

A robust authentication and access control protocol for securing wireless healthcare sensor networks

Zeeshan Ali^a, Anwar Ghani^a, Imran Khan^a, Shehzad Ashraf Chaudhry^b, SK Hafizul Islam^{c,*}, Debasis Giri^d

^a Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan

^b Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University Istanbul, 34310, Turkey

^c Department of Computer Science and Engineering, Indian Institute of Information Technology Kalyani, West Bengal 741235, India

^d Department of Information Technology, Maulana Abul Kalam Azad University of Technology, West Bengal, India

ARTICLE INFO

Article history:

Available online 1 April 2020

Keywords:

Wireless sensor network
Healthcare system
Elliptic curve cryptography
Authentication
Access and control
BAN Logic
AVISPA
Formal security

ABSTRACT

Wireless Healthcare Sensor Network (WHSN) has become one of the major research fields over the past decades that play a very prominent role in the medical field. Due to the rapid growth of technology in wireless communication, different security challenges have been raised in WHSN. Authentication protocols are used to secure the information transferred over the public channels by WHSN. For this prospect recently, Liu & Chung proposed an authentication and data transmission mechanism for WHSN. However, Challa et al. identified that Liu-Chung's scheme is vulnerable to stolen smart-card, offline password guessing, privileged insider, and user impersonation attacks. Challa et al. then proposed an enhanced scheme to overcome beforehand stated flaws. This paper denotes out that in accession to before mentioned attacks, Liu-Chung's scheme is also prone to users' private key leakage and user impersonation attacks towards sensors. Moreover, Challa et al.'s scheme suffers from incorrectness, broadcasting problem, lack of authentication between Trusted Authority (TA) and sensor nodes, replay attack, Denial of Service (DoS) attack, forgery attack and delay in communication due to the involvement of the TA. Using the elliptic curve cryptography and bilinear paring, an improved scheme is proposed in this paper, to mitigate the weaknesses of Challa et al. and Liu-Chang schemes. The formal security analysis using simulation tool AVISPA and BAN logic demonstrate that the proposed scheme is secure. The rigorous informal security analysis also attests that our scheme is safe against well-known attacks.

© 2020 Elsevier Ltd. All rights reserved.

1. Introduction

Recent progress in the digital wireless communication infrastructure for sensors has backed the development of multifunctional small size, low-power and cost-efficient sensor nodes to communicate wirelessly in short distances [1]. These tiny sensor nodes typically consist of a micro-controller, transceiver, memory and a power source [2,3]. These miniature nodes collaborate to form a sensor network [4]. The tiny sensors can be used to monitor healthcare once installed inside or outside of human body to avoid conventional way of in-person illness monitoring [5]. *eHealth* is the utilization of information and communication technologies

(ICT) for health monitoring and diagnosis [6]. ICT based healthcare services can be used to overcome the shortcomings of the typical healthcare system like remote health monitoring, healthcare data analytics [7,8]. A new type of network called Wireless Body Area Network (WBAN) has been evolved to fully utilize and to take advantage of wireless sensor technologies [9]. In WBAN number of sensors are implanted in or out of the body to continuously monitor and give real-time feedback to the physician/doctor or user/patient [10]. The data accumulated by the sensors can be stored for a lengthier period, thus enhancing the quality of gather data [11]. The data obtained with the help of sensors is transmitted remotely to data centers at the rear end for processing and analysis to make the treatment decisions [12]. As the WBAN reap the benefits of continuous progress, it will not only be employed in medical but will also be integrated into the military applications and sports activities and can save human lives. With tremendous potential for raising quality of healthcare, WBAN can play decisive role for improvement of healthcare facilities in remote areas.

* Corresponding author.

E-mail addresses: zeeshan.mscs1053@iiu.edu.pk (Z. Ali), anwar.ghani@iiu.edu.pk (A. Ghani), imran.khan@iiu.edu.pk (I. Khan), sashraf@gelisim.edu.tr, ashraf.shehzad.ch@gmail.com (S.A. Chaudhry), hafiz786@gmail.com (S.H. Islam), debasish_giri@hotmail.com (D. Giri).

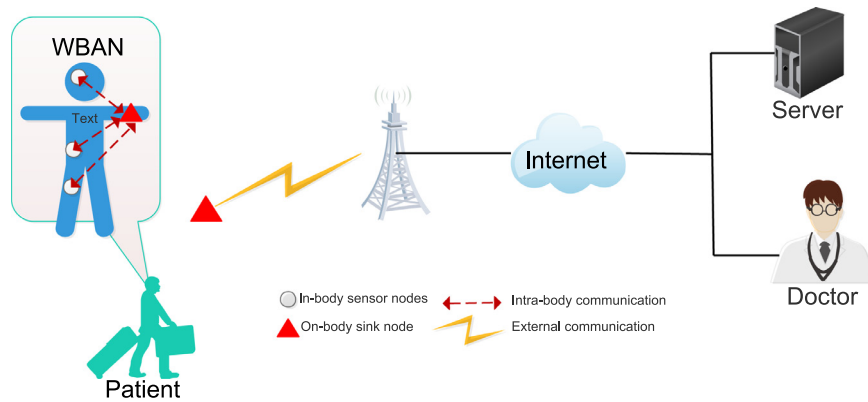


Fig. 1. Architecture of typical WBAN system.

A distinctive healthcare-monitoring scenario using WBAN has an exhibit in Fig. 1. To match the expectation of healthcare, the future will see further integration between wireless sensor technologies and current specialized medical resources [13]. Healthcare applications require trustworthiness that data measured by sensors are accurate. WSNs used in healthcare collect daily data and transfer it to remote servers. Furthermore, as the adaption of sensor networks for health monitoring increases importance to secure such systems also rises [14,15]. While setting up a WSNs for healthcare multiple limitations need to be faced due to their micro size such as limited energy, memory and processing limits, limited network capacity, privacy and security and system reliability [16–18]. Sensors need to combat both insider and outsider attack as sensor nodes may not be temper proof [19].

Using WSNs for collecting physiological data of patients also gives rise to personal privacy. Its crucial for WSNs applied to medical care to prevent attackers or eavesdropper from malicious network intrusion while keeping the protection and privacy of user data [20]. Only legal users will be enabled to login and access the system resources with secure authentication scheme. Different schemes have been proposed to overcome these security challenges each of these schemes have their own strengths and weaknesses which will be discussed in related work section. Following are the general contributions of this article:

- The cryptanalysis of the scheme by Liu-Chung [15] and Challa et al. [21] are performed to show that, Li-Chung's scheme is vulnerable to users private key leakage and user impersonation attack towards sensors, and Challa et al.'s scheme suffers from incorrect, broadcasting problem, lack of mutual authentication between TA and sensor nodes, and is prone to communication delay.
- A three-factor (password, biometric and smart-card) based authentication scheme is proposed to overcome the drawbacks in Challa et al.' and Liu-Chung's schemes.
- The proposed scheme is analyzed formally, through BAN Logic and simulated through the AVISPA tool for robustness proof; furthermore, meticulous informal security analysis is accomplished to show its' resistance against the known attacks.
- The comparative analysis of the proposed scheme with Liu-Chung's and Challa et al.'s as well as other state-of-the-art protocols is performed using the computation and communication costs and security requirements metrics.

1.1. Adversarial model

As adopted in [22–27], the common adversary model is taken up in this article, where the adversary $\mathcal{I}$ is considered to be equipped with following capabilities:

1. The communication is under complete control of $\mathcal{I}$
2. $\mathcal{I}$ is allowed to intercept, replay old message, modify, stop or send a fabricated message.
3. $\mathcal{I}$ has the capabilities to launch power analysis and get data stored in smart card [22,27].
4. Except the TA, any insider or outsider can try to break the security and privacy.
5. TA's private key cannot be compromised i.e no attacker $\mathcal{I}$ is allowed to have access to private key of TA.

The paper is organized as follows. Section 2 briefly describes the existing literature and their issues. Section 3 provides basics of the cryptographic primitives used in this article. Liu-Chung's [15] and Challa et al.'s [21] scheme are reviewed in Section 4, and their cryptanalysis is done in Section 5. Our scheme and its security analysis using BAN logic, informal way and through AVISPA simulation are describes sequentially in Section 6 and 7. The comparisons with respect to performance and security features are solicited in Section 8. The paper is finally concluded in Section 9.

2. Related work

Various authentication schemes for securing healthcare sensors networks are outlined in this section. Many researchers came up with the schemes to secure healthcare sensor networks over the past years. Smys et al. [28] stated the architecture and requirements for securing wireless body area network (WBAN). The architecture contained a cluster with a cluster head to forward the aggregated data to base station. Shen et al. [29] proposed a multilayer authentication protocol, in which they divided communication of Wireless body area networks (WBANs) into two layers inside and outside authentication. Inside authentication is between sensors and PDA (personal digital assistance) and outside authentication is between PDA and AP. In the communication layer between PDA and sensor, PDA is regarded as a cluster head with sufficient memory and computational power. Liu et al. [30] identified that Shen et al.'s scheme has some security vulnerabilities like mutual impersonation and mutual authentication attack, so they provided an enhanced scheme to overcome these flaws. A new health monitoring system architecture for Wireless medical sensor network (WMSN) was proposed by Amin et al. [31]. They proposed an architecture in WMSN for patient monitoring health-care system and provided a mutual authentication protocol for mobile users while preserving anonymity. However, Ali et al. [32] proved some weaknesses of Amin et al.'s scheme against different attack. Wu et al. [33] proposed a three factor remote authentication scheme for mobile mobile client-server networks. Proposed scheme consists of three factors identity, password and biometric along with Elliptic curve cryptography (ECC). Wu et al. stated

that there scheme is secure against all known attacks and is secure against Insider attack, Off-line guessing attack, User impersonation attack, Server spoofing attack, Known-key attack and provides User anonymity. However, Xie et al. [34] identified that Wu et al.'s scheme is vulnerable against Impersonation attack. Xie et al. stated that their scheme is secure against Replay attack, Off-line password guessing attack, Privileged insider attack, Impersonation attack, Stolen-verifier attack, Man-in-the-middle attack and provides User anonymity, Session key security and Mutual authentication.

Liu-Chung [15] proposed an user authentication scheme for WHSN (wireless healthcare sensor networks) in which, when patients are in healthcare center or hospital their physiological data is continuously stored in the system. Patients need to wear mobile-care devices, in order to record their physiological data. They stated that their scheme is secure against attacks like Stolen-verifier, Online password guessing attack, Offline password guessing attack. Later Challa et al. [21] identified that Liu-Chung's scheme is vulnerable against several attacks and proposed an improved scheme. Some other latest developments for securing healthcare services were also presented in [35–39]; whereas some criterion for authentication security were proposed in [40–43]. In 2019, Zhang et al. [44] proposed the first white-box implementation of the identity-based signature scheme in the IEEE P1363 standard. Their implementation can avoid the leakage of the private key during the algorithm executed in the untrusted environment. Therefore, it could be used to implement the authentication of the mobile devices. However, this paper shows that Liu-Chang's scheme is still prone to user's private key leakage. Also, Challa et al.'s scheme suffers from the incorrectness, broadcasting problem, lack of mutual authentication between TA and sensor nodes, replay attack, DoS attack, forgery attack, and is prone to communication delay. In this paper, an enhanced three-factor based scheme has been proposed to overcome the mentioned drawbacks.

3. Preliminaries

In this section, we describe some cryptographic primitives used in the paper.

3.1. Elliptic-curve cryptography (ECC)

Elliptic-curve cryptography (ECC) is based on the elliptic curves of the finite field $\mathcal{Z}_q = \{1, 2, 3, \dots, p-1\}$ and is a type of public key cryptography defined by the equation:

$$E_p(a, b) : y^2 \bmod q \equiv (x^3 + ax + b) \bmod q$$

where $a, b \in \mathcal{Z}_q$ and $(4a^3 + 27b^2) \bmod q \neq 0$. The points over $E_p(a, b)$ define an additive abelian group and is defined as $G_1 = \{(x_1, x_2) : x_1, x_2 \in \mathcal{Z}_q \text{ and } (x_1, x_2) \in E_p(a, b)\} \cup \{\mathcal{O}\}$, where the identity element $\mathcal{O}$ is called "point of infinity". In $E_q(a, b)$, the scalar multiplication is used to calculate multiplication by doing repeated addition. For example $r \cdot P = P + P + \dots + P$ (r times), where $P \in E_q(a, b)$.

3.2. Bilinear pairing

Identity based encryption (IBE) is first proposed by Shamir et al. [45], which employs the users personal information as a public key. An efficient IBE is proposed by Boneh and Franklin [46] by utilizing the pairing function. The bilinear map function $\hat{e} : G_1 \rightarrow G_2$ has subsequent properties:

Bilinear: Let $P, Q, R \in G_1$, where $a, b \in \mathcal{Z}_q^*$. Then $\hat{e}(aP, bQ) = \hat{e}(bP, aQ) = \hat{e}(P, R)^{ab}$, $\hat{e}(P, Q + R) = \hat{e}(P, Q) \cdot \hat{e}(P, R)$ and $\hat{e}(P + Q, R) = \hat{e}(P, R) \cdot \hat{e}(Q, R)$.

Non-degenerate: If G_1 is produced by P . Then G_2 is generated by $\hat{e}(P, P)$ such that $\hat{e}(P, P) \neq 1$.

Computable: All $P, Q \in G_1$ can be calculated in polynomial time through an existing algorithm such that $\hat{e}(P, Q) \in G_2$.

3.3. Hash function

A non-invertible function $H : \{0, 1\}^* \rightarrow \{0, 1\}^n$ called as one-way hash, it takes a variable-size input say $x \in \{0, 1\}^*$ and produces a binary string of fixed size say $y \in \{0, 1\}^n$. A hash function $H(\cdot)$ has the following properties:

- For any given input $x \in \{0, 1\}^*$, the computation of $y = H(x) \in \{0, 1\}^n$ is usually easy.
- **One-way property:** From a given value of hash $y \in \{0, 1\}^n$ and a function $H(\cdot)$, it is hard to obtain the input $x \in \{0, 1\}^*$. This property is called **preimage resistance**.
- **Resistance property of weak-collision:** For any given input $x_1 \in \{0, 1\}^*$, obtaining any other input $x_2 \in \{0, 1\}^*$, with $x_1 \neq x_2$, such that $H(x_1) = H(x_2)$, is hard to determine. This property is called **second preimage resistance**.
- **Resistance property of strong-collision:** Deriving a pair of inputs (x_1, x_2) , with $x_1 \neq x_2$, such that $H(x_1) = H(x_2)$ is also hard to calculate.

4. Review of previous schemes

The security schemes of Liu-Chung [15] and Challa et al. [21] are briefly reviewed in this section. The symbols adopted for the review and description purposes are depicted in Table 1.

4.1. Review of Liu-Chung's scheme

In this section, the review of the scheme by Liu-Chung [15] is presented. Trusted Authority (TA), Sensor Node (SN) and Patients are the three principal parties in this scheme. In Fig. 2 the considered system architecture is illustrated. In the given situation, the patients are in the healthcare centers or hospital and are equipped with wireless monitoring devices used to read the individual's data continuously. Sensors on patients are requested by the base station for updates of physiological data periodically. Requested data after collection, is uploaded by the base station to the hospital or healthcare center servers for diagnosis purposes by medical professionals. To guarantee legal access, an individual must register with the TA and obtain legitimate credentials. The scheme is arranged in four phases, all phases are described in the succeeding subsections:

4.1.1. Setup phase

Following steps are performed by the TA in setup phase:

- Step P1:** TA selects a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ and $P_0 \in G_1$.
- Step P2:** TA generates two one way hash functions $H_1 : \{0, 1\}^* \rightarrow G_2$, and $H_2 : G_2 \rightarrow \{0, 1\}^*$.
- Step P3:** TA selects a random number $S_0 \in \mathcal{Z}_q^*$, and then computes a public parameter $P_{pub} = S_0 \cdot P_0$.

4.1.2. Registration phase

User needs to personally attend the medical institution to register, and demonstrate his identification. Following are the steps performed in registration phase:

- Step P1:** User U_i selects UID_i and PWD_i to register with the TA.
- Step P2:** The TA selects a public key U_{pub} and calculates the private key ($U_{priv} = S_0 \cdot U_{pub}$) of the U_i .
- Step P3:** TA stores $\{h, U_{priv}, UID_i, PWD_i, a\}$ into the smart-card, a is a private parameter created by TA.
- Step P4:** TA transfers the smart-card to U_i over a private channel.

Table 1
Notation guide.

Notations	Description
TA, UID_i, SN_j	Trusted authority, i th user identity, j th sensor node, respectively
USC_i	i th user's smart-card
PWD_i, BIO_i	i th user's password, personal biometrics template, respectively
$Gen(\cdot), Rep(\cdot)$	Generation, Reproduction processes of fuzzy extractor
t	Fuzzy extractor's error tolerance threshold
σ_i, τ_i	Biometric secret key & public reproduction parameter, respectively
K_{priv}, K_{pub}	1024-bit private-key only known to the TA, and public-key
$E_p(a, b), p$	Elliptic Curve, Large prime number
$P = (x_p, y_p), k, P$	A point over $E_p(a, b)$ and multiplication of P with scalar k , respectively
$T_{sv}, \Delta T$	Session-validity period and max transmission delay
T_i, T_{ta}, T_{sn}	Current timestamps of i th user, TA and SN_j respectively
$\mathcal{I}, \mathcal{A}, \mathcal{U}_A$	An intruder, adversary and privileged user
$h(\cdot), \oplus, \parallel$	One-way cryptographic hash function, Bitwise XOR and concatenation operations, respectively

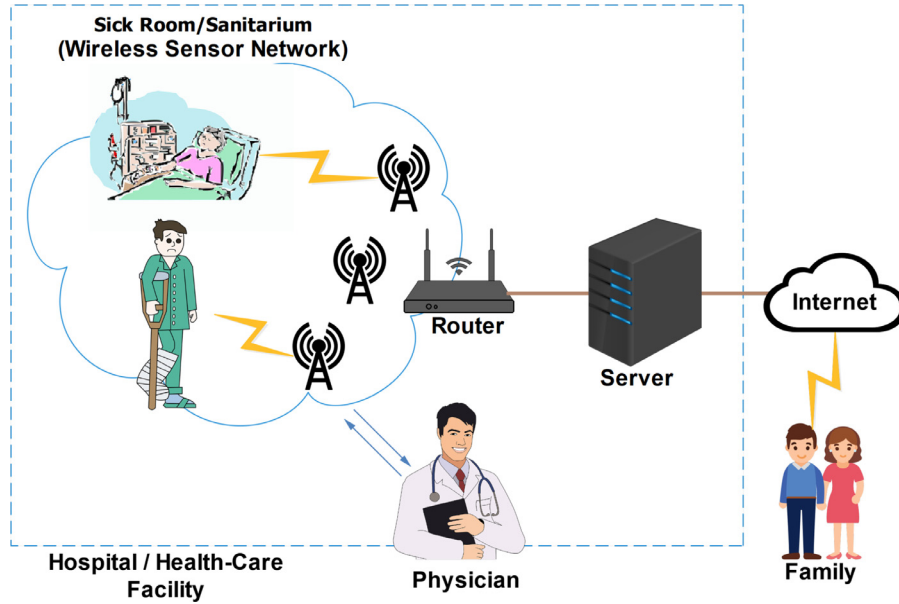


Fig. 2. System architecture.

4.1.3. Verification phase

TA performs the following steps to verify the authenticity of U_i upon receiving the message $\{Sig, r, T_L, UID_i\}$:

- Step P1:** TA verifies if UID_i is stored and $\hat{e}(P_0, Sig) = \hat{e}(P_{pub}, r \cdot U_{pub})$.
- Step P2:** If $T_c - T_L < \Delta T$, TA will proceed to Step P3.
- Step P3:** TA chooses an arbitrary number b , calculates $E = h(b \oplus U_{pub})$ and transmits E to U_i and $\{T_u, b, UID_i\}$ to all SN_j 's over the insecure channel. T_u is the allocated time for which the user can fetch the data from SN_j .

4.1.4. Access control and encryption phase

After authentication, legal user will be allowed to access the data from SN_j for the limited time. Subsequent steps are executed in this phase:

- Step P1:** U_i implants USC_i and provides his/her UID_i and PWD_i , USC_i verifies whether entered credentials are same as stored. If true Step P2 will be executed.
- Step P2:** $C = h(a \parallel UID_i) \oplus E$ will be computed by USC_i , and a message containing $\{C, UID_i, T'\}$ will be transmitted to accessed nodes(SN).
- Step P3:** SN_j verifies $T_c - T' < \Delta T$ and $T_{now} = T_u$ upon receiving the message.

Step P4: SN computes $C' = h(a \parallel UID_i) \oplus h(b \oplus U_{pub})$ by using b received from TA. And checks if $C = C'$. If true, then data will be transmitted else algorithm ends.

Step P5: SN transmits requested data M to U_i by using the computation $M = m \oplus H_2(\hat{e}(U_{pub}, P_{pub}))$.

Step P6: U_i computes $M = m \oplus H_2(\hat{e}(U_{priv}, W))$ to get the original message.

4.2. Review of Challa et al.'s scheme

In this section, a review of the scheme by Challa et al [21], is presented. Challa et al.'s scheme consists of three entities Patients, Sensor Nodes (SN), and Trusted Authority (TA). System architecture considered is depicted in Fig. 2. A Patient, who is admitted in a hospital or healthcare, is equipped with the sensors/wireless monitoring devices. The base station requests the sensors to send the physiological data of the patient periodically; and on reception, uploads it to the hospital/care center server, so that the medical professionals can analyze it. Each user has to register with the TA and get valid smart-card based credentials to ensure that invalid user is not allowed to access data. The scheme consists of four phases, each phase is described in the subsequent subsections:

4.2.1. Setup phase

Following are the steps executed by the TA to setup the system:

Step P1: TA picks a larger prime number p , a base point P of order n from $E_p(a, b)$ over a finite field $\mathbb{Z}_p$, a secret master-key $S_0 \in \mathbb{Z}_p^*$, a one-way cryptographic hash function $h(\cdot)$ and computes $P_{pub} = S_0 \cdot P$.

Step P2: The fuzzy extractor was utilized to perform biometric authentication, which consists of a pair of functions (i) $Gen(\cdot)$ (probabilistic random generation function) and (ii) $Rep(\cdot)$ (deterministic function). Where $Gen(\cdot)$ takes users personal biometric as an input and yields the l bits long random biometric-key $\sigma_i \in \{0, 1\}^l$ along with reproduction (τ_i) parameter. Whereas, function $Rep(\cdot)$ takes users biometric and τ_i as an input for authentication and checks if the difference between old-biometric and new-biometric is $\leq$ than error tolerance threshold value (t). $Rep(\cdot)$ returns the value of genuine biometric as an output.

Step P3: Finally, TA kept the parameter S_0 private and $\{P_{pub}, P, t, p, h(\cdot), E_p(a, b), Rep(\cdot), Gen(\cdot)\}$ are announced publicly.

4.2.2. Sensor node pre-deployment phase

In this phase each SN_j is registered with the TA in the offline mode:

Step P1: TA chooses a unique identity SID_j , master secret-key $mk_j \in \mathbb{Z}_p^*$ for each SN_j and computes $S_j = h(SID_j || mk_j)$.

Step P2: Finally, TA stores $\{SID_j, S_j\}$ in its own database and in the memory of SN_j .

4.2.3. User registration phase

In this phase, the user is verified physically and then the user is registered with the TA by executing the following steps:

Step P1: U_i picks UID_i , an arbitrary number $K \in \mathbb{Z}_p^*$, computes $RID_i = h(K || UID_i)$ and transfers the request containing RID_i to the TA over a private channel.

Step P2: Next, TA calculates $R_i = h(RID_i || S_0)$ and saves it on USC_i , and transfers the USC_i to U_i via a private channel.

Step P3: U_i receives USC_i and picks a PWD_i , imprints BIO_i and calculates $Gen(BIO_i) = (\sigma_i, \tau_i)$, $RPW_i = h(PWD_i || K)$, $X_i = h(RPW_i || \sigma_i)$, $Y_i = h(UID_i || PWD_i || \sigma_i) \oplus K$, $R'_i = h(UID_i || \sigma_i) \oplus R_i$.

Step P4: To complete this step, U_i stores $\{Y_i, R'_i, X_i, \tau_i, Rep(\cdot), Gen(\cdot), h(\cdot), t\}$ in the USC_i and removes R_i from memory.

4.2.4. Login phase

Subsequent steps are executed by U_i , to login to the TA:

Step P1: U_i puts USC_i , enters his/her UID'_i , PWD'_i and imprints BIO'_i at the sensor of a particular terminal.

Step P2: USC_i calculates $R'_i = Rep(BIO'_i, \tau_i)$, $K' = Y_i \oplus h(UID'_i || PWD'_i || R'_i)$, $RPW'_i = h(PWD'_i || K')$ and $X'_i = h(RPW'_i || R'_i)$, and checks if $X'_i \stackrel{?}{=} X_i$ is true than Step P3 is executed else session terminates.

Step P3: U_i picks an arbitrary number $m \in \mathbb{Z}_p^*$ and current T_i . Further, U_i submits request message $\{DID_j, RID_i, V_i, M_i, T_i\}$ to TA, after computing $M_i = m \cdot P = (M_i^x, M_i^y)$, $N_i = m \cdot P_{pub} = (N_i^x, N_i^y)$, $RID'_i = h(K' || UID'_i)$, $DID_i = RID'_i \oplus N_i^y$, $DID_j = SID_j \oplus N_i^y$, $R'_i = R'_i \oplus h(UID'_i || R'_i)$, and $V_i = h(DID_i || DID_j || T_i || M_i || R'_i)$.

4.2.5. Authentication and key agreement phase

TA authenticates the U_i and mediates the establishment of session key between SN_j and U_i by implementing following procedure:

Step P1: Upon receiving the message from U_i , TA checks the condition $T'_i - T_i \leq \Delta T$. If true, then TA computes $N_{TA} = S_0 \cdot M_i = (N_{TA}^x, N_{TA}^y)$, $RID_i = DID_i \oplus N_{TA}^y$, $SID_j^* = DID_j \oplus N_{TA}^y$, $R_i = h(RID_i || S_0)$ and $V_i^* = h(DID_i || DID_j || T_i || M_i || R_i)$. TA validates the U_i 's authenticity by checking $V_i^* \stackrel{?}{=} V_i$ and verifies if SID_j^* is present in the database. If both conditions are true TA executes the Step P2, else the session is terminated.

Step P2: TA selects the present time-stamp T_{TA} and calculates $W_{TA} = h(R_i) \oplus h(S_j || T_{TA} || T_i)$, and transfers the message $\{W_{TA}, T_{TA}, T_i\}$ to SN_j via public channel.

Step P3: SN_j receives the message $\{W_{TA}, T_{TA}, T_i\}$ and checks the freshness by examining the condition $T'_{TA} - T_{TA} \leq \Delta T$. If true, SN_j selects the present time-stamp T_j and calculates $h(R_i) = h(S_j || T_{TA} || T_i) \oplus W_{TA}$, $SK_{ij} = h(SID_j || h(R_i) || h(S_j) || T_i || T_j)$, $V_{SN_j} = h(SK_{ij} || SID_j || T_j)$ and $W_j = h(S_j) \oplus h(SID_j || h(R_i))$. SN_j transfers the message $\{W_j, V_{SN_j}, T_j\}$ to U_i directly via public channel.

Step P4: U_i checks the freshness of the message $\{W_j, V_{SN_j}, T_j\}$ by checking the condition $T'_j - T_j \leq \Delta T$. If true U_i computes $h(S_j) = h(SID_j || h(R'_i)) \oplus W_j$, $SK'_{ij} = h(SID_j || h(R'_i) || h(S_j) || T_i || T_j)$ and $V'_{SN_j} = h(SK'_{ij} || SID_j || T_j)$. U_i checks if $V'_{SN_j} \stackrel{?}{=} V_{SN_j}$. If true, then U_i and SN_j have the session key $SK'_{ij} (= SK_{ij})$ else session terminates.

4.2.6. Credentials updation phase

This phase is executed locally by U_i without the involvement of the TA in the following manner:

Step P1: U_i provides the UID_i , PWD_i^{old} , BIO_i^{old} and USC_i computes $\sigma_i^{old} = Rep(BIO_i^{old}, \tau_i)$, $K' = h(UID_i || PWD_i^{old} || \sigma_i^{old}) \oplus Y_i$, $RPW_i^{old} = h(PWD_i^{old} || K')$, $X_i^{old} = h(RPW_i^{old} || \sigma_i^{old})$. USC_i examines the condition $X_i^{old} = X_i$, if true Step P2 is executed else session is terminated.

Step P2: USC_i permits U_i to enter new password PWD_i^{new} and imprint new biometrics BIO_i^{new} at the sensor of a specific terminal. USC_i then computes $Gen(BIO_i^{new}) = (\sigma_i^{new}, \tau_i^{new})$, $RPW_i^{new} = h(PWD_i^{new} || K')$, $X_i^{new} = h(RPW_i^{new} || \sigma_i^{new})$, $Y_i^{new} = K' \oplus h(UID_i || PWD_i^{new} || \sigma_i^{new})$, $R_i^{new} = (R'_i \oplus h(UID_i || \sigma_i^{old})) \oplus h(UID_i || \sigma_i^{new}) = R_i \oplus h(UID_i || \sigma_i^{new})$.

Step P3: The parameters $\{R'_i, X_i, Y_i, \tau_i\}$ on USC_i are replaced with R_i^{new} , X_i^{new} , Y_i^{new} , τ_i^{new} , respectively. Hence, the USC_i finally holds the information $\{R_i^{new}, X_i^{new}, Y_i^{new}, Gen(\cdot), Rep(\cdot), \tau_i^{new}, h(\cdot), t\}$.

4.2.7. User revocation phase

A legal user U_i can get a new smart-card USC_i^{new} if required by implementing following procedure:

Step P1: U_i provides the same identity UID_i , picks an arbitrary number $K^{new} \in \mathbb{Z}_p^*$ and transfers a registration request containing $RID_i^{new} = h(K^{new} || UID_i)$ to the TA over the secure channel.

Step P2: Next TA calculates and stores $R_i^{new} = h(RID_i^{new} || S_0)$ into the smart-card and transfers a USC_i^{new} to U_i over the private channel.

Step P3: U_i selects a new PWD_i^{new} , BIO_i^{new} and calculates $RPW_i^{new} = h(K^{new} || PWD_i^{new})$, $Gen(BIO_i^{new}) = (\sigma_i^{new}, \tau_i^{new})$, $X_i^{new} = h(RPW_i^{new} || \sigma_i^{new})$, $Y_i^{new} = K^{new} \oplus h(UID_i || PWD_i^{new} || \sigma_i^{new})$, $R'_i = R_i^{new} \oplus h(UID_i || \sigma_i^{new})$.

Step P4: Finally, the values $\{R'_i, X_i^{new}, Y_i^{new}, \tau_i, h(\cdot), t, Gen(\cdot), Rep(\cdot)\}$ are stored in U_i 's new USC_i^{new} and the TA delivers SC_i^{new} to U_i via secure channel.

4.2.8. Dynamic sensor node addition phase

Following steps executed by TA, depicts the dynamic deployment of a new sensor node SN_j^{new} in the existing network:

- Step P1:** For SN_j^{new} , the TA chooses a novel identity UID_j^{new} and a master secret key $mk_j^{new} \in \mathbb{Z}_p^*$. It then computes a secret value $S_j^{new} = h(SID_j^{new} || mk_j^{new})$.
- Step P2:** SID_j^{new} and S_j^{new} are then stored in SN_j^{new} 's memory before deploying in the sensor network. The TA also saves SID_j^{new} and S_j^{new} in its database.
- Step P3:** The TA also broadcasts the SN_j^{new} 's identity SID_j^{new} so that all users can access this sensor node.

5. Cryptanalysis of previous schemes

In this section previous schemes are critically reviewed to find their weakness:

5.1. Cryptanalysis of Liu-Chung's scheme

In this section, we will discuss a few limitations of Liu-Chung [15] scheme:

5.1.1. Leakage of user's private key

All the communication is happening on the public channel, an intruder $\mathcal{I}$ can intercept it when a user inserts its smart-card and enter UID_i , PWD_i , after verification a message $\{Sig, r, T_L, UID_i\}$ will be transmitted to the TA. $\mathcal{I}$ can compute users private key U_{priv} by adopting the following procedure:

- The $\mathcal{I}$ intercepts the message of U_i containing: $\{Sig, r, T_L, UID_i\}$.
- $\mathcal{I}$ computes r^{-1} .
- At last, the intruder computes the private key of the user as follow:
 $U_{priv} = Sig \cdot r^{-1}$, where $Sig = r \cdot U_{priv}$

5.2. User impersonation towards sensor node

In the Liu-Chung's scheme $\mathcal{I}$ can impersonate as a legal user towards sensor nodes and can access data from those. In the verification phase, TA sends the message containing E to the user, and $\langle T_u, \underline{b}, ID \rangle$ to all the sensor nodes via the open channel. The intruder can intercept both messages and save them. Later U_i sends a message containing $\langle C, ID, T' \rangle$ to sensor, where $C = h(a || ID) \oplus E$ and $h(a || ID)$ will remain same for all sessions. $\mathcal{I}$ can generate $E_{\mathcal{I}} = h(\underline{b} \oplus U_{pub})$ as U_{pub} is public and he/she knows $\underline{b}$. $\mathcal{I}$ can also compute $Z_{\mathcal{I}} = h(a || ID) = C \oplus E$. Then $\mathcal{I}$ can forge the entire message as follow:

- The $\mathcal{I}$ first computes $C_{\mathcal{I}}$: $C_{\mathcal{I}} = h(a || ID) \oplus E_{\mathcal{I}}$
- $\mathcal{I}$ will generate its own current timestamp T_A and will send the following message to sensor node impersonating as a U_i : $\langle C_{\mathcal{I}}, ID, T_{\mathcal{I}} \rangle$

5.3. Cryptanalysis of Challa et al.'s scheme

In this section, some potential shortcomings in Challa et al.'s [21] scheme are discussed:

5.3.1. Incorrectness of scheme

Challa et al.'s scheme also suffers from incorrectness [47], first User (U_i) gets authenticated from (TA), later TA sends a message to SN_j and SN_j communicates with U_i directly, but:

- No UID_i is exposed to SN_j .
- SN_j is sending message to U_i without knowing his UID_i .
- The message sent by SN_j does not contain address/identity of user.

5.3.2. Delay in communication

In the login and authentication phase, U_i needs to first verify itself with the TA to access SN_j . With the increase in the number of users, this will become the bottleneck for the whole system and will cause a delay.

5.3.3. Broadcast by trusted authority and sensor node

In Challa et al.'s scheme, TA sends a message containing $\{W_{TA}, T_{TA}, T_i\}$ to all the SN_j 's once it verifies the U_i . In this process, all of the SN_j 's will receive this message, because the message does not hold the address of intended sensor, neither sensors check whether message is meant for them, so all of the sensors will do the computation and will again broadcast the message containing $\{W_j, V_{SN_j}, T_j\}$. Due to this broadcasting, all of the other SN_j 's will process this login request, which can eventually drain the node's batteries. The issue with the sensor nodes is that they are equipped with limited battery power. Hence, security and energy efficiency become critical issues. Also, all of the users will receive this broadcast message from SN_j 's, hence involving the unintended users. This results in performance degradation and often causes network choking.

5.3.4. Lack of authentication between trusted authority and sensor node

During login and authentication phase TA sends the message $\langle W_{TA}, T_{TA}, T_i \rangle$ to SN_j . SN_j checks the freshness of timestamp and proceeds the computation, without further checking the authenticity of the received message. This deficit in authentication induces to reply, forgery, and DoS attack, as shown in the subsequent subsection.

5.3.5. Replay attack

In Challa et al.'s scheme, upon receiving the login message from TA, SN_j only verify the freshness of the timestamp. So the intruder ($\mathcal{I}$) will intercept and forge the message as described in the Section 1.1 by inserting the current timestamp and will retransmit the message. SN_j will verify the timestamps freshness by checking the condition $|T'_{TA} - T_{\mathcal{I}}| \leq \Delta T$ and this will be true because the adversary has inserted the fresh timestamp. Furthermore, the sensor will do further computation and sends the login message to the U_i .

- The $\mathcal{I}$ will intercept the message: $\langle W_{TA}, T_{TA}, T_i \rangle$
- The $\mathcal{I}$ will forge the message: $\langle W_{TA}, T_{\mathcal{I}}, T_i \rangle$
- The SN_j will check the following condition: $|T'_{TA} - T_{\mathcal{I}}| \leq \Delta T$
- As $T_{\mathcal{I}}$ is freshly generated, the condition in (c) will be true so SN_j will compute:

$$\begin{aligned} h(R_i) &= W_{TA} \oplus h(S_j || T_{\mathcal{I}} || T_i), \\ SK_{ij} &= h(SID_j || h(R_i) || h(S_j) || T_i || T_j), \\ V_{SN_j} &= h(SK_{ij} || SID_j || T_j), \\ W_j &= h(SID_j || h(R_i)) \oplus h(S_j) \end{aligned}$$

- Finally SN_j will send the following message to U_i :

$$\langle W_j, V_{SN_j}, T_j \rangle.$$

5.3.6. Denial of service (DoS) attack

Considering the timestamps are transmitted by an open channel, the $\mathcal{I}$ can effortlessly get hold of the timestamp values by eavesdropping the channel. As revealed in the Section 5.3.5 that timestamp value is hashed with additional parameters but never verified by SN_j , the attacker can transform the value $\{T_{TA}\}$. In the verification part of the authentication phase, the timestamp value will be different due to modification by the $\mathcal{I}$, but authentication will be succeeded. Hence, the scheme suffers from the DoS attack [47].

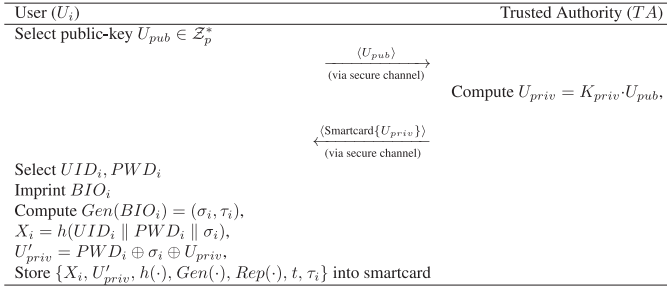


Fig. 3. User registration phase of proposed scheme.

5.3.7. Forgery attack

As revealed in Fig. 3 and 5.3.5 that SN_j does not verify the authenticity of message $\langle W_{TA}, T_{TA}, T_i \rangle$. The $\mathcal{I}$ will intercept the message and replace the parameters with some arbitrary parameters and will send a forged message say $\langle W'_{TA}, T'_{TA}, T'_i \rangle$ to SN_j . SN_j will simply validate the timestamp and will do the further computation and will send a message $\langle W_j, V_{SN_j}, T_j \rangle$ to U_i .

6. Proposed scheme

In subsequent subsections, the improved scheme with enhanced security is presented to overcome the deficiencies of Liu-Chung's and Challa et al.'s schemes.

6.1. Setup phase

Following are the steps performed by the TA in setup phase:

- Step P1** TA picks $E_p(a, b)$, base point P and a secret master key $K_{pri} \in \mathcal{Z}_p^*$.
- Step P2** TA chooses $h(\cdot)$ and computes $K_{pub} = K_{pri} \cdot P$ (public key).
- Step P3** The fuzzy extractor is selected to perform biometric authentication, which consists of a pair of functions (i) $Gen(\cdot)$ (probabilistic random generation function) and (ii) $Rep(\cdot)$ (deterministic function). Where $Gen(\cdot)$ takes users personal biometric as an input and yields the l bits long random biometric-key $\sigma_i \in \{0, 1\}^l$ along with τ_i a public reproduction parameter. Whereas, function $Rep(\cdot)$ takes users biometric and τ_i as an input for authentication and checks if the difference between old-biometric and new-biometric is $\leq$ than error tolerance threshold value (t). $Rep(\cdot)$ returns the value of genuine biometric as an output.
- Step P4** Finally, TA keeps K_{pri} private and publicizes $\{h(\cdot), p, E_p(a, b), K_{pub}, P, Rep(\cdot), Gen(\cdot), t\}$ are announced publicly.

6.2. Sink node pre-deployment registration phase

TA registers all SN_j 's in offline mode by adopting the following procedure:

- Step P1** TA picks a unique SID_j and a master-secret key MK_j for each SN_j and computes secret $S_j = h(SID_j \parallel MK_j)$.
- Step P2** TA chooses a unique public-key $SN_{pub_j} \in \mathcal{Z}_p^*$ for each sensor node, and computes a private-key $SN_{priv_j} = K_{priv} \cdot SN_{pub_j}$.
- Step P3** TA saves $\{SID_j, S_j\}$ in own database and $\{SID_j, S_j, SN_{pub_j}, SN_{priv_j}\}$ in SN_j 's memory before deployment in the target field.

6.3. User registration phase

To utilize available services U_i needs to be physically present in order to register with the TA. After successful registration U_i is

presented with a smart-card USC_i . This phase as illustrated in Fig. 3, is executed as follow:

- Step P1** U_i selects his/her public-key $U_{pub} \in \mathcal{Z}_p^*$ and sends registration request containing $\langle U_{pub} \rangle$ over a private channel.
- Step P2** Upon request TA calculates the U_i 's private key $U_{priv} = K_{priv} \cdot U_{pub}$ and stores into USC_i , and then sends USC_i to U_i over the private channel.
- Step P3** Next, U_i selects $\{UID_i, PWD_i\}$ pair and imprints his/her biometric BIO_i . USC_i then computes $Gen(BIO_i) = (\sigma_i, \tau_i)$, $X_i = h(UID_i \parallel PWD_i \parallel \sigma_i)$, $U'_{priv} = PWD_i \oplus \sigma_i \oplus U_{priv}$.
- Step P4** Finally U_i stores $\{X_i, U'_{priv}, h(\cdot), Gen(\cdot), Rep(\cdot), t, \tau_i\}$ into USC_i .

6.4. Login phase

The login and verification phases are also illustrated in Fig. 4. U_i adopts the subsequent procedure to login to the TA:

- Step P1** U_i inserts USC_i , provides his/her UID'_i, PWD'_i and imprints biometric BIO'_i .
- Step P2** USC_i computes $Rep(BIO'_i, \tau_i) = \sigma'_i$, $X_i = h(UID'_i \parallel PWD'_i \parallel \sigma'_i)$ and checks if $X'_i = X_i$ is true.
- Step P3** If the verification succeeds, then USC_i selects a random numbers $r_1 \in \mathcal{Z}_p^*$, generates current timestamp T_i and computes $M_i = r_1 \cdot P$, $N_i = r_1 \cdot P_{pub} = (N_i^x, N_i^y)$, $DID_i = UID'_i \oplus N_i^x$, $SID'_j = SID_j \oplus N_i^y$, $U_{priv} = PWD_i \oplus \sigma_i \oplus U'_{priv}$, $G_i = h(U_{priv} \parallel T_i \parallel N_i \parallel UID'_i)$, and sends a message containing $M_{sg1} = \langle G_i, SID'_j, DID_i, M_i, T_i \rangle$ to TA through open channel.

6.5. Verification phase

Upon receiving a login message from U_i , TA verifies the legality of U_i and helps to establish a session among SN_j and U_i . This phase completes by executing following steps:

- Step P1** TA first checks the freshness of M_{sg1} by verifying the condition $T_c - T_i \leq \Delta T$. If condition holds TA calculates $N_{ta} = K_{priv} \cdot M_i = (N_{ta}^x, N_{ta}^y)$, $U_{priv} = K_{priv} \cdot U_{pub}$, $UID'_i = DID_i \oplus N_{ta}^x$, $SID_j = SID'_j \oplus N_{ta}^y$, and $G_i \stackrel{?}{=} h(U_{priv} \parallel T_i \parallel N_{ta} \parallel UID'_i)$. If Condition holds and SID_j is registered, then TA will proceed to next step else session will be terminated.
- Step P2** TA chooses the temporary-identity TID_i , current timestamp T_{ta} and session-validity period T_{sv} for i th user. After this TA will compute the following $W = h(SID_j \parallel S_j \parallel T_{ta})$, $U'_{pub} = U_{pub} \oplus S_j \oplus T_{ta}$, $TID'_i = TID_i \oplus S_j \oplus T_{ta}$, $T'_{sv} = T_{sv} \oplus S_j \oplus T_{ta}$ and sends the message $M_{sg2} = \langle SID_j, TID'_i, W, U'_{pub}, T_{sv}, T_{ta} \rangle$ to SN_j .
- Step P3** After sending the message to SN_j , TA will compute $Y_s = h(SID_j \parallel S_j \parallel T_{ta} \parallel TID'_i)$, $V = h(N_{ta} \parallel U'_{priv} \parallel UID_i \parallel T_{ta} \parallel T_{sv})$, $TID'_i = TID_i \oplus U'_{priv} \oplus N_{ta}^x$, and send the message $M_{sg3} = \langle Y_s, V, TID'_i, T_{sv}, T_{ta} \rangle$ to U_i via open channel.
- Step P4** After receiving the message M_{sg2} from TA, SN_j will first check if $T_c - T_i \leq \Delta T$ and $W \stackrel{?}{=} h(SID_j \parallel S_j \parallel T_{ta})$. If both conditions are true, then SN_j will compute the following $TID_i = TID'_i \oplus S_j \oplus T_{ta}$, $U_{pub} = U'_{pub} \oplus S_j \oplus T_{ta}$, and $T_{sv} = T'_{sv} \oplus S_j \oplus T_{ta}$. Finally, SN_j will store the following into the memory $\langle TID_i, T_{sv}, U_{pub} \rangle$.
- Step P5** Upon receiving message M_{sg3} from TA, U_i first checks the transmission delay $T_c - T_{TA} \leq \Delta T$ and $V \stackrel{?}{=} h(N_i \parallel U_{priv} \parallel UID_i \parallel T_{ta} \parallel T_{sv})$, if both conditions hold U_i will compute

User (U_i)	Trusted Authority (TA)	Sensor Node (SN_j)
Enter UID'_i , PWD'_i and imprint BIO'_i Compute $Rep(BIO'_i, \tau_i) = \sigma'_i$ $X'_i = h(UID'_i \parallel PWD'_i \parallel \sigma'_i)$ if $X'_i \stackrel{?}{=} X_i$ then Choose $r_1 \in \mathcal{Z}_p^*$, T_i and compute $M_i = r_1 \cdot P$ $N_i = r_1 \cdot K_{pub} = (N_i^x, N_i^y)$ $SID'_j = SID_j \oplus N_i^y$ $DID_i = UID'_i \oplus N_i^x$ $U_{priv} = PWD'_i \oplus \sigma'_i \oplus U'_{priv}$ $G_i = h(U_{priv} \parallel T_i \parallel N_i \parallel UID'_i)$ (1) $\xrightarrow[M_{sg1} = \langle G_i, SID'_j, DID_i, M_i, T_i \rangle]{\text{via open channel to TA}}$	Check $T_c - T_i \leq \Delta T$ and compute $N_{ta} = K_{priv} \cdot M_i = (N_{ta}^x, N_{ta}^y)$ $SID_j = SID'_j \oplus N_{ta}^y$ $U_{priv} = K_{priv} \cdot U_{pub}$ $UID'_i = DID_i \oplus N_{ta}^x$ $G_i \stackrel{?}{=} h(U_{priv} \parallel T_i \parallel N_{ta} \parallel UID'_i)$ Choose TID_i , T_{ta} , T_{sv} Compute $W = h(SID_j \parallel S_j \parallel T_{ta} \parallel T_{sv})$ $U'_{pub} = U_{pub} \oplus S_j \oplus T_{ta}$ $TID'_i = TID_i \oplus S_j \oplus T_{ta}$ (2) $\xrightarrow[M_{sg2} = \langle SID_j, TID'_i, W, U'_{pub}, T_{sv}, T_{ta} \rangle]{\text{via open channel to } SN_j}$	Check $T_c - T_{ta} \leq \Delta T$ and compute $W \stackrel{?}{=} h(SID_j \parallel S_j \parallel T_{ta})$ $TID_i = TID'_i \oplus S_j \oplus T_{ta}$ $U_{pub} = U'_{pub} \oplus S_j \oplus T_{ta}$ $T_{sv} = T'_{sv} \oplus S_j \oplus T_{ta}$ Store $\{TID_i, T_{sv}, U_{pub}\}$ into memory
Check $T_c - T_{ta} \leq \Delta T$ and compute $V \stackrel{?}{=} h(N_i \parallel U_{priv} \parallel UID_i \parallel T_{ta} \parallel T_{sv})$ $TID_i = TID'_i \oplus U_{priv} \oplus N_i^x$ $Y'_s = Y_s \oplus \sigma'_i \oplus PWD'_i$ Store $\{Y'_s, T_{sv}, TID_i\}$ into smartcard	(3) $\xleftarrow[M_{sg3} = \langle Y_s, V, TID'_i, T_{sv}, T_{ta} \rangle]{\text{via open channel to } U_i}$	

Fig. 4. Summary of login and authentication phase of proposed scheme.

$TID_i = TID'_i \oplus U_{priv} \oplus N_i^x$, $Y'_s = Y_s \oplus \sigma'_i \oplus PWD'_i$. Finally, U_i will store $\{Y'_s, T_{sv}, TID_i\}$ into smart-card.

6.6. Access control and encryption phase

Once U_i is authenticated, he can access SN_j for time-bound access of data, collected by SN_j by completing following steps, which are also summarized in Fig. 5:

- Step P1** U_i inserts USC_i , enters his/her UID'_i , PWD'_i and imprints biometric BIO'_i .
- Step P2** USC_i computes $Rep(\sigma'_i) = (\sigma'_i, \tau_i)$, $X'_i = h(UID'_i \parallel PWD'_i \parallel \sigma'_i)$ and checks if $X'_i = X_i$ is true.
- Step P3** If the verification succeeds, then USC_i will generate the timestamp T_i and will compute $Y_s = Y'_s \oplus \sigma'_i \oplus PWD'_i$, $Y_i = h(Y_s \parallel T_i)$ and will send the request containing $\langle Y_i, TID_i, SID_j, T_i \rangle$ to SN_j via open channel.
- Step P4** Upon receiving a message SN_j checks $T_c - T_i \leq \Delta T$ and $T_{sv} < T_c$ and will check if TID_i has permission to access the sensor.
- Step P5** If the antecedent three conditions are true than, sensor-node will check another condition $Y \stackrel{?}{=} h(h(SID_j \parallel S_j \parallel T_{ta} \parallel TID_i) \parallel T_i)$, if true session will continue else terminated.
- Step P6** Than SN_j will generate the current timestamp T_{sn} , and will compute the following $B_{pj} = \hat{e}(U_{pub}, S_i \cdot P_{pub})$, $M = m \oplus h(B_{pj} \parallel T_{sn})$, $Z = h(m \parallel B_{pj} \parallel T_{sn})$. Finally SN_j sends the response containing the following $\langle TID_i, SID_j, M, Z, T_{sn} \rangle$ to U_i via open channel.
- Step P7** Upon receiving the message U_i will check if $T_c - T_{sn} \leq \Delta T$, if verification succeeds U_i will get the message by following method $B_{pi} = \hat{e}(U_{priv}, S_p)$, $m = M \oplus h(B_{pi} \parallel T_{sn})$

User (U_i)	Sensor Node (SN_j)
Enter UID'_i , PWD'_i and imprint σ'_i , Compute $Rep(\sigma'_i) = (\sigma'_i, \tau_i)$, $X'_i = h(UID'_i \parallel PWD'_i \parallel \sigma'_i)$, if $X'_i \stackrel{?}{=} X_i$ then Generate timestamp T_i $Y_s = Y'_s \oplus \sigma'_i \oplus PWD'_i$ $Y_i = h(Y_s \parallel T_i)$ (1) $\xrightarrow[\text{via open channel to } SN_j]{\text{request}(\langle Y_i, TID_i, SID_j, T_i \rangle)}$	If $T_c - T_i \leq \Delta T$ and $T_{sv} \leq T_c$, then, Check if TID_i has access $Y \stackrel{?}{=} h(h(SID_j \parallel S_j \parallel T_{ta} \parallel TID_i) \parallel T_i)$ Generate T_{sn} , and compute $B_{pj} = \hat{e}(U_{pub}, S_i \cdot P_{pub})$, $M = m \oplus h(B_{pj} \parallel T_{sn})$, $Z = h(m \parallel B_{pj} \parallel T_{sn})$ (2) $\xleftarrow[\text{via open channel}]{\text{response}(\langle TID_i, SID_j, M, Z, T_{sn} \rangle)}$
If $T_c - T_{sn} \leq \Delta T$ then Compute $B_{pi} = \hat{e}(U_{priv}, S_p)$ $m = M \oplus h(B_{pi} \parallel T_{sn})$ $Z \stackrel{?}{=} h(m \parallel B_{pi} \parallel T_{sn})$ If true, accept the data, else, discard	

Fig. 5. Access control and encryption phase of proposed scheme.

and checks the following condition $Z \stackrel{?}{=} h(m \parallel B_{p_i} \parallel T_{sn})$, if true message will be kept else discarded.

6.7. User credentials update phase

U_i can execute this phase without mediation of TA to reduce the communication cost and to off-load TA. The steps involve in this phase are as follow:

- Step P1** U_i inserts USC_i , enters his/her UID_i , PWD_i^{old} and imprints biometric BIO_i^{old} .
- Step P2** USC_i computes $Rep(BIO_i^{old}, \tau_i) = \sigma_i^{old}$, $X_i^{old} = h(UID_i \parallel PWD_i^{old} \parallel \sigma_i^{old})$ and if $X_i^{old} \stackrel{?}{=} X_i$ is true than next step will be executed else the process will be terminated.
- Step P3** USC_i authorizes the U_i to select a new password PWD_i^{new} and to imprints new BIO_i^{new} at the sensor of specific terminal. USC_i then computes $Gen(BIO_i^{new}) = \sigma_i^{new}$, τ_i^{new} , $X_i^{new} = h(UID_i \parallel PWD_i^{new} \parallel \sigma_i^{new})$, $U_{priv}^{new} = (PWD_i^{old} \oplus \sigma_i^{old} \oplus U_{priv}') \oplus (PWD_i^{new} \oplus \sigma_i^{new}) = U_{priv} \oplus PWD_i^{new} \oplus \sigma_i^{new}$.
- Step P4** Finally USC_i replaces $\{X_i, U_{priv}', \tau_i\}$ with $\{X_i^{new}, U_{priv}^{new}, \tau_i^{new}\}$. Hence the smart-card USC_i finally contains the information $\{X_i^{new}, U_{priv}^{new}, h(\cdot), Gen(\cdot), Rep(\cdot), t, \tau_i^{new}\}$.

6.8. New user addition, revocation and re-registration phase

For the lost/stolen card and for new user registration, the user can accomplish it in the following manner:

- Step P1** User U_i selects his/her public-key $U_{pub}^{new} \in \mathcal{Z}_p^*$ and sends registration request containing (U_{pub}^{new}) to TA over a secure channel.
- Step P2** TA computes the $U_{priv}^{new} = K_{priv} \cdot U_{pub}^{new}$, and stores U_{priv}^{new} into the new smart-card USC_i^{new} . TA then sends the USC_i^{new} to the user U_i over a secure channel.
- Step P3** Upon receiving new smart-card user enters his/her old identity UID_i , selects new PWD_i^{new} and imprints new biometric BIO_i^{new} . U_i then computes $Gen(BIO_i^{new}) = (\sigma_i^{new}, \tau_i^{new})$, $X_i^{new} = h(UID_i \parallel PWD_i^{new} \parallel \sigma_i^{new})$, $U_{priv}^{new'} = PWD_i^{new} \oplus \sigma_i^{new} \oplus U_{priv}^{new}$.
- Step P4** Finally, the values $\{X_i^{new}, U_{priv}^{new'}, h(\cdot), Gen(\cdot), Rep(\cdot), t, \tau_i\}$ are stored into the new smart-card USC_i^{new} .

6.9. Dynamic sensor node addition phase

Sometimes, a new sensor may be added to the network to replace the exhausted or stolen sensor. To add a new sensor SN_j^{new} , TA executes the following steps offline:

- Step P1** The TA chooses new and unique SID_j^{new} and a master-secret key MK_j^{new} for each sensor node SN_j^{new} . The TA also computes a secret-value $S_j^{new} = h(SID_j^{new} \parallel MK_j^{new})$.
- Step P2** TA chooses a unique public-key $SN_{pub_j}^{new} \in \mathcal{Z}_p^*$ for each sensor node, and computes a private-key $SN_{priv_j}^{new} = K_{priv} \cdot SN_{pub_j}^{new}$.
- Step P3** The TA stores $\{SID_j^{new}, S_j^{new}\}$ in its database and $\{SID_j^{new}, S_j^{new}, SN_{pub_j}^{new}, SN_{priv_j}^{new}\}$ in SN_j 's memory before deployment in the target field. The TA also broadcasts the newly added sensor SN_j^{new} 's identity SID_j^{new} to all users, so that they can access it.

Notation	Meaning
$A \models B$	A believes a statement B
$A \xrightarrow{K} Y$	Share a key K between A and Y
$\#B$	B is fresh
$A \triangleleft B$	A sees B
$A \sim B$	A said B
$(B, C)_K$	B, C is hashed by key K
$\{B\}_K$	B is hashed with key K
$< B >_K$	B is encrypted with key K

Fig. 6. BAN logic notations.

Rule	Meaning
$\frac{A \models A \xrightarrow{K} Y, A \triangleleft < B >_K}{A \models Y \mid \sim K}$	Message-meaning rule
$\frac{A \models \#B, A \models Y \mid \sim B}{A \models Y \mid \sim K}$	Nonce-verification rule
$\frac{A \models B, A \models C}{A \models (B, C)}$	Belief Rule
$\frac{A \models \#B, A \models C}{A \models \#(B, C)}$	Fresh conjuncatenation rule
$\frac{A \models Y \Rightarrow B, A \models Y \mid \sim B}{A \models B}$	Jurisdiction rule

Fig. 7. Postulates for BAN logic.

7. Security analysis

The security analysis: 1) formal, 2) automated as well as 3) informal of the proposed is accomplished in this section.

7.1. Formal analysis

For formal analysis purposes, the widely accepted Burrows Abadi Needham (BAN) logic method is adopted [48]. The notation guide for BAN logic analysis is given in Fig. 6.

7.1.1. Postulates for BAN logic

Some of the logical postulates of BAN logic and the meaning related to the postulates are given below in Fig. 7:

7.1.2. Security goal establishment

Established security goal is as follows:.

$$G_1: U_i \models SN_j \mid \equiv U_i \xrightarrow{m} SN_j$$

7.1.3. Messages generic form

Following are the idealized transformation of our introduced scheme:

$$Msg_1: SN_j \rightarrow U_i: \{TID_i, SID_j, m \oplus h(B_{p_j} \parallel T_{sn}), h(m \parallel B_{p_j} \parallel T_{sn}), T_{sn}\}$$

7.1.4. Messages idealized form

Following are the idealized transformation of our introduced scheme:

$$Msg_1: SN_j \rightarrow U_i: (U_i \xrightarrow{TID_i} SN_j, U_i \xrightarrow{SID_j} SN_j, \langle m \rangle_{U_i \xrightarrow{B_{p_j}} SN_j}, T_{sn}, \langle m, T_{sn} \rangle_{U_i \xrightarrow{B_{p_j}} SN_j}, T_{sn})$$

7.1.5. Assumptions

- A1: $|U_i| \equiv \#(T_{sn})$
 A2: $|SN_j| \equiv \#(T_i)$
 A3: $|U_i| \equiv (U_i \xleftrightarrow{SID_j} SN_j)$
 A4: $|SN_j| \equiv (U_i \xleftrightarrow{SID_j} SN_j)$
 A5: $|U_i| \equiv (U_i \xleftrightarrow{TID_i} SN_j)$
 A6: $|SN_j| \equiv (U_i \xleftrightarrow{TID_i} SN_j)$
 A7: $|U_i| \equiv SN_j \Rightarrow SN_j \sim X$
 A8: $|U_i| \equiv SN_j \Rightarrow (U_i \xrightarrow{m} SN_j)$
 A9: $|U_i| \equiv (U_i \xleftrightarrow{B_{pj}} SN_j)$
 A10: $|SN_j| \equiv (U_i \xleftrightarrow{B_{pj}} SN_j)$

7.1.6. Proposed schemes proof

S_1 : From Msg_1 , we get

$$U_i \triangleleft (U_i \xleftrightarrow{TID_i, SID_j} SN_j, \langle m, T_{sn} \rangle \xleftrightarrow{B_{pj} SN_j}, T_{sn}, T_{sn})$$

S_2 : Based on Assumption A3, A6, S_1 and message-meaning rule, we get

$$|U_i| \equiv SN_j \mid \sim \langle m, T_{sn}, T_{sn} \rangle$$

S_3 : Based on Assumption A1, S_2 , Freshness rule and Nonce verification rule, we get

$$|U_i| \equiv SN_j \mid \equiv \langle m \rangle$$

S_4 : Based on Assumption A7, S_3 and Jurisdiction rule, we get

$$|U_i| \equiv \langle m \rangle$$

S_5 : Based on Assumption A5, A8, S_4 and Belief rule, we get

$$|U_i| \equiv SN_j \mid \equiv U_i \xrightarrow{m} SN_j$$

7.2. Informal security analysis of the proposed scheme

Following subsections describe the resistance of the proposed scheme against some known attack along with some security features extended by the same:

7.2.1. Privileged-insider attack

In the proposed scheme, the TA does not store any critical information relating to the user password or private key in the verifier database. Therefore, even if a privileged-insider gets/steals user smart card, he cannot guess user password or private key $\langle U_{priv} \rangle$. Therefore, he has no advantage over ordinary attackers to break the robustness of the proposed scheme.

7.2.2. Impersonation attacks

Let $\mathcal{I}$ be an intruder and he intercepts the login message M_{sg1} of user U_i . $\mathcal{I}$ may try to generate fake login message to impersonate as U_i . To do this $\mathcal{I}$ can generate its own message by selecting random numbers $r_1^{\mathcal{I}}$, $\mathcal{I}$ may try to compute $M_i^{\mathcal{I}} = r_1^{\mathcal{I}} \cdot P$, $N_i = r_1^{\mathcal{I}} \cdot K_{pub}$, $G_i^{\mathcal{I}} = h(U_{priv} \parallel T_i^{\mathcal{I}} \parallel N_i^{\mathcal{I}} \parallel UID_i^{\mathcal{I}})$, $SID_j^{\mathcal{I}} = SID_j \oplus N_i^{y_{\mathcal{I}}}$, $UID_i^{\mathcal{I}} = UID_i^{\mathcal{I}} \oplus N_i^{x_{\mathcal{I}}}$; however, for this $\mathcal{I}$ needs to know r_1 , UID_i , PWD_i , N_i , K_{priv} and U_{priv} in order to successfully login.

7.2.3. Offline password guessing attack

Let $\mathcal{A}$ gets access to data $\{X_i, U'_{priv}, h(\cdot), Gen(\cdot), Rep(\cdot), t, \tau_i\}$ stored in U_i 's smart-card USC_i . It is still computationally infeasible for the $\mathcal{A}$ to compute UID_i , PWD_i and U_{priv} of U_i . Hence, guessing password in offline method is no advantageous in proposed scheme.

7.2.4. Stolen smart-card attack

Let $\mathcal{A}$ has access to data $\{X_i, U'_{priv}, h(\cdot), Gen(\cdot), Rep(\cdot), t, \tau_i\}$ stored in stolen/lost smart card of U_i . However, due to hash functions one-way property $\mathcal{A}$ cannot extract any sensitive information.

7.2.5. Replay attack

Due to the current timestamps of U_i , TA, and SN_j in login and authentication messages, $\mathcal{I}$ cannot reply to the previous message. Also, the timestamp is hashed and Exclusive or ($\oplus$) with other parameters. Furthermore, transmission delay ΔT is sufficiently small to stop reply. Hence the attacker cannot pass the authentication test by transmitting replayed messages.

7.2.6. Denial-of-service attack

Due to local authentication of user U_i by checking condition $X'_i = X_i$, login request is sent to TA only after correct UID_i , PWD_i and BIO_i . So due to this scheme is secure against denial-of-service attack.

7.2.7. Mutual authentication

TA authenticates user with the condition $G_i \stackrel{?}{=} h(U_{priv} \parallel T_i \parallel N_{ta} \parallel UID_i')$, and U_i also authenticates the TA by checking $V \stackrel{?}{=} h(N_i \parallel U_{priv} \parallel UID_i \parallel T_{ta} \parallel T_{sv})$. SN_j and U_i also authenticate each other with the help of trusted authority, by checking the conditions $Y \stackrel{?}{=} h(h(SID_j \parallel S_j \parallel T_{ta} \parallel TID_i) \parallel T_i)$ and $Z \stackrel{?}{=} h(m \parallel B_{pi} \parallel T_{sn})$. $\mathcal{A}$ requires the knowledge of U_{priv} , N_i , UID_i , K_{priv} to construct these.

7.2.8. User anonymity

It's difficult for $\mathcal{I}$ to identify/distinguish user as U_i 's identity UID_i is masked in each phase. Also for each session new random numbers r_1 is chosen by U_i to compute N_i , so $DID_i' = UID_i' \oplus N_i^x$ is new for each session. Therefore, user anonymity as well as untraceability is extended by proposed scheme.

7.3. AVISPA Simulation

In extension to the informal and formal security analysis, we present the simulation results for the proposed scheme by employing the broadly trusted automated tool Automated Validation of Internet Security Protocols and Applications (AVISPA) [49]. Based on High-Level Protocol Specification Language (HLPSP), AVISPA can validate the security of the under investigation protocols. Using OFMC and CL-AtSe backend [50] for the formal security verification, we have implemented our protocol in the HLPSP language. Figs. 8–10 provide role specification of user, sensor and TA; respectively, along with session, goal and environment role specifications in Fig. 11. The simulation results depicted in Figs. 12 and Fig. 13 reveal that the proposed scheme fulfills the design requirements and is safe against the replay as well as man-in-the-middle attack. In the OFMC backend, a total of 400 nodes were searched in 5.38 s with a depth of 9 piles. The CL-AtSe backend analyzed 5372 states the translation and computation taken for this backend are 0.35 s and 0.12 s, respectively.

8. Performance analysis

In this section, the comparison among the proposed and few recent schemes presented in [15,21,33,51] is performed taking into account communication and computation overheads.

8.1. Security requirements

Proposed schemes security requirement is listed in Table 2 against schemes which are already developed [15,21,33,51]. Here “ I_n ” is a particular security requirement/ feature, ($\checkmark$) tells if a feature is present in a scheme and ($\times$) tells if a scheme lacks a particular feature.

```

role role_USERS (USERS, TA, SENSOR:agent, Skui:symmetric_key, Kpub:
:public_key, H:hash_func, SND, RCV:channel (dy))
played_by USERS
def=
local
  State:nat,
  Upub:public_key,
  Rl,Mi,Ni,Gi,Ti,Tta,Yi,Nta,Sj,Tsv,Ys,Tsn,TIDi,Bpj,P,Kpriv,
  UIDi,SIDj,DIDi,Message:text,
  F:hash_func
init
  State := 0
transition
  1. State=0
    /\ RCV(start) => State':=1
    /\ Upub':=new()
    /\ SND({Upub'}_Skui)
  2. State=1
    /\ RCV({F(Kpriv.Upub)}_Skui) => State':=2
    /\ secret(Kpriv,sec_l,{TA})
    /\ Rl':=new() /\ Ti':=new() /\ Mi':=F(Rl'.P)
    /\ Ni':=F(Rl'.F(Kpriv.P))
    /\ Gi':=H(H(F(Kpriv.Upub).Ti'.Ni'.UIDi))
    /\ SIDj':=xor(SIDj,Ni') /\ DIDi':=xor(UIDi,Ni')
    /\ SND(Gi'.SIDj'.DIDi'.Mi'.Ti')
    /\ witness(USERS,TA,user_ta_ti,Ti')
    /\ witness(USERS,TA,user_ta_rl,Rl')
  5. State=2
    /\ RCV(H(SIDj.Sj'.Tta'.TIDi').H(Nta'.F(Kpriv.Upub).UIDi
    .Tta'.Tsv').xor(xor(TIDi',F(Kpriv.Upub)),Nta').Tsv'.Tta')
    => State':=3 /\ request(USERS,TA,user_ta_tta,Tta')
    /\ request(USERS,TA,user_ta_tsv,Tsv')
    /\ request(USERS,TA,user_ta_tidi,TIDi')
    /\ Ti':=new() /\ Yi':=H(H(SIDj.Sj'.Tta'.TIDi').Ti')
    /\ SND(Yi'.TIDi'.SIDj.Ti')
  7. State=3
    /\ RCV(TIDi.SIDj.xor(Message',H(Bpj'.Tsn'))).H(Message'
    .Bpj'.Tsn') => State':=4
    /\ request(USERS,SENSOR,user_sensor_tsn,Tsn')
end role
c@FancyV

```

Fig. 8. Role specification for the U_i .

```

role role_SENSOR (SENSOR,USERS,TA:agent,Kpub:public_key,H:hash_
func,SND,RCV:channel(dy))
played_by SENSOR
def=
local
  State:nat,
  Upub:public_key,
  TTIDi,Sj,SIDj,Tsn,Z,Tta,Tsv,Ti,Ys,TIDi,Bpj,M,Message:text,
  SNjpub:public_key,
  Bilinear,Product,F:hash_func
init
  State := 0
transition
  4. State=0
    /\ RCV(SIDj.xor(xor(TTIDi',Sj'),Tta').H(SIDj.Sj'.Tta'
    .Tsv').xor(xor(Upub,Sj'),Tta').Tsv'.Tta') => State':
    =1
    /\ request(SENSOR,TA,sensor_ta_tta,Tta')
    /\ request(SENSOR,TA,sensor_ta_tsv,Tsv')
    /\ request(SENSOR,TA,sensor_ta_tidi,TIDi)
  6. State=1
    /\ RCV(H(H(SIDj.Sj'.Tta'.TIDi').Ti').TIDi'.SIDj.Ti')
    => State':=2
    /\ Bpj':=Bilinear(Upub.Product(SNjpub.Kpub))
    /\ Message':=new()
    /\ Tsn':=new()
    /\ M':=xor(Message',H(Bpj'.Tsn'))
    /\ Z':=H(Message'.Bpj'.Tsn')
    /\ SND(TIDi'.SIDj.M'.Z'.Tsn')
    /\ witness(SENSOR,USERS,user_sensor_tsn,Tsn')
end role
c@FancyV

```

Fig. 9. Role specification for the SN_j .

```

role role_TA (TA,USERS,SENSOR:agent,Skui:symmetric_key,Kpub:
public_key,H:hash_func,SND,RCV:channel(dy))
played_by TA
def=
local
  State:nat, Upub:public_key, MKj,TTIDi,W,UUpub,TTTIDi,V,
  Rl,Mi,Ni,Gi,Ti,Tta,Nta,Sj,Tsv,Ys,Tsn,TIDi,Bpj,P,Kpriv,
  UIDi,SIDj,DIDi,Message:text,
  F:hash_func
init
  State := 0
transition
  1. State=0
    /\ RCV({Upub'}_Skui) => State':=1
    /\ secret(Kpriv,sec_l,{TA})
    /\ SND({F(Kpriv.Upub')}_Skui)
  3. State=1
    /\ RCV(H(F(Kpriv.Upub).Ti'.Ni'.UIDi).xor(SIDj,Ni').xor(UIDi
    ,F(Rl'.F(Kpriv.P)).F(Rl'.P).Ti') => State':=2
    /\ request(TA,USERS,user_ta_ti,Ti')
    /\ request(TA,USERS,user_ta_rl,Rl')
    /\ secret(Kpriv,sec_l,{TA}) /\ TIDi':=new()
    /\ Tta':=new() /\ Sj':=H(SIDj.MKj)
    /\ Tsv':=new() /\ TTTIDi':=xor(xor(TTIDi',Sj'),Tta')
    /\ W':=H(SIDj.Sj'.Tta'.Tsv')
    /\ UUpub':=xor(xor(Upub,Sj'),Tta)
    /\ SND(SIDj.TTIDi'.W'.UUpub'.Tsv'.Tta')
    /\ witness(TA,SENSOR,sensor_ta_tta,Tta')
    /\ witness(TA,SENSOR,sensor_ta_tsv,Tsv')
    /\ witness(TA,SENSOR,sensor_ta_tidi,TIDi')
    /\ Nta':=F(Kpriv.F(Rl'.P))
    /\ Ys':=H(SIDj.Sj'.Tta'.TIDi')
    /\ V':=H(Nta'.F(Kpriv.Upub).UIDi.Tta'.Tsv')
    /\ TTTIDi':=xor(xor(TIDi',F(Kpriv.Upub)),Nta')
    /\ SND(Ys'.V'.TTTIDi'.Tsv'.Tta')
    /\ witness(TA,USERS,user_ta_tta,Tta')
    /\ witness(TA,USERS,user_ta_tidi,TIDi')
end role
c@FancyV

```

Fig. 10. Role specification for the TA .

```

role session (USERS,TA,SENSOR:agent,Skui:symmetric_key,Kpub:
public_key,H:hash_func)
def=
local
  SND3,RCV3,SND2,RCV2,SND1,RCV1:channel(dy)
composition
  role_SENSOR (SENSOR,USERS,TA,Kpub,H,SND3,RCV3)
  /\ role_TA (TA,USERS,SENSOR,Skui,Kpub,H,SND2,RCV2)
  /\ role_USERS (USERS,TA,SENSOR,Skui,Kpub,H,SND1,RCV1)
end role
role environment ()
def=
const
  users,ta,sensor:agent,tsn,tta,ti,const_l:text,
  skui:symmetric_key,kpub:public_key,h:hash_func,
  sec_l,sec_2,sec_3,user_ta_tta,user_ta_rl,user_ta_tsv,user_
  ta_tidi,user_ta_ti,sensor_ta_tta,sensor_ta_tsv,sensor_ta_t
  di,user_sensor_tsn:protocol_id
intruder_knowledge = {h,ti,tta,tsn}
composition
  session(users,ta,sensor,skui,kpub,h)
  /\ session(i,ta,sensor,skui,kpub,h)
  /\ session(users,i,sensor,skui,kpub,h)
  /\ session(users,ta,i,skui,kpub,h)
end role
goal
  secrecy_of sec_l,sec_2,sec_3
  authentication_on user_ta_tta
  authentication_on user_ta_tsv
  authentication_on user_ta_tidi
  authentication_on sensor_ta_tta
  authentication_on sensor_ta_tsv
  authentication_on sensor_ta_tidi
  authentication_on user_sensor_tsn
  authentication_on user_ta_ti
  authentication_on user_ta_rl
end goal
environment ()
c@FancyVerbLi

```

Fig. 11. Role specification for session, goal and environment.

```

% OFMC
% Version of 2006/02/13

SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/MA_AC.if

GOAL
as_specified
BACKEND
OFMC
COMMENTS

STATISTICS
parseTime: 0.00s
searchTime: 5.38s
visitedNodes: 400 nodes
depth: 9 plies
c@FancyVerbLine

```

Fig. 12. The result of the analysis using OFMC backend of our scheme.

```

% CL-ATSE
SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL

PROTOCOL
/home/span/span/testsuite/results/MA_AC.if

GOAL
As Specified

BACKEND
CL-AtSe

STATISTICS

Analysed      : 5372 states
Reachable     : 662 states
Translation: 0.35 seconds
Computation: 0.12 seconds

```

Fig. 13. The result of the analysis using CL-AtSe backend of our scheme.

8.2. Communication overhead comparison

The communication overhead comparison is depicted in Table 3. For comparison purposes, we assume: the user identity is 128 bits, sensor node identity is 16 bits, random number is 128 bits, timestamp is 32 bits, hash digest is 160 bits and cost for ECC point $P = (P_x, P_y)$ is $(160 + 160) = 320$ bits, respectively.

Under these deliberations, the messages sent throughout the login and authentication phase $M_{sg1} = \langle G_i, SID'_j, DID_i, M_i, T_i \rangle$, $M_{sg2} = \langle SID_j, TID'_i, W, U'_{pub}, T_{sv}, T_{ta} \rangle$, $M_{sg3} = \langle Y_s, V, TID''_i, T_{sv}, T_{ta} \rangle$ need 832 bits, 560 bits and 544 bits respectively. Combining all these costs, the whole communication cost in the proposed scheme

Table 2
Comparison of functionality features.

	[15]	[33]	[21]	[51]	Our
I_1	×	✓	✓	✓	✓
I_2	×	✓	✓	✓	✓
I_3	×	✓	✓	✓	✓
I_4	×	✓	✓	✓	✓
I_5	✓	×	×	✓	✓
I_6	×	✓	✓	✓	✓
I_7	×	×	✓	✓	✓
I_8	×	✓	✓	✓	✓
I_9	✓	✓	×	✓	✓
I_{10}	×	×	×	✓	✓
I_{11}	×	✓	✓	✓	✓
I_{12}	×	✓	✓	×	✓
I_{13}	×	×	✓	×	✓
I_{14}	✓	×	×	×	✓
I_{15}	✓	✓	×	✓	✓

Note: I_1 : user anonymity property; I_2 : privileged-insider attack; I_3 : off-line password guessing attack; I_4 : stolen smart-card attack; I_5 : denial-of-service attack; I_6 : known session key attack; I_7 : impersonation attack; I_8 : man-in-the middle attack; I_9 : replay attack; I_{10} : mutual authentication; I_{11} : session key agreement; I_{12} : BAN logic analysis; I_{13} : AVISPA validation; I_{14} : Provides access control to sensor node; I_{15} : Forgery attack.

Table 3
Comparison of communication overhead.

Scheme	# of messages	# of bits
Liu-Chung (L&A phase) [15]	3	928
Liu-Chung (AC&E phase) [15]	2	480
Wu et al. [33]	2	1712
Arshad-Nikooghadam [51]	3	1792
Challa et al. [21]	3	1428
Proposed (L&A phase)	3	1936
Proposed (AC&E phase)	2	832

Table 4
Approximate time required for various operations [53].

Notation	Description	computation time(ms)
T_h	Hash function	0.0023
T_{ecm}	ECC point multiplication	2.226
T_{sym}	Symmetric enc/dec	0.0046
T_m	Modular multiplication	0.0288
T_{bp}	Bilinear pairing	5.811
T_{fe}	Fuzzy extractor function	2.226

throughout the login and authentication phase becomes 1,936 bits. Also the messages send during access control and encryption phase $\langle Y_i, TID_i, SID_j, T_i \rangle$ and $\langle TID_i, SID_j, M, Z, T_{sn} \rangle$ need 336 bits and 496 bits. Combining all, the total communication overhead for access control and encryption phase is 832 bits. In the proposed scheme during the login and authenticate phase, three messages are exchanged between the parties at the communication cost of 1936 bits and during the access control and encryption phase U_i and SN_j communicates directly with overhead of 832 bits as long as the session is valid.

8.3. Computation overhead comparison

As discussed in [52], computation time required for the hash is 0.0023 ms, for ECC point multiplication 2.226 ms, for bilinear pairing 5.811 ms, for fuzzy extractor 2.226 ms and symmetric enc/dec requires the 0.0046 ms. Using the argument presented in [53], the running time for the fuzzy extractor function is considered same as that for T_{ecm} , that is, $T_{fe} \approx T_{ecm} = 2.226$ ms. Table 4 depicts the no-

Table 5
Comparison of computation overhead.

Protocol	User side	TA/Server side	Sensor node side	Total overhead
Liu-Chung (L&A phase) [15]	$1T_h + 1T_{ecm}$	$1T_h + 2T_{bp}$	-	$1T_{ecm} + 2T_h + 2T_{bp} \approx 13.8256$
Liu-Chung (AC&E phase) [15]	$2T_h + 1T_{bp} + 1T_{ecm}$	-	$3T_h + 1T_{bp} \approx 5.8179$	$1T_{ecm} + 5T_h + 2T_{bp} \approx 13.8595$
Wu et al. [33]	$2T_{ecm} + 2T_{sym} + 5T_h + 1T_{fe}$	$2T_{ecm} + 2T_{sym} + 6T_h$	-	$4T_{ecm} + 4T_{sym} + 11T_h + 1T_{fe} \approx 11.1737$
Arshad-Nikooghadam [51]	$2T_{ecm} + 1T_m + 8T_h$	$2T_{ecm} + 1T_m + 1T_{inv} + 8T_h$	-	$4T_{ecm} + 2T_m + 1T_{inv} + 15T_h \approx 8.9961$
Challa et al. [21]	$2T_{ecm} + 11T_h + 1T_{fe}$	$1T_{ecm} + 4T_h$	$6T_h \approx 0.0138$	$3T_{ecm} + 21T_h + 1T_{fe} \approx 8.9523$
Proposed (L&A phase)	$2T_{ecm} + 3T_h + 1T_{fe}$	$1T_{ecm} + 4T_h$	$1T_h \approx 0.0023$	$3T_{ecm} + 8T_h + 1T_{fe} \approx 8.9224$
Proposed (AC&E phase)	$4T_h + 1T_{fe} + 1T_{bp}$	-	$4T_h + 1T_{bp} \approx 5.8202$	$8T_h + 1T_{fe} + 2T_{bp} \approx 13.8664$

tation and running time of each cryptographic primitive as per the experiment conducted in [52]. In Table 5, we have compared the proposed scheme with some related schemes for computation cost incurred during the login and authentication phase and access and control phase. In the proposed scheme U_i initiates login and authentication, in response, a session establishes with the computation cost of ≈ 8.9224 ms and after this U_i and SN_j can communicate directly with the computation cost of ≈ 13.8664 ms as long as the session is valid.

9. Conclusion

In this paper, a secure three-factor (smart-card, biometric, password) authentication scheme for WSNs has been proposed to overcome the pitfalls in Liu-Chung and Challa et al.'s schemes. After briefly investigating the above-mentioned schemes some drawbacks have been observed such as users private key leakage in Liu-Chung's scheme and the incorrectness, delay in communication, along with related weaknesses in Challa et al.'s scheme. To overcome the drawbacks, we proposed an enhanced three-factor based authentication scheme. BAN logic and AVISPA tool are used for formal analysis. Through informal security analysis, it is argued that our scheme is secure against various kind of attacks. Moreover, performance analysis of proposed scheme along with other related schemes is furnished in the context of communication and computation costs. It is evident from performance and analysis that the proposed scheme is more secure and performs better than related schemes in computation overheads. Therefore, the proposed scheme can extend low cost, more security benefit in sensitive healthcare applications.

Declaration of Competing Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:[10.1016/j.jisa.2020.102502](https://doi.org/10.1016/j.jisa.2020.102502).

References

- [1] Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. Wireless sensor networks: a survey. *Comput Netw* 2002;38(4):393–422.
- [2] Gautam KK, Gautam NK, Agrawal DP. Memory required for wireless sensor nodes on the basis of characteristics and behaviour when using TinyOS. *Int J Emerg Technol Adv Eng* 2014;4(1):26–34.
- [3] Galar D, Kumar U. Chapter 1 - sensors and data acquisition. eMaintenance. Galar D, Kumar U, editors. Academic Press; 2017. <https://doi.org/10.1016/B978-0-12-811153-6.00001-4>. ISBN 978-0-12-811153-6, p. 1–72.
- [4] Wang B. Coverage problems in sensor networks: a survey. *ACM Comput Surv* 2011;43(4) 32:1–32:53. doi:[10.1145/1978802.1978811](https://doi.org/10.1145/1978802.1978811).
- [5] Pramanik PKD, Nayyar A, Pareek G. Wban: driving e-healthcare beyond telemedicine to remote health monitoring: architecture and protocols. In: *Telemedicine technologies*. Elsevier; 2019. p. 89–119.
- [6] Ghamari M, Janko B, Sherratt RS, Harwin WS, Piechockic R, Soltanpur C. A survey on wireless body area networks for healthcare systems in residential environments. *Sensors* 2016;16(6):831. <https://academic.microsoft.com/paper/2412353053>
- [7] Pramanik PKD, Pal S, Mukhopadhyay M. Healthcare big data: a comprehensive overview. In: *Intelligent systems for healthcare management and delivery*. IGI Global; 2019. p. 72–100.
- [8] Pramanik PKD, Upadhyaya BK, Pal S, Pal T. Internet of things, smart sensors, and pervasive systems: enabling connected and pervasive healthcare. In: *Healthcare data analytics and management*. Elsevier; 2019. p. 1–58.
- [9] Latré B, Braem B, Moerman I, Blondia C, Demeester P. A survey on wireless body area networks. *Wirel Netw* 2011;17(1):1–18. doi:[10.1007/s11276-010-0252-4](https://doi.org/10.1007/s11276-010-0252-4).
- [10] Teshome AK, Kibret B, Lai DTH. A review of implant communication technology in wban: progress and challenges. *IEEE Rev Biomed Eng* 2019;12:88–99.
- [11] Parihar N. A review paper on healthcare and hospital monitoring system using wireless sensor network. *Int J Comput Sci Mob Comput* 2019;8(1):62–8.
- [12] Gogate U, Bakal J. Refining healthcare monitoring system using wireless sensor networks based on key design parameters. In: *Information and communication technology for intelligent systems*. Springer; 2019. p. 341–9.
- [13] Zhang Y, Sun L, Song H, Cao X. Ubiquitous WSN for healthcare: recent advances and future prospects. *IEEE Internet Things J* 2014;1(4):311–18.
- [14] Ko J, Lu C, Srivastava MB, Stankovic JA, Terzis A, Welsh M. Wireless sensor networks for healthcare. *Proc IEEE* 2010;98(11):1947–60.
- [15] Liu C-H, Chung Y-F. Secure user authentication scheme for wireless healthcare sensor networks. *Comput Electr Eng* 2017;59:250–61.
- [16] Ng H, Sim M, Tan C. Security issues of wireless sensor networks in healthcare applications. *BT Technol J* 2006;24(2):138–44.
- [17] Darwish A, Sayed GI, Hassanien AE. The impact of implantable sensors in biomedical technology on the future of healthcare systems. *Intelligent pervasive computing systems for smarter healthcare*; 2019.
- [18] Wang D, Wang P, Chenyu W. Efficient multi-factor user authentication protocol with forward secrecy for real-time data access in WSNs, vol. 3. ACM; 2019. p. 1–25.
- [19] Shi E, Perrig A. Designing secure sensor networks. *IEEE Wirel Commun* 2004;11(6):38–43.
- [20] Nidhya R, Karthik S. Security and privacy issues in remote healthcare systems using wireless body area networks. In: *Body area network challenges and solutions*. Springer; 2019. p. 37–53.
- [21] Challa S, Das AK, Odelu V, Kumar N, Kumari S, Khan MK, et al. An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. *Comput Electr Eng* 2018;69:534–54.
- [22] Dolev D, Yao A. On the security of public key protocols. *IEEE Trans Inf Theory* 1983;29(2):198–208.
- [23] Eisenbarth T, Kasper T, Moradi A, Paar C, Salmasizadeh M, Shalmani MTM. On the power of power analysis in the real world: a complete break of the KeeLoq code hopping scheme. In: *Annual international cryptography conference*. Springer; 2008. p. 203–20.
- [24] Yang W-H, Shieh S-P. Password authentication schemes with smart cards. *Comput Secur* 1999;18(8):727–33.
- [25] Hölbl M, Welzer T, Brumen B. An improved two-party identity-based authenticated key agreement protocol using pairings. *J Comput Syst Sci* 2012;78(1):142–50.
- [26] Kocher P, Jaffe J, Jun B. Differential power analysis. In: *Annual international cryptography conference*. Springer; 1999. p. 388–97.
- [27] Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans Comput* 2002;51(5):541–52.
- [28] Smys S, Kumar AD. Secured WBANs for pervasive m-healthcare social networks. In: *Intelligent systems and control (ISCO), 2016 10th international conference on*. IEEE; 2016. p. 1–4.
- [29] Shen J, Chang S, Shen J, Liu Q, Sun X. A lightweight multi-layer authentication protocol for wireless body area networks. *Future Gener Comput Syst* 2018;78:956–63.
- [30] Liu X, Jin C, Li F. An improved two-layer authentication scheme for wireless body area networks. *J Med Syst* 2018;42(8):143.
- [31] Amin R, Islam SH, Biswas G, Khan MK, Kumar N. A robust and anonymous patient monitoring system using wireless medical sensor networks. *Future Gener Comput Syst* 2018;80:483–95.

- [32] Ali R, Pal AK, Kumari S, Sangaiah AK, Li X, Wu F. An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring. *J Ambient Intell Humaniz Comput* 2018;1–22.
- [33] Wu F, Xu L, Kumari S, Li X. A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks. *Comput Electr Eng* 2015;45:274–85.
- [34] Xie Q, Tang Z, Chen K. Cryptanalysis and improvement on anonymous three-factor authentication scheme for mobile networks. *Comput Electr Eng* 2017;59:218–30.
- [35] Chaudhry SA, Naqvi H, Khan MK. An enhanced lightweight anonymous biometric based authentication scheme for TMIS. *Multimed Tools Appl* 2018;77(5):5503–24.
- [36] Chaudhry SA, Mahmood K, Naqvi H, Khan MK. An improved and secure biometric authentication scheme for telecare medicine information systems based on elliptic curve cryptography. *J Med Syst* 2015;39(11):175.
- [37] Chaudhry SA, Khan MT, Khan MK, Shon T. A multiserver biometric authentication scheme for TMIS using elliptic curve cryptography. *J Med Syst* 2016;40(11):230.
- [38] Chaudhry S, Naqvi H, Shon T, Sher M, Farash M. Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems. *J Med Syst* 2015;39(6):66.
- [39] Khan I, Chaudhry SA, Sher M, Khan JI, Khan MK. An anonymous and provably secure biometric-based authentication scheme using chaotic maps for accessing medical drop box data. *J Supercomput* 2018;74(8):3685–703.
- [40] Chen C-M, Xiang B, Liu Y, Wang K-H. A secure authentication protocol for internet of vehicles. *IEEE Access* 2019;7:12047–57.
- [41] Chen C-M, Wang K-H, Yeh K-H, Xiang B, Wu T-Y. Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications. *J Ambient Intell Humaniz Comput* 2019;10(8):3133–42.
- [42] Hussain S, Chaudhry SA. Comments on biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment. *IEEE Internet Things J* 2019;6(6):10936–40.
- [43] Irshad A, Usman M, Ashraf Chaudhry S, Naqvi H, Shafiq M. A provably secure and efficient authenticated key agreement scheme for energy internet based vehicle-to-grid technology framework. *IEEE Transactions on Industry Applications* 2020. doi:10.1109/TIA.2020.2966160. 1–1
- [44] Zhang Y, He D, Huang X, Wang D, Choo K-KR, Wang J. White-box implementation of the identity-based signature scheme in the IEEE P1363 standard for public key cryptography. *IEICE Trans Inf Syst* 2019;1(99):1–8. doi:10.1587/transinf.2019INP0004.
- [45] Shamir A. Identity-based cryptosystems and signature schemes. In: *Workshop on the theory and application of cryptographic techniques*. Springer; 1984. p. 47–53.
- [46] Boneh D, Franklin M. Identity-based encryption from the weil pairing. In: *Annual international cryptology conference*. Springer; 2001. p. 213–29.
- [47] Chaudhry SA, Shon T, Al-Turjman F, Alsharif MH. Correcting design flaws: an improved and cloud assisted key agreement scheme in cyber physical systems. *Comput Commun* 2020;153:527–37. doi:10.1016/j.comcom.2020.02.025.
- [48] Burrows M, Abadi M, Needham RM. A logic of authentication. *Proc R Soc London A* 1989;426(1871):233–71.
- [49] Armando A, Basin D, Cuellar J, Rusinowitch M, Viganò L. AVISPA: automated validation of internet security protocols and applications. *ERCIM News* 2006;64(January).
- [50] Basin D, Mödersheim S, Viganò L. OFMC: a symbolic model checker for security protocols. *Int J Inf Secur* 2005;4(3):181–208.
- [51] Arshad H, Nikooghadam M. Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems. *J Med Syst* 2014;38(12):136.
- [52] Kilinc HH, Yanik T. A survey of sip authentication and key agreement schemes. *Commun Surv Tutorials IEEE* 2014;16(2):1005–23.
- [53] He D, Kumar N, Lee J-H, Sherratt RS. Enhanced three-factor security protocol for consumer USB mass storage devices. *IEEE Trans Consum Electron* 2014;60(1):30–7.