International Journal of Control and Automation
Vol. 7, No. 11 (2014), pp. 391-400
http://dx.doi.org/10.14257/ijca.2014.7.11.38

Enhanced Identity Authentication and Context Privacy Preservation in Ubiquitous Healthcare System

Hyunsung Kim

Dept. of Cyber Security, Kyungil University
Kyungsan, Kyungbuk 712-701, Korea
kim@kiu.ac.kr

Abstract

Ubiquitous healthcare (uHealthcare) technology is emerging as a solution to increasing chronic disease patients with the advent of aging of society. uHealthcare improves accessibility to medical services but it increases probability of privacy violation of personal medical information. Recently, Huang et al. proposed an identity authentication and context privacy preservation in wireless health monitoring system. However, Lee et al. showed that their scheme has lack of data privacy consideration and not enough security system for physician. Thereby, this paper proposes an enhanced identity authentication and context privacy preservation to solve the problems mentioned in Lee et al. The proposed scheme uses smartcard for the additional authentication and easiness to keep secret values and encryption algorithms for the contextual privacy. Analysis demonstrates the security of the proposed scheme.

Keywords: *Ubiquitous healthcare, Security, Identity authentication, Context privacy*

1. Introduction

Recent technology advances in integration and miniaturization of physical sensors, microprocessors and radio interfaces on a single chip have enabled a new generation of wireless sensor networks (WSNs) suitable for many applications [1]. One of the most promising uses of WSNs is uHealthcare system to monitor patient [2-3]. Sensor node can be placed on the human body to collect patient's health information (PHI) that is called medical body area network (BANs) [4-5]. Remote monitoring based on BANs allows an individual's PHI to be collected and sent to uHealthcare center, where physician is able to view the data remotely. Despite such benefits for the patient being monitored, uHealthcare system leaves patient's PHI highly vulnerable [6-7]. Thereby, the most important challenge in uHealthcare system is how to ensure the patient privacy during transmission of PHI to avoid the threat from attackers.

There are many researches to propose mechanisms to enhance privacy and security in uHealthcare system [8-11]. Jian *et al.*, proposed a location privacy routing protocol, call LPR, to achieve path diversity [8]. By combining LPR with fake packet injection, the location privacy of the receiver can be protected, and subsequently, the contextual privacy is achieved. Similar to [8], Lin *et al.*, in [9] deal with the contextual privacy also from protecting the receiver's location privacy. They proposed a strong anti-wiretapping privacy protection system which used the identity-based cryptography (IBC) to encrypt data based on Diffie-Hellman problem, verify the information sent by the patient through the digital signature, and applied the broadcast mechanism for the global network eavesdropping to achieve the objective of protecting patient privacy. Recently, Huang *et al.*, proposed identity authentication and context privacy preservation in wireless health monitoring system [10]. They argued that the scheme could provide confidentiality, authenticity,

ISSN: 2005-4297 IJCA

efficiency and the context privacy. However, Lee *et al.*, in [11] reported the security and privacy concerns that Huang *et al.*, scheme has lack of context privacy and not enough security for physician.

The purpose of this paper is to enhance the security and privacy concerns of Huang *et al.*, security scheme reported by Lee *et al.*, To do this, this paper reviews Huang *et al.*, security scheme in detail and Lee *et al.*, security concerns on it. Then we will propose an enhanced identity authentication and context privacy preservation, which uses smartcard for entity authentication. Analysis shows that the proposed security scheme could efficiently solve the security and privacy concerns in Huang *et al.*, scheme.

This paper is organized as follows. Section 2 reviews the related works focused on Huang *et al.*, security scheme and Lee *et al.*, security concerns on it. An enhanced identity authentication and context privacy preservation scheme is proposed to solve the security concerns in Huang *et al.*, scheme at Section 3. Security analyses and conclusion are given in Sections 4 and 5, respectively.

2. Related Works

This section reviews uHealthcare system configuration, healthcare monitoring architecture, Huang *et al.*, security scheme and Lee *et al.*, security concerns on Huang *et al.*, scheme [10-11].

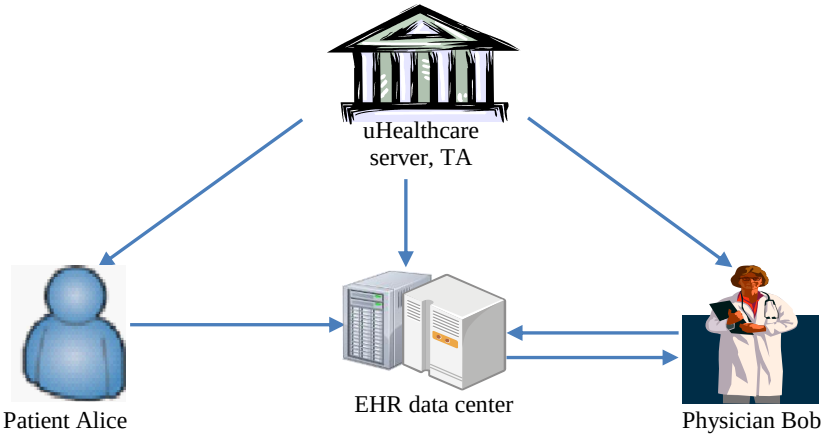


Figure 1. uHealthcare System Configuration

2.1. uHealthcare System Configuration

The design of uHealthcare system came with a lot of emerged challenges. The government has established stringent regulations to ensure that the security and privacy of patients PHI are properly protected, for example, HIPAA [12]. However, if an observer knows that a patient often sends his/her PHI to a specific physician, the observer can correctly guess the patient's disease with a high probability.

To preserve the context privacy, uHealthcare system is organized by an uHealthcare server, also named as a trusted authority (TA). The system model includes the registered patients, physicians, electric health record (EHR) database in the uHealthcare server and TA, as shown in Figure 1. Patient Alice, after registering herself to TA, can get the body sensor devices suitable to her, and then deploy a BAN at home so that PHI can be collected and sent to the EHR database and physicians.

2.2. Huang et al.'s Scheme

This section reviews Huang *et al.*, identity authentication and context privacy preservation on the concept of IBC [10, 13]. Huang *et al.*, scheme includes the generation of system parameters, the registering of patients and doctors, and the transmission, reception, storage and access of PHI. The main key distribution is depending on the TA as shown in Figure 1. Table 1 defines notations used in this paper.

Table 1. Notations

Symbol	Description
A, B	Patient Alice and physician Bob
ID_i	Identification of i
k	Security parameter
G_i	Cyclic group
P_0	Generator of G_1
$\hat{e}$	Bilinear pairing $G_1 \times G_1 \rightarrow G_2$
s_0	Master key of TA
S_i	Private key of i
Q_i	Public key of i
IBC_Q	IBC encryption by Q
IBS_S	IBS signature by S
H	Hash function
H_1	Hash function 1, which maps $\{0,1\}^* \rightarrow G_1$
H_2	Hash function 2, which maps $G_1 \rightarrow \{0,1\}^n$
$\|\|$	Concatenation
T	Time stamp
$\oplus$	Exclusive OR operation

System Parameter Generation: To set up the system, TA first initializes all required system parameters (q, G_1, G_2, $\hat{e}$, P_0, H_1). TA selects a random number $s_0 \in Z_q^*$ as a master-key and always keeps it secret. Then the two hash functions H_1 and H_2, and a generator P_0 are chosen. The system uses IBC as the encryption algorithm and IBS as the signature algorithm. All PHIs are stored in the EHR database. TA issues the private key $S_{EHR} = s_0 H_1(ID_{EHR})$ and the corresponding public key $Q_{EHR} = s_0 P$ for the health monitoring server with EHR database.

Physician and Patient Registration: Alice is a heart disease patient. The cardiovascular disease doctor Bob diagnoses Alice in hospital. When Alice registers in the health monitoring system, she inputs her personal information and then gets her personal identity ID_A from the health monitoring server. TA computes her private key $S_A = s_0 H_1(ID_A)$, and transfers the corresponding public key $Q_A = sP$ to the health monitoring server. Alice gets the medical equipment of heart disease, Bob's ID and public key Q_{EHR} of the EHR data center.

The cardiovascular disease doctor Bob gets his identity ID_B when he fills in personal information to register the health monitoring server. Bob inputs the personal logon password PWD_B, computes the hash value $H(PWD_B)$ which is stored in EHR data center. Bob gets his private key $S_B = s_0' H_1(ID_B)$ and the corresponding public key $Q_B = s_0' P$ from TA.

Patient Health Information Transmission: After Alice gets the medical equipment and goes back to home, the BAN constructed by these instruments can collect her health data m. Before the information are sent to the EHR data center through

Internet, it is necessary to take corresponding encryption and put signature to ensure that during the information transmission process it can resist the malicious attacks like decryption, tamper and forging, etc. At the same time, the scheme uses time stamp technology to against replay attack. The input is the collected Alice's health information m, and the output is a cipher text $C=IBC_{Q_{EHR}}\{T||ID_A||m||ID_B||IBS_{S_A}(ID_A||m||ID_B)\}$, which is ready to be sent.

Patient Health Information Receiving and Storing: Patient Alice's PHI is transferred to the EHR data center. When EHR data center receives the cipher text C, firstly it uses its own private key to decrypt the message and verify the legitimate identity of Alice. The message stored in the EHR data center is the cipher text $C=IBC_{Q_{EHR}}(ID_A||m||ID_B)$ encrypted with the private key of the health monitoring server.

Patient Health Information Recovering: The health monitoring server sends a notice message which shows the receiving information of the patient Alice to the doctor Bob. Registered Bob enters the health monitoring server with the password PWD_B. After the health monitoring server authenticates Bob's identity of physician based on role-based access control, Bob enters into the system and access the information m by querying.

2.3. Lee et al.'s Security Concerns on Huang et al.'s Scheme

Lee *et al.*, showed that Huang *et al.*, scheme has lack of context privacy and not enough security for physician [11]. This subsection reviews Lee et al.'s the security and privacy concerns.

Lack of Data Privacy Consideration: Huang *et al.*, claimed that cutting off the direct link between a patient and his/her physician is necessary to provide the context privacy. Through the traffic analysis, an attacker can identify the relation between patients and doctors then determine the patient's health condition. In the Huang et al.'s scheme, the EHR database center keeps the data and physicians take the initiative to log on EHR data center to access information. Huang *et al.*, argued that the information $IBC_{Q_{EHR}}(ID_A||m||ID_B)$ in the scheme achieves unconditional link privacy by doctors' logging on and the only way for the adversary to find $IBC_{Q_{EHR}}(ID_A||m||ID_B)$'s destination is by using all traffic information he/she could obtained. However, in the eye of the adversary, each physician will get message only if they log on. It is not at the same time that the patients and doctors send or get messages. The adversary does not know the information from a certain patient transports to which doctor. However, the problem of Huang et al.'s scheme is the disclosure of PHI to the EHR database center. For example, in the absence of patient consent, an insider of the EHR database center may damage the patient's data and harm the patient for their personal reasons. In a patient medical record system, insiders may modify the medical records intentionally. For example, suppose an insider wrongly alters the patient's medical data, such as, illness conditions, severe allergies, and specifically blood type, all of which pose life-threatening risks.

Not Enough Security System for Physician: The patients send remotely the health information to the EHR data center. Then the IBS is used to sign the information. After the EHR health center receives the cipher text message, the information is determined whether it is from a legitimately registered user by verifying the identity signature of patient. If the communication party is found as an illegal user, the process is terminated immediately so that we can resist effectively the false information or identity from an attacker to deceive the hospital. Doctors also need to

be authenticated with identity and password for accessing to EHR data center in order to against forgery attacks. However, Doctors only use $H(PWD_B)$ to be authenticated to the EHR data center, which has weak entropy for the security and weak against password guessing attack. Furthermore, there are lots of tendency that insiders of the EHR could perform masquerading attack due to the verifier table which should be keep in the EHR.

3. Improved Identity Authentication and Context Privacy Preservation

In this section, we propose an improved identity authentication and context privacy preservation for uHealthcare system to solve the security problems noted by Lee et al. in [11]. Privacy issues become a big issue in ubiquitous computing and need to be considered to design security schemes in uHealthcare system. It is necessary to look into privacy issues in Huang et al.'s security scheme. Their scheme's privacy issues are divided into two categories: content oriented privacy and contextual privacy. Contextual privacy attack means an adversary has the ability to link the source and the destination of a message in the system. If an adversary can link the patient with a specific physician, the patient's contextual privacy will be disclosed. An improved privacy scheme should be devised to withstand the attack by using smartcard for the authentication and available encryption algorithms for the contextual privacy.

The proposed scheme also includes the generation of system parameters, the registering of patients and doctors, and the transmission, reception, storage and access of PHI.

3.1. Initial Registration

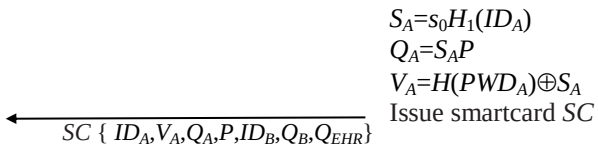
Figure 2 shows the overview of initial registration phase. All registrations are carried out by TA, which could think as the uHealthcare server, via a secure channel. When Alice who is a heart disease patient, registers in the uHealthcare system, she inputs her personal information PI and password PWD_A, computes the hash value $H(PWD_A)$ and sends PI and the hashed value to TA. TA computes Alice's private key $S_A=s_0H_1(ID_A)$, the corresponding public key $Q_A=S_AP$ and the verifier $V_A=H(PWD_A)\oplus S_A$, and stores Q_A in it. Alice gets the medical equipment of heart disease and a smartcard stored in { ID_A, V_A, Q_A, ID_B, Q_B, Q_{EHR} }, where ID_B is identification of Bob who is a cardiovascular disease doctor in hospital, and Q_B and Q_{EHR} are public keys of Bob and EHR data center.

The cardiovascular disease doctor Bob gets his identity ID_B when he fills in personal information to register the uHealthcare server. Bob inputs the personal logon password PWD_B, computes the hash value $H(PWD_B)$, and sends { ID_B, $H(PWD_B)$ } to EHR data center. TA computes Bob's private key $S_B=s_0H_1(ID_B)$, the corresponding public key $Q_B=S_BP$ and verifiers $V_B=H(PWD_B)\oplus S_B$ and $VP_B=H(PWD_B)\oplus s_0$, and transfers Q_B and VP_B to the health monitoring server, which need to be stored in EHR data center. Bob gets his smartcard stored in { ID_B, V_B, Q_B, Q_{EHR} } from TA.

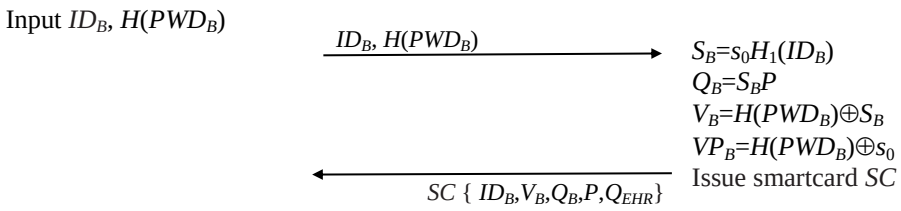
3.2. Patient Health Information Transmission

Figure 3 shows the overview of patient health information transmission. After Alice gets the medical equipment and goes back to home, the BAN constructed by these

Patient (*A*)		**Trusted Authority (TA)**
Input PI, $H(PWD_A)$	$PI,H(PWD_A)$ →	Select ID_A



(a) Patient registration



(b) Physician registration

Figure 2. Initial Registration Phase

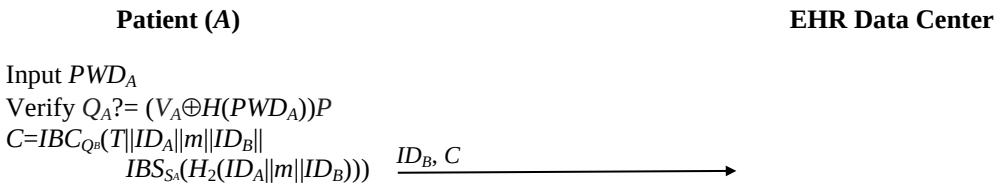


Figure 3. Patient Health Information Transmission Phase

instruments can collect her health data m. Before the information are sent to the EHR data center through Internet, it is necessary to take corresponding authentication and encryption, and put signature to ensure that during the information transmission process it can resist the malicious attacks like decryption, tamper and forging, etc. Authentication is performed by verifying whether Q_A is equal to the value $(V_A\oplus H(PWD_A))P$ on the smartcard after the input password PWD_A. Only after the successful authentication, the scheme uses time stamp technology to against replay attack, computes a cipher text $C=IBC_{Q_B}(T||ID_A||m||ID_B||IBS_{S_A}(H_2(ID_A||m||ID_B)))$ with the collected Alice's health information m, and sends { ID_B, C } to EHR data center.

3.3. Patient Health Information Receiving and Storing

Patient Alice's PHI is transferred to the EHR data center. When EHR data center receives the message { ID_B, C }, it stores the message, notifies to Bob, and waits until Bob checks the message. The message stored in the EHR data center is the cipher text $C=IBC_{Q_B}(T||ID_A||m||ID_B||IBS_{S_A}(H_2(ID_A||m||ID_B)))$ encrypted with the private key of the physician Bob. Only doctor Bob can access Alice's health message.

3.4. Patient Health Information Recovering

Figure 4 shows the overview of patient health information recovering phase. The uHealthcare server sends a notice message which shows the receiving information of the patient Alice to the doctor Bob. Registered Bob could login to the uHealthcare server with the password PWD_B only after the success of authentication.

Authentication is performed by verifying whether Q_B is equal to the value $(V_B \oplus H(PWD_B))P$ on the smartcard after the input password PWD_B. Only after the successful authentication, the smartcard sends $\{ID_B, H(PWD_B)\}$ to the uHealthcare server over the intranet, which could use secure socket layer to secure the communication. After the uHealthcare server authenticates Bob's identity and password based on role-based access control, Bob enters into the system and accesses the information m by decrypting C by using his private key S_B only if the hashed signature $IBS_{S_A}(H_2(ID_A||m||ID_B))$ is successfully verified by using the public key Q_A supported by the uHealthcare server. Bob sends a history data $HS=IBC_{Q_{EHR}}(ID_A||m||ID_B)$ to EHR data center to keep the history of the patient.

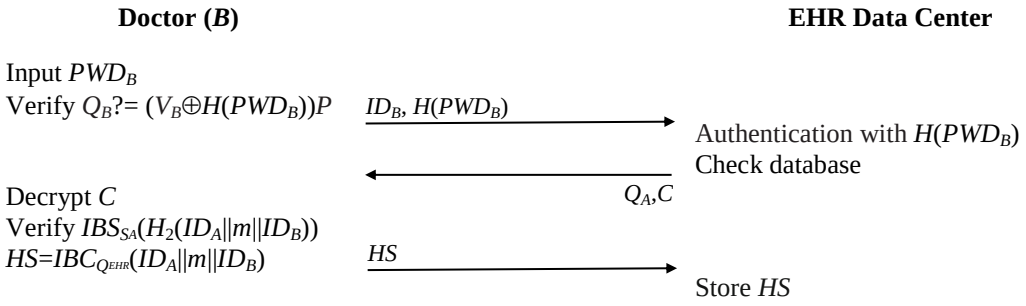


Figure 4. Patient Health Information Recovering Phase

4. Security Analyses

This section discusses security analyses by comparing the proposed scheme with Huang *et al.*, scheme in [10]

Although it is important to provide a formal security proof on any cryptographic schemes, the formal security proof of security schemes remains one of the most challenging issues for cryptography research. Until now, a simple, efficient and convincing formal methodology for correctness analysis on security schemes is still an important subject of research and an open problem. Because of these reasons, most security schemes have been demonstrated with a simple proof. Therefore, we follow the approaches used in [14-16] for comparison purpose.

We will analyze the security of the proposed security scheme to verify the overall security requirements including passive and active attacks, and contextual privacy issue as follows.

[Proposition 1] The proposed identity authentication and context privacy preservation scheme is secure against passive and active attacks.

Proof: We assume that an adversary succeeds if the adversary finds the master key s_0 or one of private keys, S_A, S_B and S_{EHR}. Therefore, we show that probability to succeed in finding the one of these keys is negligible due to the difficulty of the underlying IBC and hash function.

1. A completeness of the protocols is already proven by describing the run of the scheme in Section 3.
2. The acceptance by all entities means that each $IBS_{S_A}(H_2(ID_A||m||ID_B))$ in the corresponding message is successfully verified. That is, $IBS_{S_A}(H_2(ID_A||m||ID_B))$ computed by using S_A is verified by using the correct corresponding public key Q_A and furthermore it is embedded inside of the cipher text $C=IBC_{Q_B}(T||ID_A||m||ID_B||IBS_{S_A}(H_2(ID_A||m||ID_B)))$ by using the Bob's public key Q_B. We show that if it is the case that entities accept the messages and continue the session, then the probability that the adversary have modified the messages being transmitted is negligible. And the only way for the adversary

to find the secrets is to solve the difficulty of the underlying IBC and hash function.

3. If the adversary is passive adversary, all the adversary can gather are as follows: ID_B and C at the patient health information transmission phase. However, it is negligible to find the related key information from them due to the difficulty of the underlying IBC and hash function. Note that the information ID_B, $H(PWD_B)$, Q_A, C and HS at the patient health information recovering phase are secured from the passive adversary by using the intranet.
4. Now, we consider the active adversary with following cases.
   (a) There is no way that an adversary could get the key related information s_0, S_A, S_B and S_{EHR} stored in the smartcard or memorized by TA due to the difficulty of the underlying IBC and XOR operation. Since S_A and S_B are stored in the smartcard by amplifying with the hashed password, we can see that they remain in secure.
   (b) An adversary cannot impersonate a patient A to cheat B or EHR data center. That is the attacker cannot generate a valid message without knowing the password PWD_A, since the attacker cannot pass the verification of Q_A in the beginning of the patient health information transmission phase.
   (c) An adversary cannot impersonate a physician B to cheat EHR data center. As described above, only the legal B can form the legal authentication message inside of the intranet by including the proper secret from the smartcard, which needs to be properly verified by using a proper password PWD_B at the beginning of the patient health information recovering phase. Even if the attacker uses the legal handshake message, the attacker still cannot get any useful information from the session information due to the difficulty of the underlying IBC, and cannot generate the consequent valid messages.

Finally, we could say our scheme is secure against passive and active attacks.

[Proposition 2] The proposed identity authentication and context privacy preservation scheme can provide contextual privacy.

Proof. The contextual privacy is defined as privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obeying the governing norms of distribution within it, and provided by supporting distinguishability between messages, which is the state of being indistinguishable to the adversary [17]. The proposed scheme uses IBC and the timestamp. By using the session dependent information and encryption, the scheme could support session contextual privacy. This means that the probability of messages in each session of the proposed scheme from the adversary's perspective stays the same before and after the adversary's observation.

We compare the proposed scheme with Huang et al.'s scheme in terms of security properties [10-11]. In Table 2, it can be seen that our scheme satisfies all above-mentioned requirements. It can be seen that Huang et al.'s security scheme in [10] cannot provide insider privacy against HER data center and does not provide full authentication for physician as mentioned in Lee *et al.*, research in [11].

Table 2. Security comparison with Huang et al.'s scheme

Property / Scheme	PR1	PR2	PR3	PR4	PR5
Huang et al.'s in [10]	Secure	Provide	Partially	Provide	N/A
Proposed scheme	Secure	Provide	Provide	Provide	Provide

* PR1 : confidentiality, PR2 : integrity, PR3 : authentication, PR4 : contextual privacy, PR5 : insider privacy

5. Conclusion

An identity authentication and context privacy preservation was proposed by Huang *et al.*, over wireless health monitoring system. However, Lee et al. showed that Huang *et al.*, security scheme has lack of data privacy consideration and not enough security system for physician. To solve the security weaknesses, this paper proposed an enhanced identity authentication and context privacy preservation to solve the problems mentioned in Lee *et al.* The proposed scheme uses smartcard for the additional authentication and easiness to keep secret values and encryption algorithms for the contextual privacy.

Acknowledgements

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575).

References

[1] R. Faludi, "Building Wireless Sensor Networks with ZigBee, XBee, Arduino, and Processing, O'Reilly Mdeia, **(2010)**.
[2] H. Kim, "Freshness Consideration of Hierarchical Key Agreement Protocol in WSNs", International Journal of Security and Its Applications, vol. 8, no. 1, **(2014)**, pp. 81-91.
[3] H. Kim and S. W. Lee, "Enhanced Novel Access Control Protocol over Wireless Sensor Networks", IEEE Transactions on Consumer Electronics, vol. 55, no. 2, **(2009)**, pp. 492-498.
[4] K. Mtonga, H. Yang, E. J. Yoon and H. Kim, "Identity-based Privacy Preservation Framework over u-Healthcare System", Lecture Notes in Electrical Engineering, vol. 240, **(2013)**, pp. 203-210.
[5] K. Mtonga, "Secure Authentication Scheme for Remote Health Monitoring System suing WBAN", M. S. Thesis, Kyungil University, **(2014)**.
[6] J. Welch, F. Guilak and S. D. Baker, "A wireless ECG smart sensor for broad application in life threatening event detection", Proc. on Engineering in Medicine and Biology Society 2004, **(2004)**, pp. 3447-3449.
[7] H. Kim, E. K. Ryu and S. W. Lee, "Security Considerations on Cognitive Radio based on Body Area Networks for u-Healthcare", Journal of Security Engineering, vol. 10, no. 1, **(2013)**, pp. 9-20.
[8] Y. Jian, S. Chen, Z. Zhang and L. Zhang, "Protecting receiver location privacy in wireless sensor networks", Proc. of INFOCOM 2007, **(2007)**, pp. 1955-1963.
[9] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, "SAGE: a strong privacy preserving scheme against global eavesdropping for ehealth system", IEEE Journal of Selected Areas of Communications, vol. 27, no. 4, **(2009)**, pp. 365-378.
[10] Q. Huang, X. Yang and S. Li, "Identity Authentication and Context Privacy Preservation in Wireless Health Monitoring System", International Journal of Computer Network and Information Security, vol. 4, **(2011)**, pp. 53-60.
[11] S. Lee, H. Kim and S. W. Lee, "Security Concerns of Identity Authentication and Context Privacy Preservation in uHealthcare System, Proc. of SNPD 2013, **(2013)**, pp. 107-114.
[12] Office for Civil Rights, United State Department of Health and Human Services, Medical Privacy, National Standards of Protect the Privacy of Personal-Health-Information. Available online: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html.
[13] W. Mao, "Modern Cryptography: Theory and Practice, Prentice Hall PTR, **(2003)**.
[14] H. Kim, Location-based Authentication Protocol for First Cognitive Radio Networking Standard, Journal of Network and Computer Applications, vol. 34, **(2011)**, pp. 1160-1167.

[15] H. Kim, "Freshness Consideration of Hierarchical Key Agreement Protocol in WSNs", International Journal of Security and Its Applications, vol. 8, no. 1, **(2014)**, pp. 81-91.
[16] H. Kim, "End-to-End Authentication Protocols for Personal/Portable Devices over Cognitive Radio Networks", International Journal of Security and Its Applications, accepted and will be appeared, vol. 8, no. 3, **(2014)**.
[17] H. Nissenbaum, Privacy as Contextual Integrity, Washington Law Review, **(2004)**, pp. 101-139.

Author

Hyunsung Kim, he is a professor at the Department of Cyber Security, Kyungil University, Korea from 2012. He received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.

