Journal of Organizational and End User Computing
Volume 33 • Issue 3 • May-June 2021

A Lightweight Three-Factor Anonymous Authentication Scheme With Privacy Protection for Personalized Healthcare Applications

Mengxia Shuai, University of Science and Technology of China, Anhui, China
Nenghai Yu, University of Science and Technology of China, Anhui, China
Hongxia Wang, Southwest Jiaotong University, Chengdu, China
Ling Xiong, Xihua University, Chengdu, China
Yue Li, Southwest Jiaotong University, Chengdu, China

ABSTRACT

Security and privacy issues in wireless medical sensor networks (WMSNs) have attracted lots of attention in both academia and industry due to the sensitiveness of medical system. In the past decade, extensive research has been carried out on these security issues, but no single study exists that addresses them adequately, especially for some important security properties, such as user anonymity and forward secrecy. As a step towards this direction, in this paper, the authors propose a lightweight three-factor anonymous authentication scheme with forward secrecy for personalized healthcare applications using only the lightweight cryptographic primitives. The proposed scheme adopts pseudonym identity technique to protect users' real identities and employs one-way hash chain technique to ensure forward secrecy. Analysis and comparison results demonstrate that the proposed scheme can not only reduce execution time by 34% as compared with the most effective related schemes, but also achieve more security and functional features.

KEYWORDS

Authentication, Forward Secrecy, Privacy Protection, User Anonymity, Wireless Medical Sensor Networks

INTRODUCTION

The Internet of Things (IoT) is an emerging mode of modern wireless telecommunications, which allows objects to be sensed or controlled remotely over existing network infrastructure. By combining with cloud computing and fog computing (Qi, Zhang, Dou, & Ni, 2017; Gill, Chana, & Buyya, 2017; Qi, Yu, & Zhou, 2017; Gong, Qi, & Xu, 2018; Qi et al., 2018a), IoT devices can be used to build many service-based applications, such as smart devices (Cui, Zhang, Cai, Liu, & Li, 2018; Cheng, Xu, Tang, Sheng, & Cai, 2018), smart home (Liu, et al., 2018) and security-related applications (Wang, Li, Shi,

DOI: 10.4018/JOEUC.20210501.oa1

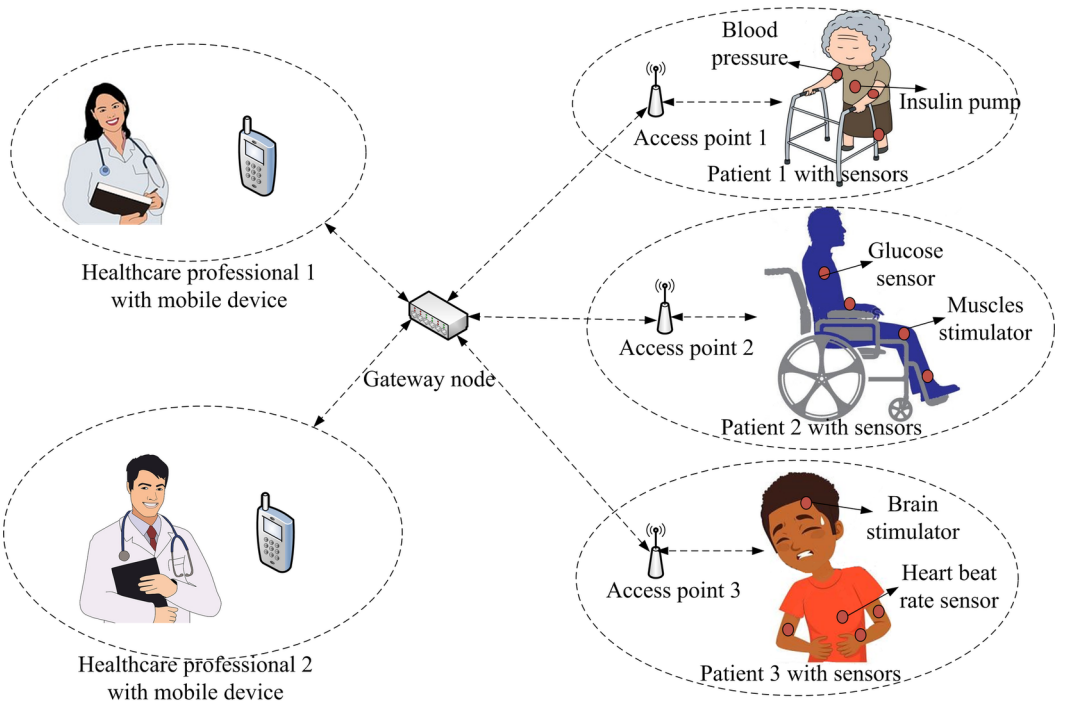
Lian, & Ye, 2016; Qi, Zhou, Yu, & Liu, 2017; Ma, Luo, Li, Bao, & Zhang, 2018; Zhang, Qin, Zhang, Liu, & Luo, 2018; Qi et al., 2018b). IoT devices can also be used to enable remote health monitoring, which is a new field known as wireless medical sensor networks (WMSNs). WMSNs have attracted lots of attention in both academia and industry because of the potential in improving the quality of medical services (Walczak & Mann, 2010; Lee, Ghapanchi, Talaei-Khoei, & Ray, 2015). Through WMSNs, healthcare professionals are able to access the patients' sensitive data collected from the medical sensor nodes which are placed on/in patients' bodies, and provide remote medical treatment, emergency medical assistance or give some constructive advice on the patients' further treatment.

A typical structure of WMSNs for personalized healthcare applications is demonstrated in Figure 1. Although WMSNs bring a lot of convenience to people's life (Siddesh et al., 2017), security and privacy issues in WMSNs are becoming great challenges due to the sensitiveness of medical system (Ameen, Liu, & Kwak, 2012; Xu, Qi, Dou, & Yu, 2017). The medical data collected from the medical sensor nodes is sensitive, and the privacy of these data is protected legally. Due to the open feature of wireless communication, an adversary can intercept and alter the transmitted messages easily. Once obtaining these sensitive data, an adversary may acquaint the disease what the patient has and profit financially by selling sensitive data, it is a serious violation of the patient's privacy. Further, the adversary can even misreport or distort the patient's physiological data to cause physical harm, it may result in improper diagnosis and treatment. Therefore, it is very important to design an effective authentication scheme to guarantee secure communication and protect patients' privacy in WMSNs.

Related Work

In the past decade, many authentication schemes are proposed to solve the security issues in WMSNs. In 2007, Hu et al. (2007) designed a telecardiology sensor network platform for real-time healthcare data collection using the symmetric cryptography. Two years later, Huang et al. (2009) presented

Figure 1. A typical structure of WMSNs



a healthcare monitoring architecture for monitoring elderly or chronic patients in their residence, which used Advanced Encryption Standard (AES) algorithm to provide authentication and secret communication. Unfortunately, neither of them could achieve mutual authentication successfully. In 2009, Malasri et al. (2009) designed a secure WMSN system for healthcare based on symmetric cryptography and elliptic curve cryptography (ECC), they implemented their mechanisms on a wireless mote platform. Later, Das (2009) presented a two-factor user authentication protocol for WSN and claimed their protocol could provide strong authentication and resist various attacks. Unfortunately, Khan et al. (2010) pointed out that Das's scheme (Das, 2009) was vulnerable to privileged-insider attack and Gateway node (GWN) bypass attack. In 2012, Kumar et al. (2012) presented an efficient and strong authentication protocol, named E-SAP, for healthcare application using WMSNs. They demonstrated that their protocol was more secure against many practical attacks. But later, He et al. (2015) in 2015 pointed out that the scheme proposed by Kumar et al. failed to resist some known attacks, liking off-line password guessing attack and privileged insider attack. To overcome their security shortcomings, they proposed a robust anonymous authentication protocol for healthcare applications using WMSNs. One year later, Li et al. (2016) pointed out that He et al.'s scheme (He et al., 2015) was not only incorrect in authentication and session key agreement phase, but also lacked wrong password detection mechanism. Further, they proposed a new user anonymous authentication protocol based on WMSNs. In their scheme, the biometric was introduced as the third authentication factor. Similarly, Mir et al. (2017) also showed that He et al.'s scheme (He et al., 2015) still suffered from various security flaws, including inefficient login phase, password guessing attack, forward secrecy. They also proposed an improved scheme and claimed that their scheme was secure in forward secrecy. However, the authors find out their scheme is still prone to forward secrecy attack. An adversary can guess the user identity offline through the transmitted message if GWN's secret key is compromised, the adversary can further compute the session key. Hence, Mir et al.'s scheme (Mir et al., 2017) failed to achieve forward secrecy. At the same year, Wu et al. (2017) also claimed that He et al.'s scheme (He et al., 2015) still had some vulnerabilities, including off-line password guessing attack, the impersonation attack and the sensor node capturing attack. Hence, they proposed an energy-efficient scheme with a lightweight design for WMSNs. But later, Srinivas et al. (2017) observed that Wu et al.'s scheme was not only failed to resist various attacks, such as off-line guessing attack, privileged insider attack and new smart card issue attack, but also not suitable for practical applications. To compensate for these defects, they designed a symmetric key based authentication protocol for WMSNs environment using only computationally efficient operations to achieve lightweight attribute. Unfortunately, the authors find that all these schemes cannot achieve forward secrecy effectively.

Motivation and Contributions

User anonymity and forward secrecy are two indispensable security properties of the authentication scheme (Gope & Hwang, 2016), especially for some scenarios containing real-time sensitive data, such as health monitoring. If the long-term keys are obtained by an adversary, it may cause the disclosure of the session key used in previous communications. Further, the content of previous communications may be revealed. The adversary can access the patients' physiological data and assess the patients' health status, it is devastating for the patients' privacy. To the best of our knowledge, none of the existing scheme can achieve user anonymity and forward secrecy at the same time. In particular, it is disturbing to find that forward security has not been considered even when designing authentication schemes (He et al., 2015; Li et al., 2016; Srinivas et al., 2017). In fact, forward secrecy is present in several major protocol implementations, such as SSH and IPsec. In addition, forward secrecy has also been seen as an important security feature and provided to users by several large internet information providers, such as Google, Twitter, Facebook and Apple. It is a consensus to take forward security into consideration in the design of an effective lightweight anonymous authentication scheme (Mir et al., 2017; Khan & Kumari, 2013; Jin et al., 2015). As a step towards this direction, in this paper,

the authors adopt pseudonym identity technique to protect healthcare professional's real identity, and employ one-way hash chain technique (Gope & Hwang, 2016) to ensure forward secrecy. The contributions of this paper are summarized mainly as follows:

1. The authors present a novel and lightweight three-factor anonymous authentication scheme with privacy protection for personalized healthcare applications using only the lightweight cryptographic primitives, which is easy to carry out in practical applications.
2. The authors use Burrows-Abadi-Needham (BAN) logic (Burrows, Abad, & Needham, 1989) to prove that the proposed scheme is secure and fulfills mutual authentication successfully.
3. The authors conduct a formal verification of the proposed scheme using the widely-accepted tool ProVerif (Burrows, 2001, pp. 82-96).
4. The security analysis shows that the proposed scheme can not only provide user anonymity and forward secrecy, but also resist various malicious attacks, such as smart card loss attack, replay attack and wrong password login attack.
5. The authors evaluate the performance of the proposed scheme with other related schemes, and the results show that the proposed scheme can reduce the computational cost substantially.

PRELIMINARY KNOWLEDGE

In this section, the authors briefly introduce security requirements for healthcare applications and adversary attack model.

Security Requirements for Healthcare Applications

Since the communications between the health professional and the medical sensor nodes are done via public channel, the designed authentication scheme must be secure and efficient. Here the authors describe some important requirements for a secure anonymous authentication scheme in WMSNs:

- **User anonymity:** The first indispensable attribute of the authentication scheme for WMSNs is user anonymity, which mainly comprises two properties. The first one is user identity-protection which means the real identity of the user cannot be figured out by the adversary. Untraceability is another important property, which guarantees the adversary neither determining who the user is nor telling apart whether two sessions are executed by the same user (Wang & Wang, 2014). Therefore, the anonymous authentication scheme is very crucial to address privacy problem in WMSNs.
- **Forward secrecy:** If the long-term keys used to generate the session key are obtained by an adversary, it may cause the disclosure of the session key used in previous communications. Further, the content of previous communications may be revealed. The adversary can access the patients' physiological data and assess the patients' health status, it is devastating for the patients' privacy. Therefore, anonymous authentication scheme must achieve forward secrecy.
- **Mutual authentication:** Mutual authentication among the health professional, GWN and the medical sensor node is needed, it is an essential requirement for all authentication schemes.
- **Session key agreement:** After mutual authentication, further communications should be encrypted using the shared session key to achieve confidentiality. Therefore, the proposed scheme should provide session key agreement.
- **Attacks resistance:** To ensure secure communication, the designed authentication scheme is able to resist various attacks, liking smart card loss attack, replay attack and wrong password login attack.

Adversary Attack Model

In this paper, the authors propose an authentication scheme based on the Dolev-Yao threat model (Dolev & Yao, 1983), which is the most widely accepted attacker model in the analysis of security protocols. According to this model, any two communicating parties communicate over an insecure channel and the endpoint entities are not considered as trusted entities. Based on this threat model and real application environments, the abilities of an adversary ***A*** are summarized as follows:

1. ***A*** may be a legitimate but malicious health professional in WMSNs.
2. ***A*** may be a legitimate but malicious medical sensor node.
3. ***A*** can intercept and modify the transmitted messages over insecure public communication channel easily (Ameen et al., 2012).
4. ***A*** can acquire all the secret values stored in the smart card using side-channel attacks (Kocher, Jaffe, & Jun, 1999).
5. ***A*** can get the long-term secret keys when forward secrecy is evaluated.
6. ***A*** is a probabilistic polynomial time attacker. That is to say, ***A*** can guess the low-entropy password and identity information within polynomial time.
7. There is no tamper-resistant hardware equipped in medical sensor nodes. In other words, ***A*** can extract all the sensitive data stored in medical sensor nodes.

THE PROPOSED SCHEME

In this section, the authors present a lightweight three-factor anonymous authentication scheme for personalized healthcare applications using WMSNs, which not only achieves the required security attributes, liking user anonymity and forward secrecy, but also withstands various attacks. The proposed scheme is divided into four phases: registration phase, login and authentication phase, password change phase. For ease of presentation, some intuitive abbreviations and notations mentioned in the proposed scheme are listed in Table 1.

Table 1. Notations

Notation	Descriptions
U_i	Remote health professional
GWN	Gateway node
SN_j	Medical sensor node
ID_i	Unique identity of U_i
PW_i	Password of U_i
fg_i	Biometric information of U_i
HID_i	Pseudonym identity of U_i
SID_j	Unique identity of SN_j
$E_k[.]/D_k[.]$	Symmetric encryption/decryption with key k
R, R_A	Random number
T_1, T_2, T_3, T_4	Current time stamp
ΔT	The maximum of the transmission delay time
K	Secret key generated by GWN
SK	Session key
$h(.)$	One-way hash function
$BH(.)$	Biohash function
$X\|\|Y$	Concatenate operation
$\oplus$	XOR operation

Registration Phase

The registration phase is divided into two parts, i.e., health professional registration phase and medical sensor node registration phase.

Health Professional Registration

When a new health professional wants to be a legitimate user in WMSNs, he/she must register in GWN first. The procedure of professional's registration is described as follows:

Step 1: The health professional U_i chooses his/her identity ID_i, password PW_i and imprints its biometrics fg_i via a sensor, and generates a random number m_i. Then U_i computes $MB_i = BH\left(m_i \,||\, fg_i\right)$, $MPW_i = h\left(ID_i \,||\, PW_i \,||\, MB_i \,||\, m_i\right)$, U_i sends the message $\{ID_i, MPW_i\}$ and his/her personal credential to GWN through a secure channel.

Step 2: Upon receiving the message, GWN generates three random integers n_i, r_i, K_1 and computes $HID_i = ID_i \oplus r_i$, $X_i = h\left(ID_i \,||\, K \,||\, n_i\right)$, $Y_i = X_i \oplus MPW_i$, $V_i = h(X_i \,||\, MPW_i)$. After that, GWN stores $\{ID_i, HID_i, n_i, K_1\}$ into its own database and also maintains a health professional personal credential table. Finally, GWN writes $\{HID_i, Y_i, V_i, K_1, h(.), BH(.)\}$ into smart card and issues it to U_i via a private channel.

Step 3: Upon receiving the smart card, U_i writes m_i into the smart card. Finally, the smart card contains $\{HID_i, Y_i, V_i, K_1, m_i, h(.), BH(.)\}$.

Medical Sensor Node Registration

The procedure of medical sensor node registration is outlined as follows:

Step 1: The medical sensor node SN_j selects the identity SID_j and transmits it to GWN via a secure channel.

Step 2: Upon receiving SID_j, GWN first checks whether SID_j exists in the medical sensor node information table. If it exists, GWN refuses the medical sensor node registration request. Otherwise, GWN generates a random integer K_2 and stores $\{SID_j, K_2\}$ into its sensor node information table. After that, GWN sends K_2 to SN_j via a private channel.

Step 3: Upon receiving the message from GWN, SN_j stores K_2 into its memory secretly.

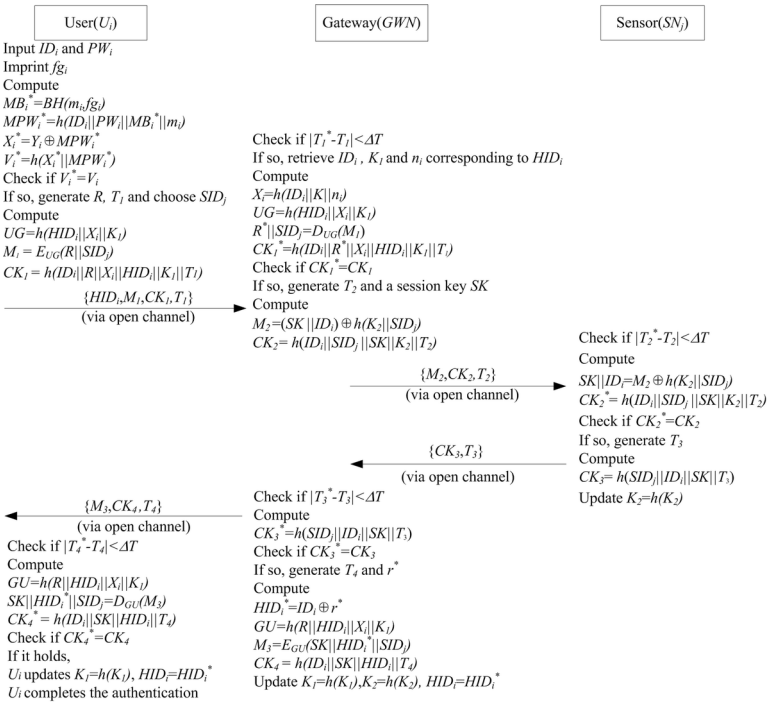
Login and Authentication Phase

When a health professional U_i wants to access a medical sensor node, he/she needs to login in GWN first. As shown in Figure 2, the procedure of health professional's login and authentication phase is described as follows:

Step 1: The health professional U_i inserts his smart card into a card reader and inputs the identity ID_i, the password PW_i and enters the fingerprint fg_i at the sensor device. Then, the smart card computes $MB_i^* = BH\left(m_i \,||\, fg_i\right)$, $MPW_i^* = h\left(ID_i \,||\, PW_i \,||\, MB_i^* \,||\, m_i\right)$, $X_i^* = Y_i \oplus MPW_i^*$, $V_i^* = h\left(X_i^* \,||\, MPW_i^*\right)$, and compares V_i* with the stored value V_i. If they are not equal, the smart card terminates the session. Otherwise, the smart card proceeds to the next step.

Step 2: After verifying the legitimacy of health professional U_i, the smart card generates a random number R and gets the current time T_1. After that, U_i selects the identity SID_j of the medical sensor node SN_j that he/she wants to access, and the smart card computes $UG = h(HID_i \,||\, X_i \,||\, K_1)$,

Figure 2. Login and authentication phase of the proposed scheme



$M_1 = E_{UG}(R \,||\, SID_j)$, $CK_1 = h(ID_i \,||\, R \,||\, X_i \,||\, HID_i \,||\, K_1 \,||\, T_1)$. Then U_i sends the login message {HID_i, M_1, CK_1, T_1} to GWN through a public channel.

Step 3: Upon receiving the login request message, GWN first checks the validity of the time stamp. GWN gets the current time T_1* and compares with the received time T_1. If the matching score $|T_1^*-T_1|$ is beyond a predefined threshold value ΔT, GWN terminates the session. Then, GWN extracts ID_i, n_i and K_1 from user information database corresponding to pseudonym identity HID_i. Next, GWN computes $X_i = h\left(ID_i \,||\, K \,||\, n_i\right)$, $UG = h\left(HID_i \,||\, X_i \,||\, K_1\right)$, $R^* \,||\, SID_j = D_{UG}(M_1)$, $CK_1^* = h(ID_i \,||\, R^* \,||\, X_i \,||\, HID_i \,||\, K_1 \,||\, T_1)$ and compares CK_1* with the received value CK_1. If they are not equal, GWN terminates the session. Otherwise, GWN believes the legitimacy of U_i. What's more, GWN generates a random number T_2, a session key SK and computes $M_2 = (SK \,||\, ID_i) \oplus h(K_2 \,||\, SID_j)$, $CK_2 = h(ID_i \,||\, SID_j \,||\, SK \,||\, K_2 \,||\, T_2)$. Finally, GWN transmits the message {M_2, CK_2, T_2} to the sensor node SN_j via open channel.

Step 4: Upon receiving the message {M_2, CK_2, T_2}, SN_j first checks the validity of the time stamp $\left|T_2^* - T_2\right| < \Delta T$ and computes $(SK \,||\, ID_i) = M_2 \oplus h(K_2 \,||\, SID_j)$, $CK_2^* = h(ID_i \,||\, SID_j \,||\, SK \,||\, K_2 \,||\, T_2)$. Then, the sensor node SN_j compares CK_2* with the received value CK_2. If it is satisfied, SN_j generates a random number T_3 and computes $CK_3 = h(SID_j \,||\, ID_i \,||\, SK \,||\, T_3)$. At last, SN_j updates K_2 with $K_2 = h(K_2)$ and sends the message {CK_3, T_3} to GWN through a public channel.

Step5: GWN first checks the freshness of the time stamp T_3 and computes $CK_3^* = h(SID_j \,||\, ID_j \,||\, SK \,||\, T_3)$. Then, the GWN checks whether CK_3* matches with the received CK_3. If it does not hold, GWN terminates the session. Otherwise, GWN generates two random numbers r_i*, T_4 and computes $HID_i^* = ID_i \oplus r_i^*$, $GU = h(R \,||\, HID_i \,||\, X_i \,||\, K_1)$, $M_3 = E_{GU}(SK \,||\, HID_i^* \,||\, SID_j)$,

$CK_4 = h(ID_i \,||\, SK \,||\, HID_i \,||\, T_4)$. After that, GWN updates K_1, K_2, HID_i with $K_1 = h(K_1)$, $K_2 = h(K_2)$, $HID_i = HID_i^*$, respectively. Finally, GWN sends the message $\{M_3, CK_4, T_4\}$ to U_i through a public channel.

Step 6: Upon receiving the message from GWN, U_i first checks the time stamp T_4. If T_4 is fresh, GWN computes $GU = h(R \,||\, HID_i \,||\, X_i \,||\, K_1)$, $(SK \,||\, HID_i^* \,||\, SID_j) = D_{GU}(M_3)$, $CK_4^* = h(ID_i \,||\, SK \,||\, HID_i \,||\, T_4)$. Then, U_i checks whether CK_4* matches with the received value CK_4. If it holds, U_i updates K_1, HID_i with $K_1 = h(K_1)$, $HID_i = HID_i^*$ and completes the authentication. Otherwise, U_i fails to authenticate GWN.

Password Change Phase

If a health professional U_i wants to change his/her password, he/she needs to run as follows:

Step 1: U_i first inserts his/her smart card into a card reader and inputs the identity ID_i, the password PW_i and imprints its biometrics fg_i via a sensor device. Then, the smart card computes $MB_i = BH\left(m_i \,||\, fg_i\right)$, $MPW_i = h\left(ID_i \,||\, PW_i \,||\, MB_i \,||\, m_i\right)$, $X_i = Y_i \oplus MPW_i$, $V_i^* = h(X_i \,||\, MPW_i)$. U_i compares V_i* with V_i which is stored in the smart card. If they are not equal, the smart card rejects the password change request. Otherwise, the smart card believes the legitimacy of U_i and allows U_i to input a new password PW_i*.

Step 2: The smart card computes $MPW_i^* = h(ID_i \,||\, PW_i^* \,||\, MB_i \,||\, m_i)$, $Y_i^* = X_i \oplus MPW_i^* = Y_i \oplus MPW_i \oplus MPW_i^*$, $V_i^* = h(X_i \,||\, MPW_i^*)$.

Step 3: At last, Y_i* and V_i* are stored in the smart card to replace Y_i and V_i, respectively.

SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section, the authors first analyze the proposed scheme using the widely-accepted BAN logic (Burrows et al., 1989). In addition, the authors conduct a formal verification of the proposed scheme with Proverif (Blanchet, 2001, pp. 82-96). Finally, the authors discuss the possible attacks on the proposed scheme.

Authentication Proof Based on the BAN Logic

The BAN logic (Burrows et al., 1989) is an efficient way to analyze the security of a protocol, which is widely-used in many works, such as (Odelu, Das, & Goswami, 2015; He, Kumar, Lee, & Sherratt, 2014). For convenience, all the notations used in the BAN logic are given in Table 2.

Some primary rules of BAN logic are as given below:

Message-meaning rule: $\dfrac{P \mid\equiv P \overset{K}{\longleftrightarrow} Q, P \lhd X_K}{P \mid\equiv Q \mid\sim X}$

Nonce-verification rule: $\dfrac{P \mid\equiv \#(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$

Jurisdiction rule: $\dfrac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$

Freshness-conjuncatenation rule: $\dfrac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$

Table 2. Notations in BAN logic

Notation	Implication
$P \lhd X$	Principal P sees a statement X
$P \mid\equiv X$	Principal P believes a statement X
$P \mid\Rightarrow X$	Principal P has jurisdiction over statement X
$P \mid\sim X$	Principal P once said a statement X
$\#(X)$	Statement X is fresh
(X,Y)	Statement X or Y is one part of statement (X,Y)
X_K	Statement X is encrypted with the key K
$<X>_Y$	Statement X is combined with statement Y
$(X)_K$	Statement X is hashed with the key K
$P \xleftrightarrow{K} Q$	Principal P and principal Q communicate with the shared key K

The proposed scheme should satisfy following four goals:

Goal 1: $U_i \mid\equiv (U_i \xleftrightarrow{SK} SN_j)$

Goal 2: $U_i \mid\equiv SN_j \mid\equiv (U_i \xleftrightarrow{SK} SN_j)$

Goal 3: $SN_j \mid\equiv (U_i \xleftrightarrow{SK} SN_j)$

Goal 4: $SN_j \mid\equiv U_i \mid\equiv (U_i \xleftrightarrow{SK} SN_j)$

First of all, messages exchanged in the proposed scheme are transformed into idealized forms as follows:

Msg1: $U_i \rightarrow GWN : < ID_i, SID_j, R, HID_i, T_1, U_i \xleftrightarrow{X_i} GWN >_{U_i \xleftrightarrow{K_1} GWN}$

Msg2: $GWN \rightarrow SN_j : < ID_i, SID_j, T_2 >_{GWN \xleftrightarrow{K_2} SN_j}$

Msg3: $SN_j \rightarrow GWN : < ID_i, SID_j, T_3 >_{SN_j \xleftrightarrow{K_2} GWN}$

Msg4: $GWN \rightarrow U_i : < ID_i, SID_j, HID_i, T_4 >_{GWN \xleftrightarrow{K_1} U_i}$

Second, some initial assumptions about the proposed scheme are listed below:

A1: $GWN \mid\equiv \#(T_1)$

A2: $SN_j \mid\equiv \#(T_2)$

A3: $GWN \mid\equiv \#(T_3)$

A4: $U_i \mid\equiv \#(T_4)$

A5: $U_i \mid\equiv U_i \xleftrightarrow{K_1} GWN$

A6: $GWN \mid\equiv U_i \xleftrightarrow{K_1} GWN$

A7: $SN_j \mid\equiv SN_j \xleftrightarrow{K_2} GWN$

A8: $GWN \mid\equiv SN_j \xleftrightarrow{K_2} GWN$

A9: $U_i \mid\equiv SN_j \mid\Rightarrow U_i \overset{SK}{\longleftrightarrow} SN_j$

A10: $SN_j \mid\equiv U_i \mid\Rightarrow U_i \overset{SK}{\longleftrightarrow} SN_j$

Third, based on the BAN logic rules and assumptions, the main proofs are performed as follows. According to the Msg1, the authors get:

S1: $GWN \lhd< ID_i, SID_j, R, HID_i, T_1, U_i \overset{X_i}{\longleftrightarrow} GWN >_{U_i \overset{K_1}{\longleftrightarrow} GWN}$

Based on assumption A6, S1 and message-meaning rule, the authors have:

S2: $GWN \mid\equiv U_i \mid\sim (ID_i, SID_j, R, HID_i, T_1, U_i \overset{X_i}{\longleftrightarrow} GWN)$

From A1 and freshness-conjuncatenation rule, the authors get:

S3: $GWN \mid\equiv \#(ID_i, SID_j, R, HID_i, T_1, U_i \overset{X_i}{\longleftrightarrow} GWN)$

From S3, S2 and nonce-verification rule, the authors get:

S4: $GWN \mid\equiv U_i \mid\equiv (ID_i, SID_j, R, HID_i, T_1, U_i \overset{X_i}{\longleftrightarrow} GWN)$

According to the Msg2, the authors get:

S5: $SN_j \lhd< ID_i, SID_j, T_2 >_{GWN \overset{K_2}{\longleftrightarrow} SN_j}$

From A7, S5 and message-meaning rule, the authors have:

S6: $SN_j \mid\equiv GWN \mid\sim (ID_i, SID_j, T_2)$

From A2 and freshness-conjuncatenation rule, the authors get:

S7: $SN_j \mid\equiv \# < ID_i, SID_j, T_2 >$

From S7, S6 and nonce-verification rule, the authors get:

S8: $SN_j \mid\equiv GWN \mid\equiv < ID_i, SID_j, T_2 >$

According to the Msg3, the authors get:

S9: $GWN \lhd< ID_i, SID_j, T_3 >_{SN_j \overset{K_2}{\longleftrightarrow} GWN}$

From A8, S9 and message-meaning rule, the authors have:

S10: $GWN \mid\equiv SN_j \mid\sim (ID_i, SID_j, T_3)$

From A3 and freshness-conjuncatenation rule, the authors get:

S11: $GWN \mid\equiv \#(ID_i, SID_j, T_3)$

From S11, S10 and nonce-verification rule, the authors get:

S12: $GWN \mid\equiv SN_j \mid\equiv (ID_i, SID_j, T_3)$

According to the Msg4, the authors get:

S13: $U_i \lhd\!< ID_i, SID_j, HID_i, T_4 >_{GWN \xleftarrow{K_1} U_i}$

From A5, S13 and message-meaning rule, the authors have:

S14: $U_i \mid\equiv GWN \mid\sim\!< ID_i, SID_j, HID_i, T_4 >$

From A4 and freshness-conjuncatenation rule, the authors get:

S15: $U_i \mid\equiv \#(ID_i, SID_j, HID_i, T_4)$

From S15, S14 and nonce-verification rule, the authors get:

S16: $U_i \mid\equiv GWN \mid\equiv (ID_i, SID_j, HID_i, T_4)$

From S12, S16 and the session key *SK*, the authors have:

S17: $U_i \mid\equiv SN_j \mid\equiv (U_i \xleftrightarrow{SK} SN_j)$ (Goal2)

From S4, S8 and the session key *SK*, the authors have:

S18: $SN_j \mid\equiv U_i \mid\equiv (U_i \xleftrightarrow{SK} SN_j)$ (Goal4)

From S17, A9 and jurisdiction rule, the authors have:

S19: $U_i \mid\equiv (U_i \xleftrightarrow{SK} SN_j)$ (Goal1)

From S18, A10 and jurisdiction rule, the authors have:

S20: $SN_j \mid\equiv (U_i \xleftrightarrow{SK} SN_j)$ (Goal3)

According to Goal1-Goal4, the authors conclude that the proposed scheme can achieve mutual authentication successfully.

Formal Security Verification Using ProVerif

ProVerif (Blanchet, 2001, pp. 82-96) is a formal verification tool which is widely used in many works, such as (Xiong, Peng, Peng, Liang, & Liu, 2017; Jiang, Zeadally, Ma, & He, 2017). Privacy and security of authentication schemes can be verified by ProVerif which supports many cryptographic primitives, including digital signatures, hash functions, encryption, Diffie-Hellman key agreements, and so on. In this subsection, the authors use ProVerif to analyze the security of the proposed scheme.

First of all, the authors define two public channels and basic types of variables. Secondly, the authors model the cryptographic functions of the proposed scheme, and the secret keys, events and authentication queries are defined. Thirdly, the authors model the process of the health professional, GWN and the medical sensor node, respectively. Finally, the authors model the whole process of the proposed scheme. The execution codes of the proposed scheme are placed on GitHub (Shuai, 2018), and the simulation results with ProVerif version 1.96 are given in Figure 3.

The results demonstrate that the proposed scheme fulfills the secrecy of session key and achieves mutual authentication successfully.

Figure 3. The simulation results with the ProVerif

```
Completing...
Starting query not attacker(snameA[])
RESULT not attacker(snameA[]) is true.
Starting query not attacker(snameB[])
RESULT not attacker(snameB[]) is true.
Starting query not attacker(snameC[])
RESULT not attacker(snameC[]) is true.
Starting query not attacker(snameD[])
RESULT not attacker(snameD[]) is true.
-- Query inj-event(SGend(x_2072)) ==> inj-event(SGbegin(x_2072))
Completing...
Starting query inj-event(SGend(x_2072)) ==> inj-event(SGbegin(x_2072))
RESULT inj-event(SGend(x_2072)) ==> inj-event(SGbegin(x_2072)) is true.
-- Query inj-event(GSend(x_4178)) ==> inj-event(GSbegin(x_4178))
Completing...
Starting query inj-event(GSend(x_4178)) ==> inj-event(GSbegin(x_4178))
RESULT inj-event(GSend(x_4178)) ==> inj-event(GSbegin(x_4178)) is true.
-- Query inj-event(GHend(x_6181)) ==> inj-event(GHbegin(x_6181))
Completing...
Starting query inj-event(GHend(x_6181)) ==> inj-event(GHbegin(x_6181))
RESULT inj-event(GHend(x_6181)) ==> inj-event(GHbegin(x_6181)) is true.
-- Query inj-event(HGend(x_8172)) ==> inj-event(HGbegin(x_8172))
Completing...
Starting query inj-event(HGend(x_8172)) ==> inj-event(HGbegin(x_8172))
RESULT inj-event(HGend(x_8172)) ==> inj-event(HGbegin(x_8172)) is true.
```

Analysis of Security Properties

In this section, the authors look at how the proposed scheme provides user anonymity, forward secrecy, mutual authentication, session key agreement, security against smart card loss attack and replay attack.

The Proposed Scheme Provides User Anonymity

In the proposed scheme, the authors adopt pseudonym identity technique to protect health professional's real identity. The pseudonym identity generated randomly by GWN is updated during every session, so the transmitted messages in current session are also different from other session. In addition, the health professional's real identity is protected by one-time hash function, the adversary cannot get it even if he/she intercept the transmitted messages. Therefore, the proposed scheme can not only protect the health professional's real identity, but also provide untraceability.

The Proposed Scheme Provides Forward Secrecy

In the proposed scheme, even if an attacker obtains the long-term keys K_1, K_2 and X_i, he/she cannot get the session key which was used in previous communications. The reason is that the long-term keys K_1* and K_2* are updated by K_1=$h(K_1$*$)$ and K_2=$h(K_2$*$)$ after each session. The attacker cannot get K_1* and K_2* from K_1 and K_2 because hash function is irreversible. Therefore, the proposed scheme provides forward secrecy.

The Proposed Scheme Achieves Mutual Authentication

In the proposed scheme, mutual authentication between health professional and GWN will be achieved by checking CK_1*=CK_1 and CK_4*=CK_4. Similarly, mutual authentication between GWN and the medical sensor node will be achieved by checking CK_2*=CK_2 and CK_3*=CK_3. Therefore, the proposed scheme achieves mutual authentication successfully.

The Proposed Scheme Provides Session Key Agreement

In the execution of the proposed scheme, health professional, GWN and the medical sensor node establish a shared session key SK to protect future communications in WMSNs. Therefore, the proposed scheme provides session key agreement.

The Proposed Scheme is Resistant to Smart Card Loss Attack

Suppose the smart card is lost/stolen, an attacker can get the stored secret values $\{HID_i, Y_i, V_i, K_1, m_i, h(.), BH(.)\}$, where $V_i = h\left(X_i \,||\, MPW_i\right)$, $X_i = h\left(ID_i \,||\, K \,||\, n_i\right)$, $Y_i = X_i \oplus MPW_i$, $HID_i = ID_i \oplus r_i$, $MB_i = BH\left(m_i \,||\, fg_i\right)$, $MPW_i = h\left(ID_i \,||\, PW_i \,||\, MB_i \,||\, m_i\right)$, $MB_i = BH\left(m_i \,||\, fg_i\right)$. Here, the authors also suppose that the transmitted messages via open channels can be eavesdropped by the attacker. Using these values, the attacker can launch a smart card loss attack and try to guess the health professional's real identity and password. However, the attack will be failed without knowing the health professional's personal biometric fg_i, GWN's secret key K and the high entropy random integer n_i generated by GWN. Therefore, the proposed scheme is resistant to smart card loss attack.

The Proposed Scheme Resists Replay Attack

The proposed scheme adopts the time stamp to avoid the replay attack. In the replay attack, an adversary cannot pass the time stamp checking process because all transmitted messages including current time stamp values, i.e., T_1, T_2, T_3, T_4. Therefore, the proposed scheme resists replay attack.

The Proposed Scheme Resists Wrong Password Login Attack

In the proposed scheme, the value V_i stored in the smart card is used to verify the legality of health professional, where $V_i^* = h\left(X_i^* \,||\, MPW_i^*\right)$, $X_i^* = Y_i \oplus MPW_i^*$, $MPW_i^* = h\left(ID_i \,||\, PW_i \,||\, MB_i^* \,||\, m_i\right)$, $MB_i^* = BH\left(m_i \,||\, fg_i\right)$. If the health professional inputs a wrong password PW_i*, the values V_i* and V_i will be not equal. At this moment, the smart card rejects the health professional's login request. Therefore, the proposed scheme resists wrong password login attack.

PERFORMANCE ANALYSIS

In this section, the authors compare the computational costs of the proposed scheme with other related schemes (He et al., 2015; Li et al., 2016; Srinivas et al., 2017). In order to evaluate the computational costs, the authors define two computational notations T_h and T_{cr}, where T_h denotes the time complexity of a one-way hash function operation, and T_{cr} denotes the time complexity of general symmetric-key encryption/decryption operation. According to the existing experimental results (He, Kumar, Lee, & Sherratt, 2014), the execution time of a one-way hash function operation and general symmetric-key encryption/decryption operation are 0.00032s and 0.0056s, respectively. The simulations are achieved on a machine characterized by a processing rate of 3.2 GHz and a memory of 4 GB, the results are averaged over 300 randomised simulation runs. The comparison results between the proposed scheme and other related schemes are shown in Table 3.

In WMSNs, medical sensor nodes are limited in terms of computation capabilities and thus, the user authentication scheme must be lightweight in terms of computation. The proposed scheme only uses the lightweight cryptographic primitives including one-way hash function and symmetric encryption/decryption algorithm, which are efficient. Although the proposed scheme increases the number of hash operations slightly, it reduces the number of symmetric encryption/decryption operations substantially. Comparison demonstrates that the proposed scheme performs better than He et al.'s scheme (He et al., 2015), Li et al.'s scheme (Li et al., 2016) and Srinivas et al.'s scheme (Srinivas et al., 2017). It is valuable to note that the proposed scheme achieves the required security attributes and is more suitable for personalized healthcare applications.

CONCLUSION

With the wide use of WMSNs in healthcare applications, security and privacy issues have become a great challenge. In order to securely transmit physiological data collected from patients, the authors propose a novel and lightweight three-factor anonymous authentication scheme with privacy protection for personalized healthcare applications using only the lightweight cryptographic primitives. Using

Table 3. Performance comparison between the proposed scheme and other related schemes

Scheme	He et al.'s scheme (He et al., 2015)	Li et al.'s scheme (Li et al., 2016)	Srinivas et al.'s scheme (Srinivas et al., 2017)	The proposed scheme
Users	$4T_h+3T_{cr}$	$7T_h+2T_{cr}$	$8T_h+3T_{cr}$	$8T_h+2T_{cr}$
GWN	$2T_h+5T_{cr}$	$7T_h+6T_{cr}$	$4T_h+2T_{cr}$	$10T_h+2T_{cr}$
Sensor node	$1T_h+2T_{cr}$	$5T_h+2T_{cr}$	$5T_h+2T_{cr}$	$4T_h$
Total cost	$7T_h+10T_{cr}$	$19T_h+10T_{cr}$	$17T_h+7T_{cr}$	$22T_h+4T_{cr}$
Execution time	0.05824s	0.06208s	0.04464s	0.02944s

the BAN logic, the authors have proved that the proposed scheme fulfills mutual authentication successfully. In addition, the authors evaluated the security of the proposed scheme with ProVerif, and the simulation results show that the proposed scheme is secure. Through the heuristic way, the authors prove that the proposed scheme can not only provide user anonymity and forward secrecy, but also resist various malicious attacks, such as smart card loss attack and replay attack. Finally, the authors evaluate the performance of the proposed scheme with other related schemes, and the results show that the proposed scheme reduces the computational cost substantially and is more suitable for personalized healthcare applications.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (NSFC) under the grant No. U1536110.

REFERENCES

Ameen, M. A., Liu, J. W., & Kwak, K. S. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems*, *36*(1), 93–101. doi:10.1007/s10916-010-9449-4 PMID:20703745

Blanchet, B. (2001). An efficient cryptographic protocol verifier based on prolog rules. *IEEE Computer Security Foundations Workshop*, *1*, 82-96. doi:10.1109/CSFW.2001.930138

Burrows, M., Abad, M., & Needham, R. M. (1989). A logic of authentication. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, 426*(1871), 233-271. doi:10.1145/74850.74852

Cheng, J. R., Xu, R. M., Tang, X. Y., Sheng, V. S., & Cai, C. T. (2018). An abnormal network flow feature sequence prediction approach for DDoS attacks detection in big data environment. *Computers Materials & Continua*, *55*(1), 95–119.

Cui, J. H., Zhang, Y. Y., Cai, Z. P., Liu, A. F., & Li, Y. Y. (2018). Securing display path for security-sensitive applications on mobile devices. *Computers Materials & Continua*, *55*(1), 17–35.

Das, M. L. (2009). Two-factor user authentication in wireless sensor networks. *IEEE Transactions on Wireless Communications*, *8*(3), 1086–1090. doi:10.1109/TWC.2008.080128

Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, *29*(2), 198–208. doi:10.1109/TIT.1983.1056650

Gill, S. S., Chana, I., & Buyya, R. (2017). IoT based agriculture as a cloud and big data service: The beginning of digital India. *Journal of Organizational and End User Computing*, *29*(4), 1–23. doi:10.4018/JOEUC.2017100101

Gong, W. W., Qi, L. Y., & Xu, Y. W. (2018). Privacy-aware multi-dimensional mobile service quality prediction and recommendation in distributed fog environment. *Wireless Communications and Mobile Computing*, *4*, 1–8.

Gope, P., & Hwang, T. (2016). A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. *IEEE Transactions on Industrial Electronics*, *63*(11), 7124–7132. doi:10.1109/TIE.2016.2585081

He, D. B., Kumar, N., Chen, J. H., Lee, C. C., Chilamkurti, N., & Yeo, S. S. (2015). Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. *Multimedia Systems*, *21*(1), 49–60. doi:10.1007/s00530-013-0346-9

He, D. B., Kumar, N., Lee, J. H., & Sherratt, R. S. (2014). Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE Transactions on Consumer Electronics*, *60*(1), 30–37. doi:10.1109/TCE.2014.6780922

Hu, F., Jiang, M., Wagner, M., & Dong, D. C. (2007). Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/software codesign. *IEEE Transactions on Information Technology in Biomedicine*, *11*(6), 619–627. doi:10.1109/TITB.2007.894818 PMID:18046937

Huang, Y. M., Hsieh, M. Y., Chao, H. C., Hung, S. H., & Park, J. H. (2009). Pervasive, secure access to a hierarchical sensor-based healthcare monitoring architecture in wireless heterogeneous networks. *IEEE Journal on Selected Areas in Communications*, *27*(4), 400–411. doi:10.1109/JSAC.2009.090505

Jiang, Q., Zeadally, S., Ma, J. F., & He, D. B. (2017). Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access: Practical Innovations, Open Solutions*, *5*, 3376–3392. doi:10.1109/ACCESS.2017.2673239

Jin, C. H., Xu, C. X., Zhao, X. J., & Zhao, J. N. (2015). A secure RFID mutual authentication protocol for healthcare environments using Elliptic Curve Cryptography. *Journal of Medical Systems*, *39*(3), 24. doi:10.1007/s10916-015-0213-7 PMID:25666925

Khan, K., & Kumari, S. (2013). An authentication scheme for secure access to healthcare services. *Journal of Medical Systems*, *37*(4), 9954. doi:10.1007/s10916-013-9954-3 PMID:23828650

Khan, M. K., & Alghathbar, K. (2010). Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks. *Sensors (Basel)*, *10*(3), 2450–2459. doi:10.3390/s100302450 PMID:22294935

Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. *Advances in Cryptology-CRYPTO'99, 1666*, 388-397.

Kumar, P., Lee, S. G., & Lee, H. J. (2012). E-SAP: Efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. *Sensors (Basel)*, *12*(2), 1625–1647. doi:10.3390/s120201625 PMID:22438729

Lee, T., Ghapanchi, A. H., Talaei-Khoei, A., & Ray, P. (2015). Strategic information system planning in healthcare organizations. *Journal of Organizational and End User Computing*, *27*(2), 1–31. doi:10.4018/joeuc.2015040101

Li, X., Niu, J. W., Kumari, S., Liao, J. G., Liang, W., & Khan, K. (2016). A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity. *Security and Communication Networks*, *9*(15), 2643–2655. doi:10.1002/sec.1214

Liu, W. Y., Luo, X. Y., Liu, Y. M., Liu, J. Q., Liu, M. H., & Shi, Y. Q. (2018). Localization algorithm of indoor Wi-Fi access points based on signal strength relative relationship and region division. *Computers Materials & Continua*, *55*(1), 71–93.

Ma, Y. Y., Luo, X. Y., Li, X. L., Bao, Z. K., & Zhang, Y. (2018). Selection of rich model steganalysis features based on decision rough set α-positive region reduction. *IEEE Transactions on Circuits and Systems for Video Technology*, *99*, 1–1.

Malasri, K., & Wang, L. (2009). Design and implementation of a securewireless mote-based medical sensor network. *Sensors (Basel)*, *9*(8), 6273–6297. doi:10.3390/s90806273 PMID:22454585

Mir, O., Munilla, J., & Kumari, S. (2017). Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks. *Peer-to-Peer Networking and Applications*, *10*(1), 79–91. doi:10.1007/s12083-015-0408-1

Odelu, V., Das, A. K., & Goswami, A. (2015). A secure biometrics-based multi-server authentication protocol using smart cards. *IEEE Transactions on Information Forensics and Security*, *10*(93), 1953–1966. doi:10.1109/TIFS.2015.2439964

Qi, L. Y., Meng, S. M., Zhang, X. Y., Wang, R. L., Xu, X. L., Zhou, Z. L., & Dou, W. C. (2018a). An exception handling approach for privacy-preserving service recommendation failure in a cloud environment. *Sensors (Basel)*, *18*(7), 2037. doi:10.3390/s18072037 PMID:29949893

Qi, L. Y., Yu, J. G., & Zhou, Z. L. (2017). An invocation cost optimization method for web services in cloud environment. *Scientific Programming*, *11*, 1–9. doi:10.1155/2017/4358536

Qi, L. Y., Zhang, X. Y., Dou, W. C., Hu, C. H., Yang, C., & Chen, J. J. (2018b). A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment. *Future Generation Computer Systems*, *88*, 636–643. doi:10.1016/j.future.2018.02.050

Qi, L. Y., Zhang, X. Y., Dou, W. C., & Ni, Q. (2017). A distributed locality-sensitive hashing based approach for cloud service recommendation from multi-source data. *IEEE Journal on Selected Areas in Communications*, *35*(11), 2616–2624. doi:10.1109/JSAC.2017.2760458

Qi, L. Y., Zhou, Z. L., Yu, J. G., & Liu, Q. (2017). Data-sparsity tolerant web service recommendation approach based on improved collaborative filtering. *IEICE Transactions on Information and Systems*, *100*(9), 2092–2099. doi:10.1587/transinf.2016EDP7490

Shuai, M. X. (2018, July 9). *The execution code of a lightweight three-factor anonymous authentication scheme with privacy protection for personalized healthcare applications.* Retrieved from https://github.com/smx12345/code/blob/master/wmsns.pv

Siddesh, G. M., Srinivasa, K. G., Kaushik, S., Varun, S. V., Subramanyam, V., & Patil, V. M. (2017). Internet of things (IOT) solution for increasing the quality of life of physically challenged people. *Journal of Organizational and End User Computing*, *29*(4), 72–83. doi:10.4018/JOEUC.2017100104

Srinivas, J., Mishra, D., & Mukhopadhyay, S. (2017). A mutual authentication framework for wireless medical sensor networks. *Journal of Medical Systems*, *41*(5), 80. doi:10.1007/s10916-017-0720-9 PMID:28364358

Walczak, S., & Mann, R. (2010). Utilization and perceived benefit for diverse users of communities of practice in a healthcare organization. *Journal of Organizational and End User Computing*, *22*(4), 24–50. doi:10.4018/joeuc.2010100102

Wang, D., & Wang, P. (2014). On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions. *Computer Networks*, *73*, 41–57. doi:10.1016/j.comnet.2014.07.010

Wang, J. W., Li, T., Shi, Y. Q., Lian, S. G., & Ye, J. Y. (2016). Forensics feature analysis in quaternion wavelet domain for distinguishing photographic images and computer graphics. *Multimedia Tools and Applications*, *76*(22), 1–17.

Wu, F., Xu, L. L., Kumari, S., & Li, X. (2017). An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks. *Multimedia Systems*, *23*(2), 195–205. doi:10.1007/s00530-015-0476-3

Xiong, L., Peng, D. Y., Peng, T., Liang, H. B., & Liu, Z. C. (2017). A lightweight anonymous authentication protocol with perfect forward secrecy for wireless sensor networks. *Sensors (Basel)*, *11*(11), 2681. doi:10.3390/s17112681 PMID:29160861

Xu, Y. W., Qi, L. Y., Dou, W. C., & Yu, J. G. (2017). Privacy-preserving and scalable service recommendation based on simHash in a distributed cloud environment. *Complexity*, *2*, 1–9. doi:10.1155/2017/3437854

Zhang, Y., Qin, C., Zhang, W. M., Liu, F. L., & Luo, X. Y. (2018). On the fault-tolerant performance for a class of robust image steganography. *Signal Processing*, *146*, 99–111. doi:10.1016/j.sigpro.2018.01.011

Mengxia Shuai received the B.S. and M.S. degrees from Fuzhou University, Fuzhou, China. Currently, he is pursuing the Ph.D. degree at University of Science and Technology of China. His research interests include cryptography and information security.

Nenghai Yu received his B.S. degree in 1987 from Nanjing University of Posts and Telecommunications, M.E. degree in 1992 from Tsinghua University and Ph.D. degree in 2004 from University of Science and Technology of China, where he is currently a professor. His research interests include multimedia security, multimedia information retrieval, video processing, information hiding and security, privacy, and reliability in cloud computing.

Hongxia Wang received the B.S. degree from Hebei Normal University, Shijiazhuang, China, in 1996, and the M.S. and Ph.D. degrees from University of Electronic Science and Technology of China, Chengdu, China, in 1999 and 2002, respectively. She pursued post-doctoral research with Shanghai Jiao Tong University, Shanghai, China, from 2002 to 2004 and was a Visiting Scholar with Northern Kentucky University, Highland Heights, KY, USA, from 2013 to 2014. She is currently a Professor with the School of Information Science and Technology, Southwest Jiaotong University, Chengdu. She has authored over 100 research papers in refereed journals and conferences, and holds 10 authorized patents. Her research interests include multimedia information security, digital forensics, information hiding, and digital watermarking.

Ling Xiong received the M.S. degree from Southwest Jiaotong University, Chengdu, China. She is currently pursuing the Ph.D. degree in the school of information science and technology of Southwest Jiaotong University. Her research interests include the formal analysis of cryptographic protocol, the security and privacy in cloud computing services environment and wireless sensor networks environment.

Yue Li received the B.S. degree from Southwest Jiaotong University, Chengdu, China. Now she is pursuing the Ph.D. degree in the school of information science and technology of Southwest Jiaotong University. Her research interests include multimedia information security, information hiding, and digital watermarking.