A Secure User Authentication Scheme with Biometrics for IoT Medical Environments

YoHan Park
Division of IT Convergence
Korea Nazarene University
Korea, Republic

***Abstract*—Internet of Things (IoT) is a ubiquitous network that devices are interconnected and users can access those devices through the Internet. Recently, medical healthcare systems are combined with these IoT networks and provide efficient and effective medical services to medical staff and patients. However, the security threats are increased simultaneously as the requirements of medical services in IoT medical environments are increased. It is essential to provide security of the networks from malicious attacks.**

In 2018, Roy et al. proposed a remote user authentication and key agreement scheme with biometrics in IoT medical environments. Unfortunately, we analyze Roy et al.'s scheme and demonstrate that their scheme does not withstand various attacks, such as replay attacks and password guessing attacks. Then we propose a user authentication scheme to overcome these security drawbacks. The proposed scheme withstands various attacks from adversaries in IoT medical environments and provide better security functionalities of those of Roy et al. We then prove the authentication and session key of the proposed scheme using *BAN* logic and analyze that our proposed scheme is secure against various attacks.

Keywords*—*IoT medical environments; Cryptanalysis; User authentication; BAN logic

I. Introduction

With the rapid development of mobile devices and wireless networks, users can access various services conveniently at any time and anywhere [1], [2]. These changes affect the healthcare environment, enabling medical devices to communicate with each other and communicate that information to the users. Those devices are also interconnected with medical servers and medical staff [3]. The changes that those developments have brought on to the daily lives of human beings are enormous. The spread of IoT medical technology enables people to utilize advanced medical services such as e-healthcare [4], [5]. The telecare medical information system (TMIS) is one of the advanced information medical system [6], [7]. Medical staff can treat patients and diagnose a case of them in the distance with the aid of medical devices and store the information of patients to a medical server. Remote monitoring can be possible efficiently with IoT connected medical devices. Sensors attached to patients can capture health data and share it through wireless connection with medical staff. The IoT technology in medical environments makes the healthcare system easy to be managed and gives a lot of possibilities of medical services.

However, the IoT environment has an enormous threat to security and privacy due to its heterogeneous and dynamic nature [8]. To make the IoT-based medical system widely accepted, security problems should be resolved in advance. Especially, user authentication is an essential prerequisite among all the security concerns to provide integrity, access control, and availability for IoT environments [9]–[11]. Without secure authentication methods, the external party can directly access user's information which are more valuable and even critical than general information. Hence, it is necessary to provide an authentication process between a user and service providers before permitting a user to access the services.

There are many authentication schemes to provide security of users medical information. To provide user security against inside attackers, Chen *et al*. proposed a dynamic ID-based authentication scheme for TMIS [12]. However, [12] was vulnerable to guessing attacks and tracking attacks. Jiang *et al*. [3] demonstrated that and [12]' scheme leaked out personal information. Then Jiang *et al*. proposed an authentication scheme which can withstand anonymity and untraceability of users. But There scheme was attacked by Kumari *et al*. [6]. They said [3] was vulnerable to password guessing attack, user impersonation attack, and so on. [7] also showed the security flawless of [3]. Many authentication schemes try to provide patients to utilize medical services securely.

Roy et al. [13] proposed a three factor remote user authentication scheme in IoT medical environments. They insisted that their scheme is resist to various attacks. Unfortunately, this paper demonstrates Roy et al.'s scheme fails to provide security against a number of attacks, such as replay attacks and offline password guessing attacks. And we show that their scheme does not provide perfect forward secrecy. Subsequently, we propose a secure three factor remote user authentication scheme to solve these security vulnerabilities.

A. Threat model

The Dolev-Yao threat (DY) model [14] is widely used in evaluating the security of a protocol [15]. Under the DY model, we assume that the capabilities of adversaries $\mathcal{A}$ are as follows.

- $\mathcal{A}$ has total controlled over the communication channel connecting the users and the remote server in login/authentication phase. Thus the adversary can intercept, insert, delete, or modify any message transmitted via a public channel.
- $\mathcal{A}$ can have a lost or stolen smart card, and extract the information stored in a smart card by means of analyzing the power consumption of the smart card [16], [17].
- $\mathcal{A}$ can perform various attacks including offline password guessing attack, replay attack, and man-in-the-middle

attack. Especially, $\mathcal{A}$ can guess identity and password simultaneously [18].

B. Contributions

The contributions made in the paper are listed below:

1) We analyze security weaknesses of Roy et al.'s scheme [13] and demonstrate that it is vulnerable to replay attack, offline password guessing attack. In addition, we show that their scheme does not provide perfect forward secrecy.
2) To overcome these security weaknesses, we propose an enhanced secure authentication scheme in IoT medical network. The proposed scheme prevents various attacks such as password guessing attack, user impersonation attack and replay attack from malicious adversaries.
3) Our scheme provides secure mutual authentication and perfect forward secrecy, and we prove the secure mutual authentication of our scheme using the BAN logic.

C. Paper Structure

The rest of the paper is organized as follows. In Section 2, we review Roy et al.'s scheme followed by the cryptanalysis of Roy et al.'s scheme in Secion 3. In Section 4, we propose a secure remote user authentication scheme in IoT medical networks to withstand the security pitfalls found in the authentication scheme of Roy et al.'s scheme, and then security and efficiency of the proposed scheme are analyzed with related existing schemes in Section 5. Finally, Section 6 concludes the paper.

II. Review of Roy et al.'s scheme

In this section, we review Roy et al.'s remote user authentication scheme. It is composed of four phases: registration, login, authentication and key establishment, and password change. Table I describe the notations used throughout the paper.

TABLE I. Notations

Notation	Meaning
U_i	user i
ID_i	identity of U_i
PW_i	password of U_i
B_i	biometric template of U_i
SC_i	smart card of user U_i
S_j	medical server j
$Gen(\cdot)$	Generation function
$Rep(\cdot)$	Reproduction function
$E_k(\cdot)/D_k(\cdot)$	encryption/decryption using key k
X_S	master secret key of S_j
TS_i	timestamp
$\|\|$	concatenate operation
$\bigoplus$	XOR operation
$h(\cdot)$	hash function

A. Registration phase

If a new user U_i wants to access the medical service, U_i must register with the remote server S_j first. The Roy et al.'s user registration phase is illustrated in Figure 1, and the detailed steps of this registration phase are as follows:

1) U_i chooses ID_i and PW_i, and imprints a biometric template B_i. U_i generates parameters $< \alpha_i, \beta_i > \leftarrow Gen(B_i)$.
2) U_i generates a random number θ_i and compute $TID_i = h(h(ID_i) \oplus h(\theta_i))$ and $RPB_i = h(ID_i||\alpha_i||h(PW_i))$. Then U_i sends TID_i to S_j via a secure channel.
3) S_j computes $\delta_i = h(h(TID_i)||h(X_S))$. S_j sends a smart card SC_i and δ_i to U_i via a secure channel.
4) U_i computes the parameters Y_1, Y_2 and Y_3 as follows:

$$\begin{aligned} Y_1 &= h(\delta_i) \oplus h(RPB_i||\theta_i) \\ Y_2 &= h(h(ID_i)||PW_i) \oplus \theta_i \\ Y_3 &= h(\alpha_i||PW_i||\theta_i) \end{aligned}$$

5) Finally, U_i store the parameters $< Y_1, Y_2, Y_3, h(\cdot), \beta_i >$ in a smart card SC_i.

B. Login phase

When the authenticated user U_i wants to use a medical service, U_i sends request messages of accessing the medical service to the remote server S_j. Roy et al.'s scheme also supposed that U_i and S_j must authenticate each other before sending the request message. The Roy et al.'s login phase is illustrated as follows:

1) U_i chooses ID_i and PW_i, and imprints biometrics B_i'. Then SC_i generates α_i, and computes θ_i' and Y_3', and then compares Y_3' with Y_3 to check a user credential as follow:

$$\begin{aligned} \alpha_i &\leftarrow Rep(B_i', \beta_i) \\ \theta_i' &= Y_2 \oplus h(h(ID_i)||PW_i) \\ Y_3' &= h(\alpha_i||PW_i||\theta_i') \\ \text{verifies } Y_3' &\stackrel{?}{=} Y_3 \end{aligned}$$

2) SC_i generates two random number RN_i and θ_i^* and computes $RPB_i, \mu_i (= h(\delta_i)), TID_i, D_1$ and H_1 as follows:

$$\begin{aligned} RPB_i &= h(ID_i||\alpha_i||h(PW_i)) \\ \mu_i &= Y_1 \oplus h(RPB_i||\theta_i) \\ TID_i &= h(h(ID_i) \oplus h(\theta_i)) \\ D_1 &= E_{\mu_i}(ID_i||\theta_i||\theta_i^*||TS_i||RN_i) \\ H_1 &= h(h(ID_i \oplus \theta_i)||\theta_i^*||TID_i||TS_i||RN_i) \end{aligned}$$

Then, U_i sends a request message $Msg_1 =< TID_i, D_1, H_1 >$ to S_j via a public channel.

C. Authentication and key establishment phase

U_i and S_j authenticate and generate a session key. Figure 2 illustrates the authentication and key establishment phase, which performs as follows:

1) S_j computes δ_i, μ_i', and decrypts D_1 and obtain $(ID_i, \theta_i, \theta_i^*, TS_i, RN_i)$ as follow:

$$\begin{aligned} \delta_i &= h(h(TID_i)||h(X_S) \\ \mu_i &= h(\delta_i) \\ D_{\mu_i}(D_1) &= \{ID_i||\theta_i||\theta_i^*||TS_i||RN_i\} \end{aligned}$$

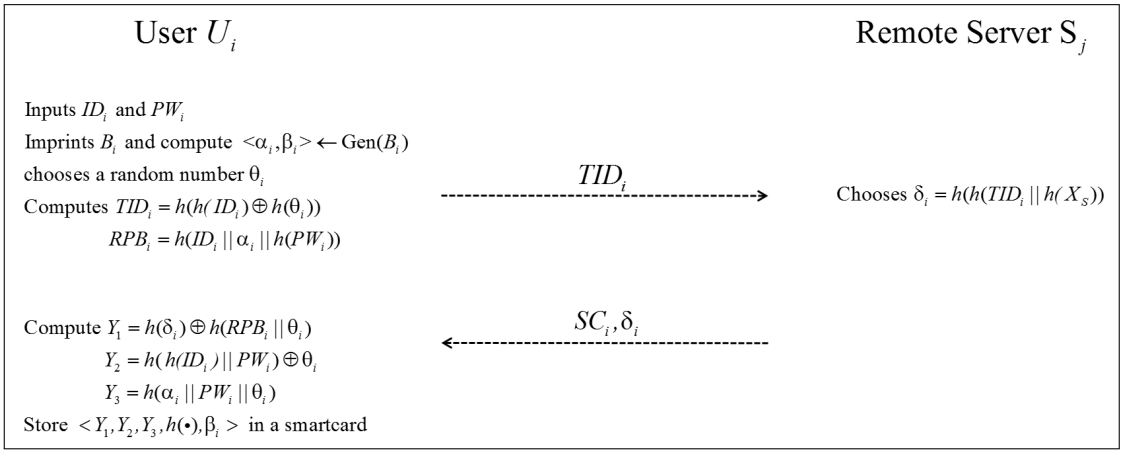

Fig. 1. User registration phase of Roy et al.'s scheme

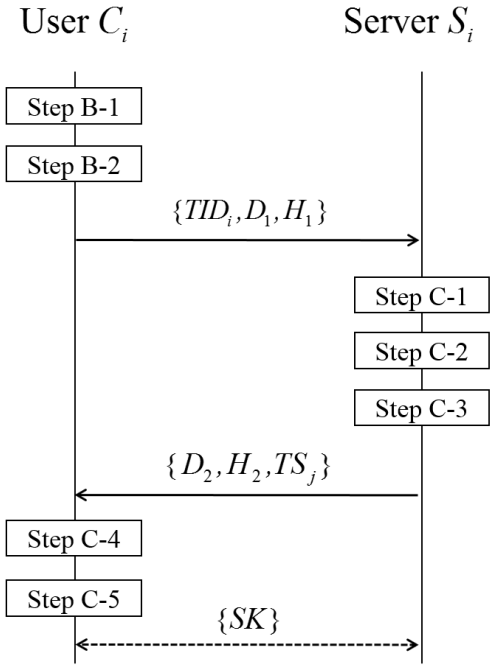

Fig. 2. Authentication and key establishment of Roy et al.'s scheme

2) S_j retrieves TS_i^* and checks $TS_i^* - TS_1 \leq \Delta T$. If it is true, S_j checks the validity of H_1 and TID_i using the decrypted parameters of D_1 as follows:

$$\begin{aligned} H_1 &\stackrel{?}{=} h(h(ID_i) \oplus \theta_i)||\theta_i^*||TID_i||TS_i||RN_i) \\ TID_i &\stackrel{?}{=} h(h(ID_i) \oplus h(\theta_i)) \end{aligned}$$

If both verifications are successful, proceed to the next step.

3) S_j computes $TID_i, \delta_i^1, \lambda_i, D_2, SK_{S_j,U_i}$ and H_2 as follows:

$$\begin{aligned} TID_i^1 &= h(h(ID_i) \oplus h(\theta_i) \oplus h(\theta_i^*)) \\ \delta_i^1 &= h(h(TID_i^1)||h(X_S)) \\ \lambda_i &= h(TID_i^1) \\ D_2 &= E_{\lambda_i}(\delta_i^1||\theta||RN_j) \\ SK_{S_j,U_i} &= h(\delta_i^1||\theta_i^*||RN_i||RN_j||TS_i||TS_j) \\ H_2 &= h(TID_i^1||\delta_i^1||SK_{S_j,U_i}||TS_j||RN_j) \\ & \text{(where, } TS_j \text{ is the time stamp.)} \end{aligned}$$

Then, S_j sends the replay message $Msg_2 =< D_2, H_2, TS_j >$ to U_i via a public channel.

4) U_i retrieves TS_j^* and checks $TS_j^* - TS_j \leq \Delta T$. If it is true, U_i computes TID_i^1, δ_i and decrypts D_2 as follows:

$$\begin{aligned} TID_i^1 &= h(h(ID_i) \oplus h(\theta_i) \oplus h(\theta_i^*)) \\ \lambda_i &= h(TID_i^1) \\ D_{\lambda_i}(D_2) &= \{\delta_i^1||\theta_i||RN_j\} \end{aligned}$$

5) Finally, U_i generates a session key $SK_{U_i,S_j} = h(\delta_i^1||\theta_i^*||RN_i||RN_j||TS_i||TS_j)$. Then U_i checks the validity of H_2 by comparing it with the computed value $h(TID_i^1||\delta_i^1||SK_{U_i,S_j}||TS_j||RN_j)$. If it is true, U_i accepts SK_{U_i,S_j} as the current session key, then updates new parameters Y_1^*, Y_2^* and Y_3^* as follows:

$$\begin{aligned} Y_1^* &= h(\delta_i) \oplus h(RPB_i||\theta_i^*) \\ Y_2^* &= h(h(ID_i)||PW_i) \oplus \theta_i^* \\ Y_3^* &= h(\alpha_i||PW_i||\theta_i^*) \end{aligned}$$

D. Password change phase

To provide a password change requirement, U_i performs following steps.

1) U_i inserts SC_i and inputs ID_i, PW_i and B_i.
2) SC_i computes θ_i from Y_2 and Y_3 using θ_i as given in step 2 of login phase.
3) If it is correct, U_i input a new password PW_i^{new} and compute new parameters Y_1^{new}, Y_2^{new} and Y_3^{new} as follows:

$$
\begin{aligned}
RPB_i^{new} &= h(ID_i||\alpha_i||h(PW_i^{new})) \\
Y_1^* &= Y_1 \oplus h(RPB_i||\theta_i) \oplus h(RPB_i^{new}||\theta_i) \\
Y_2^* &= h(h(ID_i)||PW_i^{new}) \oplus \theta_i \\
Y_3^* &= h(\alpha_i||PW_i^{new}||\theta_i)
\end{aligned}
$$

III. Cryptanalysis of Roy et al.'s Scheme

In this section, we demonstrate that Roy et al.'s scheme cannot prevent replay attacks and offline password guessing attacks. We also show that their scheme cannot provide perfect forward secrecy, and an adversary can trace users freely. We assumed that an adversary $\mathcal{A}$ could steal or obtain the user's smart card SC_i. In addition, an adversary $\mathcal{A}$ could extract information $\{Y_1, Y_2, Y_3\}$ from the smart card and could get previous session messages transmitted through public network. The description of the security weaknesses of Roy et al.'s scheme is as follows.

A. Reply attack

If the adversary $\mathcal{A}$ obtains the transmitted parameter TID_i, $\mathcal{A}$ can attempt to reuse it as it's registration message, and then $\mathcal{A}$ can get δ_i used as a secret key between a user and a server. The procedure of replay attack is as follow.

1) $\mathcal{A}$ captures the transmitted parameter TID_i and sends it to S_j.
2) S_j which received TID_i from $\mathcal{A}$ computes $\delta_i = h(H(TID_i)||X_S)$ which is exactly same as that of U_i.
3) S_j sends δ_i to $\mathcal{A}$ via a secure channel.
4) $\mathcal{A}$ computes a session key $\mu_i = h(\delta_i)$ and may use it to decrypt D_1.

The result of this attack indicates that Roy et al.'s scheme is vulnerable to replay attack.

B. Offline password guessing attack

If the adversary $\mathcal{A}$ somehow steals SC_i of U_i, $\mathcal{A}$ can attempt to guess the password of U_i, and then $\mathcal{A}$ can guess identity and password of U_i successfully. The procedure of offline password guessing attack is as follows:

1) From the password dictionary space D_{PW}, the adversary $\mathcal{A}$ randomly chooses the password PW_i^*, and picks up the identity ID_i^* from the identity dictionary space D_{ID}.
2) $\mathcal{A}$ calculates $\theta_i^* = Y_2 \oplus h(h(ID_i^*)||PW_i^*)$
3) $\mathcal{A}$ calculates $TID_i^* = h(h(ID_i^*) \oplus h(\theta_i^*)$
4) To check the correctness of PW_i^*, $\mathcal{A}$ examines whether $TID_i^* = TID_i$, where TID_i is previous transmitted parameter. If it is correct, $\mathcal{A}$ guesses identity and password of U_i correctly.

Therefore, Roy et al.'s scheme is vulnerable to offline password guessing attack.

C. Lack of perfect forward secrecy

We assume that $\mathcal{A}$ intercepts and store messages transmitted in the previous session, and a session key μ_i is compromised by $\mathcal{A}$. In Roy et al.'s scheme, D_1 is computed as $D_1 = E_{\mu_i}(ID_i||\theta_i||\theta_i^*||TS_i||RN_i)$. Once μ_i is revealed to $\mathcal{A}$, $\mathcal{A}$ can decrypt the previous encrypted messages using μ_i. Therefore, Roy et al.'s scheme does not support perfect forward secrecy.

IV. Proposed Scheme

In this section, we present the secure biometric based remote user authentication scheme for IoT medical networks that overcomes the security weaknesses of Roy et al's scheme. To provide perfect forward secrecy, we refer Reddy et al.'s technique [19]. The proposed scheme consists of four phases as in the Roy's scheme, namely 1) Registration phase, 2) Login phase, 3) Authentication and key establishment phase, and 4) password change. It is worth noticing that the password change phase of the proposed scheme remains same as that of Roy et al.'s scheme.

A. Registration phase

If a new user U_i wants to access the medical service, U_i must register with the remote server S_j first. User registration phase in the proposed scheme is illustrated in Figure 3, and the detailed steps of this registration phase are as follows:

1) U_i chooses ID_i and PW_i, and imprints a biometric template B_i. U_i generates parameters $< \alpha_i, \beta_i > \leftarrow Gen(B_i)$.
2) U_i generates a random number θ_i and compute $TID_i = h(h(ID_i) \oplus h(\theta_i))$ and $RPW_i = h(ID_i||\alpha_i||h(PW_i))$. Then U_i sends TID_i, RPW_i to S_j via a secure channel.
3) S_j chooses two master key X_{S_1} and X_{S_2}. Then S_j computes $\delta_i = h(h(TID_i)||RPW_i||h(X_{S_1}))$, $B_i = h(\delta_i), C_i = h(X_{S_2} \oplus \delta_i)$. Then S_j sends a smart card SC_i and δ_i, B_i, C_i to U_i via a secure channel.
4) U_i computes the parameters Y_1, Y_2 and Y_3 as follows:

$$
\begin{aligned}
Y_1 &= B_i \oplus h(RPW_i||\theta_i) \\
Y_2 &= h(h(ID_i)||PW_i||\alpha_i) \oplus \theta_i \\
Y_3 &= h(\alpha_i||PW_i||\theta_i)
\end{aligned}
$$

5) Finally, U_i store the parameters $< Y_1, Y_2, Y_3, B_i, C_i, h(\cdot), \beta_i >$ in a smart card SC_i.

B. Login phase

When the authenticated user U_i wants to use a medical service, U_i sends request messages of accessing the medical service to the remote server S_j. The proposed scheme also supposed that U_i and S_j must authenticate each other before sending the request message. Login phase in the proposed scheme is illustrated as follows:

1) U_i chooses ID_i and PW_i, and imprints biometrics B_i'. Then SC_i generates α_i, and computes θ_i' and Y_3', and then compares Y_3' with Y_3 to check a user credential as follow:

$$
\begin{aligned}
\alpha_i &\leftarrow Rep(B_i', \beta_i) \\
\theta_i' &= Y_2 \oplus h(h(ID_i)||PW_i||\alpha_i) \\
Y_3' &= h(\alpha_i||PW_i||\theta_i') \\
\text{verifies } Y_3' &\stackrel{?}{=} Y_3
\end{aligned}
$$

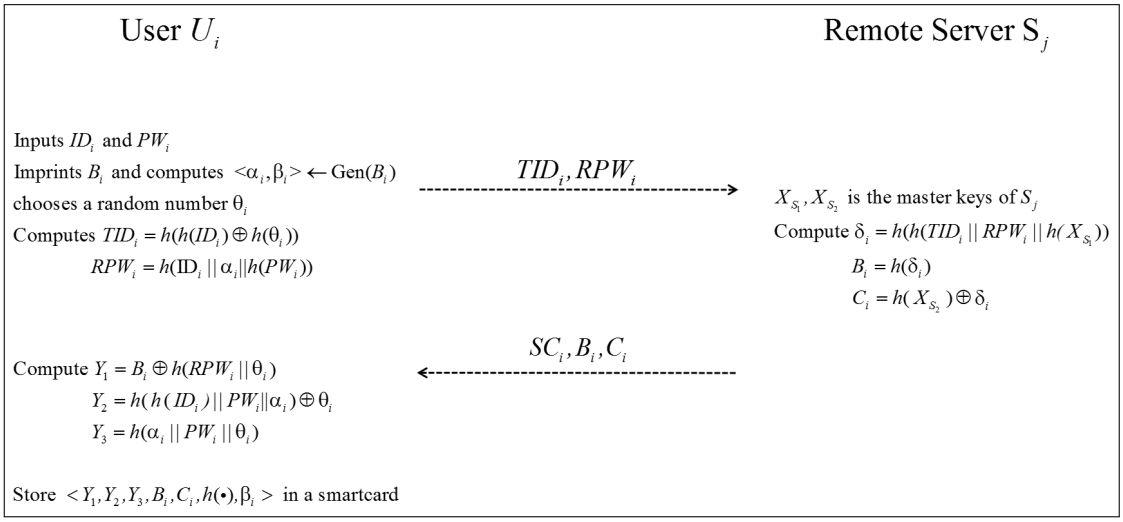

Fig. 3. User registration phase of the proposed scheme

2) SC_i generates two random number r_i and RN_i and computes RPW_i, K_i, PID_i, D_1 and H_1 as follows:

$$\begin{aligned} TID_i &= h(h(ID_i) \oplus h(\theta_i)) \\ RPW_i &= h(ID_i||\alpha_i||h(PW_i)) \\ B_i &= Y_1 \oplus h(RPW_i||\theta_i) \\ K_i &= h(C_i) \oplus r_i \\ PID_i &= TID_i \oplus r_i \\ M_i &= h(B_i) \oplus r_i \\ D_1 &= E_{K_i}(ID_i||\theta_i||r_i||TS_i||RN_i) \\ H_1 &= h(h(ID_i \oplus \theta_i)||r_i||TID_i||TS_i||RN_i) \end{aligned}$$

Then, U_i sends a request message $Msg_1 =< PID_i, C_i, M_i, D_1, H_1 >$ to S_j via a public channel.

C. Authentication and key establishment phase

U_i and S_j authenticate and generate a session key. Figure 4 illustrates the authentication and key establishment phase, which performs as follows:

1) S_j computes δ_i, r_i, K_i, and decrypts D_1 using K_i and obtain $(ID_i, \theta_i, r_i, TS_i, RN_i)$ as follow:

$$\begin{aligned} \delta_i &= C_i \oplus h(X_{S_2}) \\ B_i &= h(X_{S_1}) \oplus \delta_i \\ r_i &= M_i \oplus h(B_i) \\ K_i &= r_i \oplus h(C_i) \\ TID_i &= PID_i \oplus r_i \\ D_{K_i}(D_1) &= \{ID_i||\theta_i||r_i||TS_i||RN_i\} \end{aligned}$$

2) S_j retrieves TS_i^* and checks $TS_i^* - TS_1 \leq \Delta T$. If it is true, S_j checks the validity of H_1 and TID_i using the decrypted parameters of D_1 as follows:

$$\begin{aligned} H_1 &\stackrel{?}{=} h(h(ID_i) \oplus \theta_i)||r_i||TID_i||TS_i||RN_i) \\ TID_i &\stackrel{?}{=} h(h(ID_i) \oplus h(\theta_i)) \end{aligned}$$

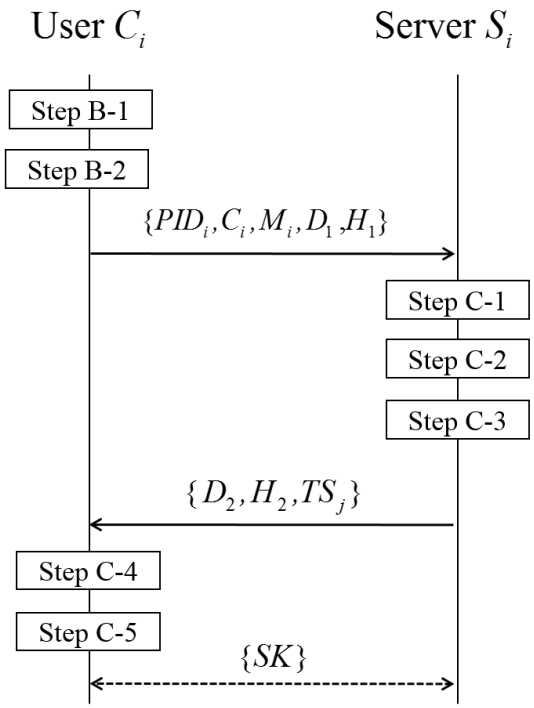

Fig. 4. Authentication and key establishment of the proposed scheme

If both verifications are successful, proceed to the next step.

3) S_j computes $TID_i, \delta_i^1, \lambda_i, D_2, SK_{S_j,U_i}$ and H_2 as follows:

$$\begin{aligned} TID_i^1 &= h(h(ID_i) \oplus h(\theta_i) \oplus h(r_i)) \\ \delta_i^1 &= h(h(TID_i^1)||h(X_{S_1})) \\ \lambda_i &= h(TID_i^1) \\ D_2 &= E_{\lambda_i}(\delta_i^1||\theta_i||RN_j) \\ SK_{S_j,U_i} &= h(\delta_i^1||r_i||RN_i||RN_j||TS_i||TS_j) \\ H_2 &= h(TID_i^1||\delta_i^1||SK_{S_j,U_i}||TS_j||RN_j) \\ & \text{(where, } TS_j \text{ is the time stamp.)} \end{aligned}$$

Then, S_j sends the replay message $Msg_2 =< D_2, H_2, TS_j >$ to U_i via a public channel.

4) U_i retrieves TS_j^* and checks $TS_j^* - TS_j \leq \Delta T$. If it is true, U_i computes TID_i^1, δ_i and decrypts D_2 as follows:

$$\begin{aligned} TID_i^1 &= h(h(ID_i) \oplus h(\theta_i) \oplus h(r_i)) \\ \lambda_i &= h(TID_i^1) \\ D_{\lambda_i}(D_2) &= \{\delta_i^1||\theta_i||RN_j\} \end{aligned}$$

5) Finally, U_i generates a session key $SK_{U_i,S_j} = h(\delta_i^1||r_i||RN_i||RN_j||TS_i||TS_j)$. Then U_i checks the validity of H_2 by comparing it with the computed value $h(TID_i^1||\delta_i^1||SK_{U_i,S_j}||TS_j||RN_j)$. If it is true, U_i accepts SK_{U_i,S_j} as the current session key, then updates new parameters Y_1^*, Y_2^* and Y_3^* as follows:

$$\begin{aligned} Y_1^* &= B_i \oplus h(RPB_i||r_i) \\ Y_2^* &= h(h(ID_i)||PW_i||\alpha_i) \oplus r_i \\ Y_3^* &= h(\alpha_i||PW_i||r_i) \end{aligned}$$

V. Analysis

We analyse security and efficiency of the proposed authentication scheme. To prove the security of our proposed scheme, we perform the formal security analysis using the the BAN logic [20]. Furthermore, We perform the informal security analysis in order to verify the security of the proposed scheme is secure with high probability.

A. BAN logic security analysis

The notations of the BAN logic are given in Table II:

TABLE II. Notations of the BAN Logic

Notation	Description
$P\mid\equiv X$	P **believes** the statement X
#X	The statement X is **fresh**
$P \lhd X$	P **sees** the statement X
$P\mid\sim X$	P once **said** X
$P \Rightarrow X$	P **controls** the statement X
$< X >_Y$	Formula X is **combined** with the formula Y
$\{X\}_K$	Formula X is **encrypted** by the key K
$P \overset{K}{\leftrightarrow} Q$	P and Q communicate using K as the **shared key**
SK	Session key used in the current authentication session

1) Postulates of BAN logic: The postulates of the BAN logic are given below:

1. Message meaning rule :

$$\frac{P \mid\equiv P \overset{K}{\leftrightarrow} Q, \quad P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X}$$

2. Nonce verification rule :

$$\frac{P \mid\equiv \#(X), \quad P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

3. Jurisdiction rule :

$$\frac{P \mid\equiv Q \mid\Longrightarrow X, \quad P \mid\equiv Q \mid\equiv X}{P \mid\equiv X}$$

4. Freshness rule :

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$$

5. Belief rule :

$$\frac{P \mid\equiv (X,Y)}{P \mid\equiv X.}$$

2) Goals: We have the following goals to demonstrate the secure mutual authentication of proposed protocol:

Goal 1: $S \mid\equiv (S \overset{SK_{U_i,S_j}}{\longleftrightarrow} U)$

Goal 2: $S \mid\equiv U \mid\equiv (S \overset{SK_{U_i,S_j}}{\longleftrightarrow} U)$

Goal 3: $U \mid\equiv (S \overset{SK_{U_i,S_j}}{\longleftrightarrow} U)$

Goal 4: $U \mid\equiv S \mid\equiv (S \overset{SK_{U_i,S_j}}{\longleftrightarrow} U)$

3) Idealized Forms: The idealized forms of the transmitted messages are given below:

Msg_1**:** $U \rightarrow S$: $(ID_i, TID_i, RN_i, r_i, TS_i, \theta_i)_{K_i}$

Msg_2**:** $S \rightarrow U$: $(\delta_i^1, RN_j, TS_j, SK_{U_i,S_j})_{\lambda_i}$

4) Assumptions: We make the following initial assumptions to perform the BAN logic proof:

A_1**:** $S \mid\equiv \#(RN_i)$

A_2**:** $U \mid\equiv \#(RN_j)$

A_3**:** $S \mid\equiv (S \overset{K_i}{\longleftrightarrow} U)$

A_4**:** $U \mid\equiv (S \overset{\lambda_i}{\longleftrightarrow} U)$

A_5**:** $S \mid\equiv U \Rightarrow (SK_{U_i,S_j})$

A_6**:** $U \mid\equiv S \Rightarrow (SK_{U_i,S_j})$

5) Proof Using BAN Logic: The detailed steps of the main proof are as follows:

Step 1: According to Msg_1, we can obtain

$$S_1 : S \lhd (ID_i, TID_i, RN_i, r_i, TS_i, \theta_i)_{K_i}$$

Step 2: In conformity with the message meaning rule with S_1 and A_3, we can get

$$S_2 : S \mid\equiv U \mid\sim (ID_i, TID_i, RN_i, r_i, TS_i, \theta_i)_{K_i}$$

Step 3: According to the freshness rule with A_1, we can get

$$S_3 : S \mid\equiv U \mid\equiv \#(ID_i, TID_i, RN_i, r_i, TS_i, \theta_i)_{K_i}$$

Step 4: According to the nonce verification rule with S_2 and S_3, we can obtain

$$S_4 : S \mid\equiv U \mid\equiv (ID_i, TID_i, RN_i, r_i, TS_i, \theta_i)_{K_i}$$

Step 5: According to the belief rule with S_3 and S_4, we can get

$$S_5 : S \mid\equiv U \mid\equiv (RN_i, r_i, TS_i)$$

Step 6: Because of $SK_{U_i,S_j} = h(\delta_i^1||r_i||RN_i||RN_j||TS_i||TS_j)$ from the S_5 and A_2, we can get. where δ_i^1, RN_j are random number selected by S_j and TS_j is current timestamp.

$$S \mid\equiv U \mid\equiv (S \overset{SK_{U_i,S_j}}{\longleftrightarrow} U) \qquad \textbf{(Goal 2)}$$

Step 7: According the jurisdiction rule with S_6 and A_5, we can obtain

$$S \mid\equiv (S \overset{SK_{U_i,S_j}}{\longleftrightarrow} U) \qquad \textbf{(Goal 1)}$$

Step 8: According to Msg_2, we can obtain

$$S_8 : U \lhd (\delta_i^1, RN_j, TS_j, SK_{U_i,S_j})_{\lambda_i}$$

Step 9: In conformity with the message meaning rule with S_8 and A_4, we can get

$$S_9 : U \mid\equiv S \mid\sim (\delta_i^1, RN_j, TS_j, SK_{U_i,S_j})_{\lambda_i}$$

Step 10: According to the freshness rule with A_2, we can get

$$S_{10} : U \mid\equiv S \mid\equiv \#(\delta_i^1, RN_j, TS_j, SK_{U_i,S_j})_{\lambda_i}$$

Step 11: According to the nonce verification rule with S_9 and S_{10}, we can obtain

$$S_{11} : U \mid\equiv S \mid\equiv (\delta_i^1, RN_j, TS_j, SK_{U_i,S_j})_{\lambda_i}$$

Step 12: According to the belief rule with S_{10} and S_{11}, we can get

$$S_{12} : U \mid\equiv S \mid\equiv (S \overset{SK_{U_i,S_j}}{\longleftrightarrow} U) \qquad \textbf{(Goal 4)}$$

Step 13: According the jurisdiction rule with S_{12} and A_6, we can obtain

$$U \mid\equiv (S \overset{SK_{U_i,S_j}}{\longleftrightarrow} U) \qquad \textbf{(Goal 3)}$$

B. Security analysis against various attacks

Replay attack. Our scheme does not send a real identity ID_i in public channels. $\mathcal{A}$ is required to know TID_i and θ_i to derive ID_i from PID_i, however, $\mathcal{A}$ cannot obtain both TID_i and θ_i. Because r_i is hidden to $\mathcal{A}$ and ID_i, θ_i is only known to an authentic user U_i. Furthermore, PID_i changes in every session, therefore, $\mathcal{A}$ cannot reuse TID_i or PID_i to get any information from S_j in registration phase as we have shown in chapter 3-A.

Resisting off-line Identity and password guessing attack. $\mathcal{A}$ may attempt to guess ID_i from PID_i and Y_2. Suppose $\mathcal{A}$ obtains these values and a smart card SC_i. To find ID_i from PID_i, $\mathcal{A}$ have to know r_i and compute TID_i first, and then guess ID_i and θ_i concurrently, The guessing probability, when ID_i consist of n characters and the hash value is 160 bits, is roughly $1/2^{6n+160}$ and it is a computationally infeasible problem [21]. Therefore, it is infeasible to guess an identity correctly in our scheme.

Resisting off-line password guessing attack. $\mathcal{A}$ may attempt to guess PW_i from Y_2 and Y_3. The probability of guessing PW_i from Y_2 and Y_3 is same as above. $\mathcal{A}$ who somehow gets RPW_i is also required to guess ID_i, PW_i and α_i concurrently, and the probability is more complicated. Therefore, it is infeasible to guess a password correctly.

Forward secrecy and session key exposure. Three keys K_i, λ_i, and SK exist in the proposed scheme. Ephemeral key K_i is computed as $r_i \oplus h(C_i)$. Though $\mathcal{A}$ somehow knows K_i, he/she cannot compute previous ephemeral keys K_i, because r_i changes in every session and is hidden to $\mathcal{A}$. Likewise $\mathcal{A}$ somehow knows λ_i, he/she cannot compute previous ephemeral keys, because r_i changes in every session and is hidden to $\mathcal{A}$. Session key contains random parameters $\{r_i, RN_i, RN_j, TS_i TS_j\}$. Therefore, our scheme provides forward secrecy and withstands the session key exposure.

User anonymity. Our scheme does not send a real identity ID_i in public channels. $\mathcal{A}$ is required to compute TID_i to derive ID_i, however, $\mathcal{A}$ cannot even obtain TID_i because of r_i is hidden. And TID_i changes dynamically into PID_i, thus $\mathcal{A}$ cannot trace U_i using identity information. Therefore, our scheme provides user anonymity.

Resisting user impersonation attack. $\mathcal{A}$ who obtains a smart card SC_i of U_i and tries to access S_j is needed to generate and send a valid login request message $\{PID_i, C_i, M_i, D_1, H_1\}$ to S_j. To compute those values, $\mathcal{A}$ needs to know TID_i, B_i and compute PID_i, M_i, however, $\mathcal{A}$ does not know these parameters. Thus, $\mathcal{A}$ cannot compute valid login messages and finally H_1. Therefore, our scheme withstands the user impersonation attack.

Resisting server impersonation attack. $\mathcal{A}$ needs to compute valid reply messages D_2 and H_2 to masquerade

as a server, however, he/she cannot compute valid reply messages because $\mathcal{A}$ cannot get δ_i^1. Therefore, our scheme withstands the server impersonation attack.

Resisting man-in-the-middle attack. $\mathcal{A}$ who knows public channel information between U_i and S_j and has a smart card SC_i can establish a secure channel when $\mathcal{A}$ knows unique information of U_i, such as PID_i, C_i, M_i..... However, as we mentioned above, $\mathcal{A}$ cannot compute those values because r_i is hidden to $\mathcal{A}$ and guess ID_i, PW_i, and α_i. Therefore, our proposal withstands the man-in-the-middle attack.

Resisting stolen smart card attack. $\mathcal{A}$ who somehow possesses a valid smart card SC_i of U_i may attempt to get authentication credentials. But, $\mathcal{A}$ cannot have any advantage because all the parameters are protected with a one-way has function. $\mathcal{A}$ also cannot obtain or compute any login information using SC_i without ID_i, PW_i and α_i. Guessing ID_i and PW_i concurrently is impractical as mentioned above. Therefore, our scheme withstands the stolen smart card attack.

We compare the functionality features of the proposed scheme with Roy et al.'s scheme in Table III. ○ indicates the scheme provides the property or is secure against the attack; × indicates the scheme does not provide the property or is vulnerable to the attack.

TABLE III. COMPARISONS OF THE FUNCTIONALITY FEATURES

	Roy et al.' scheme [13]	Proposed scheme
replay attack	×	○
ID guessing attack	×	○
password guessing attack	×	○
forward secrecy	×	○
user anonymity	○	○
efficient password change	○	○
user impersonation attack	○	○
server impersonation attack	○	○
man-in-the-middle attack	○	○
stolen smart card attack	○	○

C. Performance

We compare the cost of computation with Roy et al's scheme in Table IV. T_h indicates the computation time for hash function; T_F indicates fuzzy extraction; XOR are not considered because it can be ignored comparing with T_h. The computation cost of ours is almost similar to [13], and the proposed scheme enhances the security.

TABLE IV. COMPARISONS OF THE COMPUTATION COSTS

	Roy et al.'s scheme [13]		Proposed scheme	
	User	Server	User	Server
Registration	$10T_h + T_F$	$3T_h$	$9T_h + T_F$	$5T_h$
Login	$11T_h + T_F$	0	$13T_h + T_F$	0
Authentication	$10T_h$	$19T_h$	$9T_h$	$19T_h$
Total	$31T_h + 2T_F$	$22T_h$	$31T_h + 2T_F$	$24T_h$

VI. CONCLUSIONS

Several biometric-based remote user authentication schemes using smart card have been proposed in the last few years. Unfortunately, most of them could not provide secure authentication and suffer from various attacks. This paper showed the security flaws of Roy et al.'s scheme. Roy et al's scheme is prone to replay attacks and offline guessing attacks. Furthermore, their scheme does not support perfect forward secrecy. We proposed a secure user authentication scheme in IoT medical environments for better security functionality than that of Roy et al. Our scheme withstands various attacks, such as replay and guessing attacks. In addition, our scheme provide perfect forward secrecy to provide secure authentication. In addition, the proposed scheme provides a dynamic identity mechanism and withstands various attacks by the malicious server.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2018R1D1A3B07050409) and was supported by the Korea Nazarene University Research Grants, 2018.

REFERENCES

[1] J. L. Tsai, N. W. Lo, and T. C. Wu, *"Novel anonymous authentication scheme using smart cards"*, IEEE Transactions on Industrial Informatics, IEEE, Computer Networks, 101(4), 192-202, 2016.

[2] M. S. Hossain and G. Muhammad, *"Cloud-assisted industrial internet of things (IIoT) âĂŞ enabled framework for health monitoring"*, 9(4), 2004-2013, 2013.

[3] Q. Jiang, J. Ma, Z. Ma, and G.Li, *"A privacy enhanced authentication scheme for telecare medical information systems,"* J. Med. Syst., 37, 2013.

[4] D. Mishra, S. Kumari, M. K. Khan, and S. Mukhopadhyay, *"An anonymous biometric-based remote-user authentication key agreement scheme for multimedia systems"*, International Journal of Communication Systems, 2015.

[5] Y. H. Park and Y. H. Park, Y. *"A Selective Group Authentication Scheme for IoT-Based Medical Information System."* Journal of medical systems, 41(4), 48, 2017.

[6] S. Kumari, M. K. Khan, and R. Kumar, *"Cryptanalysis and improvement of 'a privacy enhanced scheme for telecare medical information systems'"*, Journal of medical systems, 37(4), 2013.

[7] T. Cao and J. Zhai, *"Improved dynamic id-based authentication scheme for telecare medical information systems"*, Journal of medical systems, 37(2), 2013.

[8] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo, *"Secure signature-based authenticated key establishment scheme for future IoT applications"*, IEEE Access, 5, 3028-3043, 2017.

[9] M. Turkanovic, B. Brumen, and M. HÃűlbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion, Ad Hoc Networks 20, pp. 96-112, 2014.

[10] X. Yao, X. Han, X. Du, and X. Zhou, A lightweight multicast authentication mechanism for small scale IoT applications, IEEE Sensors Jour., 13(10), pp. 3693-3701, Oct., 2013.

[11] B. Ndibanje, H. J. Lee, and S. G. Lee, Security analysis and improvements of authentication and access control in the internet of Things, Sensors, 14(8), pp. 14786-14805, 2014.

[12] H. M. Chen, J. W. Lo, and C. K. Yeh, An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems, J. Med. Syst., 36(6), pp. 3907-3915, Dec., 2012.

[13] S. Roy, S. Chatterjee, and G. Mahapatra, *"An efficient biometric based remote user authentication scheme for secure internet of things environment",* Journal of Intelligent & Fuzzy Systems, 34(3), 1403-1410, 2018.

[14] D. Dolev and A. Yao, *"On the security of public key protocols"*, IEEE Trans. Inf. Theory, 29(2), 198-208, 1983.

[15] K. S. Park, Y. H. Park, Y. H. Park, and A. K. Das, *"2PAKEP: Provably Secure and Efficient Two-Party Authenticated Key Exchange Protocol for Mobile Environment,"* IEEE Access, 6, 2018.

[16] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, *"Examining smart-card security under the threat of power analysis attacks",* IEEE Trans. Comput., 51(5), 541-552, 2002.

[17] P. Kocher, J. Jaffe, and B. Jun, *"Differential power analysis",* in Proc. 19th Annu. Int. Cryptol. Conf., Santa Barbara, CA, USA, Aug. 1999.

[18] G. Xu, S. Qiu, H. Ahmad, G. Xu, Y. Guo, M. Zhang, and H. Xu, *"A Multi-Server Two-Factor Authentication Scheme with Un-Traceability Using Elliptic Curve Cryptography",* Sensors, 18(7), 2018.

[19] A. G. Reddy, E. J. Yoon, A. K. Das, and K. Y. Yoo, *"Lightweight authentication with key-agreement protocol for mobile network environment using smart cards,"* IET Information Security, 10(5), 2016.

[20] M. Burrows, M. Abadi, and R. Needham, *"A logic of authentication,"*, ACM Trans. Comput. Syst., 8(1), 1990.

[21] A. K. Das and A. Goswami, *"A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care,"* Journal of medical systems, 37(3), 2013.