is lost. - provides RBAC (Role Based Access Control) between Programmer and Cloaker.

MCU (Micro Controller Unit) is used for IMD to decrease power consumption and hardware size. MCU is

manufactured by T1, freescale, microchip, cypress, and so on. In general, the processing units of MCU adopt 8 to 16 bits machine, and frequencies are various, 8 to 48MHz. In this paper, we assume that MCU has the lowest hardware performance to verify efficiency of our system. Cloaker can be designed as mobile device which has lower hardware performance than present PDA. External device includes smart phone and smart TV. A server PC in the hospital can be as web service. Table 7 shows hardware specifications in our system [10][11][12].

TABLE VII. HARDWARE SPECIFICATIONS

Device	CPU(Frequency)	Network	Memory
IMD	8bit, 8MHz	Wi-Fi/RF 400~406MHz Frequency	32KB
Cloaker	32bit, 500MHz	Wi-Fi/RF	128MB
Programmer	32bit, 500MHz	Wi-Fi	128MB
External Device	16bit, 1GHz	Wi-Fi/3G/ Bluetooth	512MB
Web Service	32bit, 2GHz	3G/LAN	2GB

C. *Proposed Scheme*

Proposed scheme is composed of normal case and emergency case.

1) *Normal case÷*

In this paper, we assume that the shared keys of Cloaker, IMD and programmer are securely distributed by off-line key distribution procedure and updated periodically.

Longhua Zhang et al. [13] proposed RBAC (Role Based Access Control) for healthcare information system. In our system, user's roles consist of doctor, surgeon, pharmacist, receptionist and nurse. Each data of u-healthcare system has permission levels that determine whether each role can access data or not. If data is level 3, roles that have lower than level 3 cannot access the data. When Cloaker requests programmer's access control, web service provides RBAC of the programmer and then it gives positive or negative permission and programmer's permission level. If Cloaker receives negative permission, access of the programmer would be denied. Moreover, data which received from IMD has higher permission level than of programmer received from web service, it would not be sent to the programmer. Our proposed scheme in normal case is as following in Figure 3.

a) IMD and Cloaker share sequence number which is set to previous sequence number($seq = seq_p$).

b) Programer generates nonce n , and sends $ID_p, E_{K_{CP}}(ID_P \| n)$ to Cloaker.

c) Cloaker decrypts $E_{K_{CP}}(ID_P \| n)$ using K_{CP} (shared key with ID_P), and verifies {decrypted message's $ID_P = ID_P$ }, sets access control of ID_P .

d) Cloaker sends $ID_C, E_{K_{CW}}(ID_C \| ID_P)$ to request permission whether the programmer is available to access or not, and get the programmer's permission level. Then web service checks Cloaker and programmer's role, performs RBAC, determines programmer's access permission. And web service sends ID_W, $E_{K_{CW}}(ID_W \| permission \| level)$ to Cloaker.

e) Cloaker checks whether permission is positive or not, and gets the programmer's permission level. If permission is negative, session would be finished.

f) Cloaker sends $ID_C, E_{K_{IC}}(ID_C \| seq)$ to IMD to request patient vital information. Then IMD verifies ID_C, seq , encrypts patient's vital information M_{Status} , and sends $E_{K_{IC}}(M_{Status} \| seq)$ to Cloaker. And then, IMD and Cloaker increase sequence number seq .

g) Cloaker creates log data, and extracts information M_{Status}' that has lower than permission level of ID_P , and then sends $ID_C, E_{K_{CP}}(ID_C \| M_{Status}' \| n)$ to programmer. All of data is encrypted in Cloaker's storage.

h) Programmer verifies n, and reads patient's vital information from M_{Status}'.

i) When programmer wants to update IMD's firmware, programmer send $ID_P, E_{K_{CP}}(ID_P \| M_{order} \| n)$ to Cloaker. Cloaker verity n, creates log data, then sends ID_C, $E_{K_{IC}}(ID_C \| M_{order} \| seq)$ to IMD

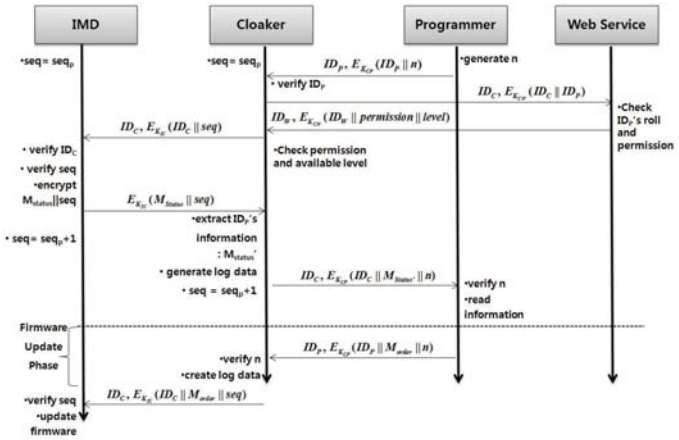

Figure 3. Proposed scheme in nomal case

In proposed scheme, patients can check their condition through external device and web site, since Cloaker communicates with external device and web service. Moreover, when patients lose their Cloaker or external device, web service is able to perform remote wiping of lost device. To support remote wiping, Cloaker has to recognize its proximity. Cloaker determines its proximity as following Figure 4.

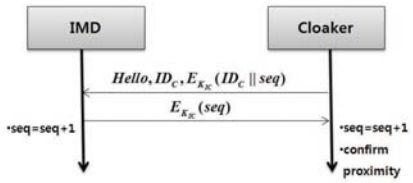

Figure 4. Proximity recognition of Cloaker

a) Cloaker generates nonce n, sends hello message $Hello, ID_C, E_{IC}(ID_C \| seq)$ to Cloaker periodically. Then IMD sends response message $E_{IC}(seq)$. If Cloaker receives response message, Cloaker determines that it is close to IMD currently.

IMD, Cloaker, external device, and web service communicate as following Figure 5 to show device status and patient's vital information.

a) External device sends request message $request$, $ID_E, E_{CE}(ID_E \| n)$ to Cloaker. Cloaker decrypts $E_{K_{CE}}(ID_E \| n)$ using K_{CE} (shared key with ID_E), and verifies {decrypted message's $ID_E = ID_E$ }.

b) Cloaker sends request message $request, ID_C$, $E_{IC}(ID_C \| seq)$ to IMD. IMD decrypts $E_{IC}(ID_C \| seq)$, verifies ID_C and seq . Then IMD sends $E_{IC}(M_{IMD-status} \| seq)$ to Cloaker. IMD and Cloaker both increase sequence number.

c) Cloaker verifies seq and sends $E_{CE}(M_{IMD-status} \| M_{Cloaker=status} \| n)$ to external device.

d) External device verifies *n*, sends ID_E, $E_{EW}(ID_E \| M_{IMD-status} \| M_{Cloaker-status} \| T)$ to web service. Web service decrypts $E_{EW}(ID_E \| M_{IMD-status} \| M_{Cloaker-status} \| T)$ using K_{EW} (shared key with ID_E), verifies ID_E, T , then confirm device status message after user authentication.

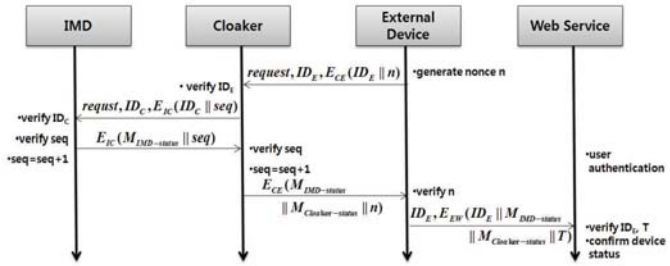

Figure 5. Intercommunication of devices

When Cloaker fails proximity recognition, Cloaker sends alarm message to external device and web service. Then web service performs remote wiping. In this case, OMA-DM protocol [14], which is become standard in mobile remote control mechanism, is recommended.

2) Emergency case

Emergency case protocol has two phases, device authentication and key exchange. Different from normal cases, Cloaker and programmer are not registered in advance. In this paper, we use the public key signature verification to authenticate devices. We assume that each country has a superior medical institution, programmer has the public key of programmer signed by the superior medical institution and Clocker has the public key of superior medical institution. Our proposed scheme in emergency case is as following in Figure 6.

[*Device Authentication Phase*]

a) programmer has $C_1 = sign_{PUK_{CA}}(PUK_P)$ issued from superior medical institution. programmer computes $C_2 = sign_{PRK_P}(T \| CHKS_{PUK_P})$, and sends $C_1 \| C_2$ to Cloaker.

b) Cloaker verifies signature C_1 using PUK_{CA} , then aquire PUK_P . Then Cloaker verifies signature of C_2 , validity of $T, CHKS_{PUK_P}$.

[*Key Exchange Phase*]

a) Cloaker computes random value x which means shared key K_{CP} with programmer. Then Cloaker computes $C_3 = E_{PUK_P}(T', K_{CP})$, and sends it to programmer.

b) Programmer decrypts C_3, and verifies validity *of* T' and acquire shared key K_{CP} .

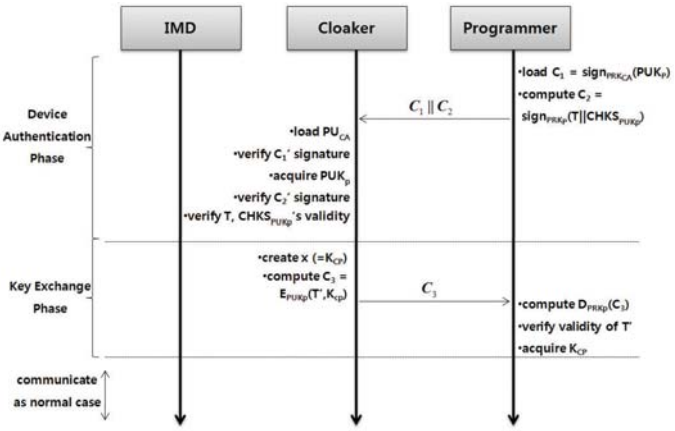

Figure 6. Proposed scheme in emergency case

V. SECURITY ANALYSIS

We analyze efficiency of proposed scheme by evaluating required time to finish the session, and evaluate the security by analyzing whether it satisfies the security requirements derived in section 3.

A. Efficiency Analysis

We analyze required time to finish session in normal case and emergency case. We assumed that proposed scheme uses AES as symmetric key encryption scheme and ECC as public key encryption scheme. The required time of each case is calculated as shown in Table 8 [15][16].

Proposed scheme takes shorter time than maximum authentication time in every case. It means that performance of each protocol is efficient.

B. Seurity Analysis

a) Authorization: Cloaker perfomrs the confidential communication and verify signature of superior medical institution. Cloaker and Programmer are registered offline, programmer that is not registered cannot access to Cloaker and IMD. Moreover, unauthorized people cannot acquire the patient's relevant information, since Cloaker extracts patient's vital information following accessing permission.

TABLE VIII. EFFICIENCY ANALYSIS

Case	Section	Computing + Transmission Time (ms)	Total Time (ms)	Maximum Authentication Time (ms)
Normal Case-data transmission	IMD ~Cloaker	0.83*2(IMD)+0.0029*2 (Cloaker)[calculation] +0.384+4.224 [transmission]	6.2738	44.56
	Cloaker ~web service	0.0029*2(Cloaker)+0.0001 39*2(web service) [calculation] + 0.0096*2 [transmission]	0.02528	
	Cloaker ~Programmer	0.0029*2(Cloaker)+0.0029 *2(Programmer) [calculation] + 0.0096 +0.56[transmission]	0.5884	
Normal Case-Firmware Update	Programmer ~IMD	0.0029(Programmer)+0.00 29*2(Cloaker)+0.83(IMD) [calculation] + 0.112 +4.48[transmission]	5.4307	44.56
Emergency Case	Programmer ~Cloaker	2.11[Programmer]+4.09*2 [Cloaker][calculation] + 0.032[transmission]	10.322	49.894
	Cloaker ~Programmer	4.09[Cloaker]+2.11 [Programmer][calculation] + 0.1024[transmission]	6.3024	

b) Availability: Since Cloaker mediates the communication with Programmer and hides IMD's identity, it can prevent the battery consumption by DoS attack to IMD. Since external device enables the battery condition of IMD and Clocker to be recognized, it is easy to know the time to replace the battery of Clocker and IMD.

c) Device Software and Setting: As programmer encrypts and transfers the commands using the registered key, unauthorized attacker cannot transfer the command.

d) Device Existence Privacy: Since IMD and programmer communicate only through Cloaker, the external device cannot recognize the device's identity and presence of IMD in patient's body.

e) Measurement and Log Privacy: When the information regarding the patient's condition is transferred from IMD to programmer, not only the transaction is encrypted, but audit log stored in Cloaker is also encrypted. Thus, proposed sheme satisfied above requirement.

f) Bearer Privacy: Medical record of patient is stored as audit log information in Cloaker and it is encrypted, the information cannot be leaked.

g) Privacy Protection against device lost: When a patient loses Cloaker, Cloaker's proximity recognition would be failed. Then, web service perform remote wiping. Since audit log would be deleted, exposure of patient's private information can be prevented against attacker.

h) Secure Device Authentication: For emergency situation, Clocker performs secure device authentication through verification of superior medical institution's siganture and timestamp. If an attacker want to get permission to Cloaker, he has to know the private key of superior medical institution PRK_{CA} or forge the signature. However, it is computationally infeasible. Moreover, although an attacker eavesdrops $C_1 \| C_2$, C_2 has timestamp T. Therfore, passive attacker cannot replay message $sign_{PRK_P}(T \| CHKS_{PUK_P})$ to perform device authentication, if he does not know programmer's private key PRK_P. Thus, proposed scheme satisfies the secure device authentication.

i) Emergency Access: In case of emergency, if programmer wants to get shared key K_{CP} from Cloaker, Clocker performs device authentication in previous step. Proposed scheme provides secure device authentication mechanism as above. Therefore, unauthorized programmer cannot acquire permission to IMD, even if an attacker disguises emergency case.

VI. CONCLUSION

In this paper, we proposed secure u-healthcare system based on Cloaker. Since access control of IMD is managed by Cloaker, battery limitation of IMD can be mitigated. Moreover, presence of IMD can be hidden by Cloaker and DoS attack towards IMD can also be mitigated. In addition, the patient's privacy can be protected since role based access control is provided when Cloaker communicates with programmer.

It is possible to check the status of IMD and Cloaker through interoperating with external device and web service. Therefore, the doctor can check physical condition at anytime and anywhere. Even if the patient is out of local hospital area and required to have a treatment, IMD can be controlled securely through device authentication and key exchange. Therefore, the treatment can be provided in emergency case. The proposed schemes allow the patient to share his personal information to the medical institution without anxiety and provide secure u-healthcare system with IMD.

ACKNOWLEDGMENT

"This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2010-(C1090-1031-0005))

This work was supported by Defense Acquisition Program Administration and Agency for Defense Development under the contract UD100002KD.

"This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the "ITRC" support program supervised by the NIPA(National IT Industry Promotion Agency)" (NIPA-2010-C1090-1001-0004)

REFERENCES

[1] Daniel Halperin, Thomas S. Heydt-Benjamin, "security and privacy for implantable medical devices", IEEE Pervasive Computing Vol 7, Issue 1, pp. 30-39, 2008.

[2] T. Denning, K. Fu, and T. Kohno, "Absence makes the heart grow fonder new directions for implantable medical device security", 3rd USENIX Workshop on Hot Topics in Security, pp.1-7, 2008.

[3] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel. "Pacemakers and implantable cardiac defibrillators: Software radio

attacks and zero-power defenses", In IEEE Symposium on Security and Privacy. IEEE Computer Society, pp. 1-14, 2008.

[4] Fuchao Zhou, Hen-I Yang, José M. Reyes Álamo, Johnny S. Wong and Carl K. Chang, "Mobile Personal Health Care System for Patients with Diabetes", 8th International Confernece on Smart Homes and Health Telematics, pp.94-101, 2010.

[5] S.K.S. Gupta, T. Mukherjee, and K. Venkatasubramanian, "Criticality aware access control model for pervasive applications", In Pervasive Computing and Communications, pp.251-257, 2006.

[6] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel, "Security and privacy for implantable medical devices" IEEE Pervasive Computing, pp.30-39, 2008.

[7] C. Israel, S. Barold. "Pacemaker systems as implantable cardiac rhythm monitors", In American Journal of Cardiology, pp. 442-445, 2001.

[8] I. Kirschenbaum, A. Wool, "How to build a lowcost, extended-range RFID skimmer", Cryptology ePrint Archive: Report 2006/054, 2006

[9] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based Access Control for Implantable Medical Devices", 16th ACM conference on Computer and communications security, pp. 411-419, 2009.

[10] Biotronik, "Biotronik Technical Manual", 2009.

[11] Biotronik, "http://www.biotronik.com/en/us/home".

[12] Texas Instruments, "http://www.ti.com/".

[13] Longhua Zhang, Gail-Joon Ahn and Bei-Tseng Chu, "A role-based delegation framework for healthcare information system", the seventh ACM symposium on Access control models and technologies, pp.125-134, 2002.

[14] Open Mobile Alliance, "OMA Device Management Security", OMA-TS-DM_Security- V1_2-20060602-C, 2006

[15] A. Ramachandran, Z. Zhou, and D. Huang, "Computing Cryptographic Algorithms in Portable and Embedded Devices," In Proceedings of the IEEE International Conference on Portable Information Devices (PORTABLE), pp. 1–7, 2007

[16] Julio Léopez, Ricardo Dahab, "Performance of Elliptic Curve Cryptosystems", Technical report IC-00-08