IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 14, 2018, accepted November 1, 2018, date of publication November 9, 2018,
date of current version December 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2880225

An Enhanced Symmetric Cryptosystem and Biometric-Based Anonymous User Authentication and Session Key Establishment Scheme for WSN

MAJID ALOTAIBI
Department of Computer Engineering, College of Computer and Information Systems, Umm al-Qura University, Mecca, Saudi Arabia
(e-mail: mmgethami@uqu.edu.sa)

ABSTRACT Wireless sensor networks (WSNs) are progressive ad hoc networks that comprise of distributed sensors that are typically and randomly deployed over the target region. The valuable information from the sensor nodes is allowed to access with the help of gateway node by the registered user. To ensure secure communication, a session key is exchanged between the participants over the insecure channel. In this paper, we identified some deficiencies in Jung et al.'s scheme and then devised an enhanced biometric-based anonymous user authentication and the key agreement scheme that is also embedded with symmetric cryptosystem for WSNs. The advantage of using biometric login is to ensure the legal user's efficient login. We conferred about preserving the security of our proposed scheme, we primarily applied formal verification BAN-logic method to check the exactness of mutual authentication. Furthermore, used automated validation of internet security protocols and applications software that is widely accepted and its results confirm that our scheme is secure against active and passive attacks, including forgery, replay, and man-in-the-middle attack. In addition, an informal analysis proves our scheme can withstand various possible attacks on authentication protocols over the insecure channel. Furthermore, our scheme is more appropriate for WSNs based upon the comparison of computational efficiency and security requirements with recent results.

INDEX TERMS Authentication, wireless sensor networks, biometrics, forgery, security, privacy.

I. INTRODUCTION

These days witness a tremendous development in Wireless Sensor Networks (WSNs). They are used in various fields for different purposes due to their advancements in hardware technology and software skills. The unattended environment where the sensor nodes are deployed along with the unreliable wireless communication offered in WSNs and the peculiar characteristics owned by WSNs pertains security relevant issues to many applications of WSNs. It is essential to ensure security services for the applications of WSNs to achieve all the benefits faultlessly. In general, WSNs consisting of users, gateways, and sensors which is the generally spreading progression, where the users are doubtlessly permitted to get to the hoped sensor's to acquire the information and further they are allowed to access the nodes as shown in the Fig. 1. Further, when sensor networks are used for applications such as monitoring and continuous tracking in surveillance, it is necessary to report event information securely and accurately in a timely manner to the respective authorities. When WSNs are used for these applications sensor nodes frequently suffer from different types of attacks such as eavesdropping, intercepting, data manipulating, replay attack, impersonation attack, and attacks denying the event reports from reaching the Gateway nodes (GWN). Hence it is necessary to design secure communication schemes to get rid of these attacks or to mitigate the impact of these attack on WSNs applications. Although WSNs perform important functions in numerous application fields, the drawbacks of the network are evident. First, WSNs are often deployed in unattended environments [1], [2] or enemy-controlled environments. Therefore, the networks are effortlessly controlled. Second, given their characteristics, WSNs consist of numerous resource-constrained nodes. The fundamental impediment focuses are as per the following [3]:

1. The transmission of WSNs is unreliable due to their deployment in the harsh environment, short transmission range, and the low data-transfer rate with high energy cost consumptions.

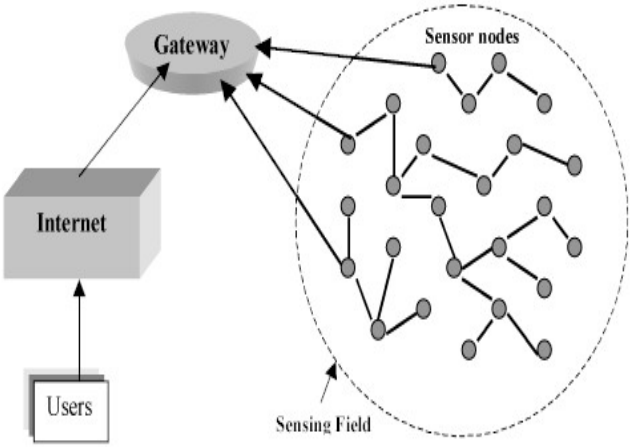

FIGURE 1. WSN architecture.

2. The modern-day sensor nodes are embedded with a small battery power due to their small size. Due to the deployment of WSNs in a hostile environment; thus, energy appurtenance is impracticable.
3. The computation cost and storage capacity is limited due to the technicality of sensor nodes.

Making the information accessible to the users who sits in remote locations, and request for completed the framework must ensure the mutual approval prior empowering the users to get to the real-time information. The low-entropy human-memorable passwords are often cased the security weakness in the two-factor authentication protocols as they are selected from the small pool of dictionary and sometimes stored in smartcards or the servers. These low-entropy passwords can be obtained in polynomial time, which gives an advantage to the attacker in guessing the user's passwords. This shows, reliability and preservation of high sensitive information which deals with security, the two-factor based methods are proven inefficient. Thus, three-factor authentication system is merely suggested in designing the authentication and key agreement for the remote user authentication. Furthermore, these three-factor methods efficiently tackle the password guessing attack [4], [38], [39].

Based on the design methodology discussed by [5] and [6] and considering the security features and attributes into account as discussed by [7], we understand there is a serious need of utilizing the three-factor adoptability. Interested readers can go through the detailed case study on biometrics modality discussed by [8], where they have discussed the various biometric extraction error comparisons of false match rate and false non-match rate.

The benefits of adapting three-factor facility are arranged as follows:

1) Biometric keys cannot be forgotten or lost.
2) Guessing of biometric information is infeasible.
3) Transmitting the biometric keys either by copying or sharing is very difficult.
4) Forgery of biometric keys is extremely hard.

There are many advantages and disadvantages in considering/using the WSN. They are listed as follows:

Advantages:

- Network setups can be carried out without fixed infrastructure.
- Suitable for the non-reachable places such as over the sea, mountains, rural areas or deep forests.
- Flexible if there is random situation when additional workstation is needed.
- Implementation pricing is cheap.
- It avoids plenty of wiring.
- It might accommodate new devices at any time.
- It's flexible to undergo physical partitions.
- It can be accessed by using a centralized monitor.

Disadvantages:

- Less secure because hackers can enter the access point and obtain all the information.
- Lower speed as compared to a wired network.
- More complicated to configure compared to a wired network.
- Easily troubled by surroundings (walls, microwave, large distances due to signal attenuation, etc).
- It is easy for hackers to hack it we couldn't control propagation of waves.
- Comparatively low speed of communication.
- Gets distracted by various elements like Blue-tooth.
- Still Costly (most importantly)

A. RELATED WORKS

In 2011, [9] proposed an ECC-based two-factor authentication scheme which seems to be well equip design. But, due to the design flaw such as the erroneous presentation of mutual authentication between the user and sensor, their scheme is proven insecure. To enhance and correct Yeh *et al.*'s scheme, [10] demonstrated an improved version of [9]'s scheme which aims to resist more security attributes and performs with minimal cost computational and communicational overhead. Furthermore, In 2014, [11] analyzed [10] scheme and proven [10]'s scheme faulty due to the stolen/lost smartcard attack, key-share attack, and exhaustive sensor energy attack. As a part of correcting scheme, Shi and Gong [10] presented enhanced authentication protocol. In the same year, [12] exhibited with a public key version using ECC was proposed in order to efficiently tackle untraceability and perfect forward secrecy.

Moreover, [13], [14], [15] shown that [16] proposal is faulty and couldn't handle the security features effectively such as user anonymity, insider attack, session key agreement, mutual authentication, and also password guessing attack. [17] demonstrated [11], [18] schemes which were meant to handle the security features efficiently but they were also proven faulty such as user anonymity attack, offline guessing attack, de-synchronization, lack of strong forward security, and forgery attack. As a remedy, Wu *et al.* comeup with a proposal with formal verification proof to enhance the security for wireless sensor networks.

In a recent advancement, [19] proposed a scheme for WSN with the symmetric cryptosystem. To strengthen their proposal, they claimed that their scheme has the potential to withstand the different variants of attacks. Furthermore, after studying and done an analysis of [19] scheme, [20] shown the faults in Chen *et al.*'s design which fails to resist smart card loss attack, and denial of service attack, due to their inefficient verification method. In addition, Chen *et al.*'s scheme fails to provide user anonymity as the identity of the user is transmitted in a plaintext form during login request. Moreover, due to the delay in detecting the incorrect login credentials such as password, Chen *et al.*'s scheme wastes the resources of the user and also sensor nodes in both communication and computational overheads costs.

B. MOTIVATIONS AND CONTRIBUTION

Reference [20] chooses to improve [19]'s design in which an anonymous user tries to authentication with the credentials provided by the gateway node and then the sensor node computes a valid session key which is agreed to be used in further communications among the communicated parties. They have finely presented their proposal and to strengthen their proposal they claimed that their scheme could withstand the security requirements such as smart card loss attacks [21], password guessing attacks [6], user impersonation attacks [7], replay attacks [22], privileged-insider attacks [30], etc. They also claimed that their scheme was highly efficient and very suited to WSN environments.

Firstly, after a thorough study of [20], during our examination it is observed that their proposal is still faulty and failed to handle password guessing attack, forgery attack, user traceability attack. Moreover, the privacy of the session key is not considered in their scheme, as a consequence, an active insider can extract the session key and impose false computations. Furthermore, due to the dynamic nature of the WSNs, their scheme fails to support node addition facility.

Second, as a remedy, we present an efficient user authentication and key agreement scheme with the capabilities of resisting the password guessing attack and forgery attack. The correctness of our scheme is presented using BAN-logic to ensure the restriction of mutual authentication, and replay attack. With the adoptability of AVISPA, which is a suitable formal security method to prove our scheme resists all the security attributes. To strengthen our discussion, with the help of informal security analysis, we proved our scheme handles the security features well and ensures the security. Furthermore, the detailed discussion on computational performance and security analysis of proposed scheme is given.

C. PAPER OUTLINE

A brief mathematical preliminaries are discussed in Section II. In Section III, we discussed Jung *et al.*'s scheme. In Section IV, we discussed the shortcomings of Jung *et al.*'s scheme. In Section V, we suggested the necessary counter measures to restrict the attacks in Jung *et al.*'s scheme. In Section VI, a new user authentication scheme is discussed. In Section VII, a formal analysis BAN-logic proof to demonstrate the mutual authentication, AVISPA tool to check the replay and man-in-the-middle attacks, and informal security analysis are presented. Section VIII gives a comparative analysis of the proposed scheme with other schemes. Finally, the paper is concluded in Section IX.

II. MATHEMATICAL PRELIMINARIES

A. BIOMETRICS AND FUZZY EXTRACTOR

Biometric verification allows one to confirm or establish an individual's identity. As statistical information regarding biometric input is unpredictable, designing cryptographic solutions for securing each scenario is tedious. Converting biometric data to uniform reproducible random strings that can for example, be used as a secret key is therefore necessary. Fuzzy extractors are a pair of functions where one function generates the uniform random bits from given input while the other recovers the string from an input close to the original input within a predefined threshold. Mathematically, the function pair in a fuzzy extractor is as follows:

Gen: is probabilistic generation function accepts the input Bio which is the personal biometrics information of the user, and in return it gives $\sigma \in \{0,1\}^l$ as the biometric key with the bit length l.

Rep: is a deterministic function which accepts the input in the form of the user biometrics, say Bio' and τ as the public reproduction parameter, considering the Hamming distance $(Bio', Bio) < t$, where t is an error tolerance threshold value. The output is the original biometric key $\sigma = Rep(Bio', \tau)$.

Using the fuzzy extractor technique, local biometric verification is performed in our scheme.

B. NOTATIONS AND RULES OF BAN-LOGIC

To verify the correctness of our AKA protocol we employ BAN-logic [24]. Here, all the participating parties during their communication undergo the verification of the transmitted messages: a legitimate user U_i and an opted sensor node SN_j agree upon a fresh shared session key. This happens when the scheme is executed and the legitimacy of the participants is verified. The notations of the BAN-logic are presented in Table 1.

We present the rules of BAN-logic as shown in Table 2, in order to present the logical posits in the formal terms [6], [24]:

C. ADVERSARY/THREAT MODEL

This section deals with the necessary characteristics and assumptions, including the attacker's capabilities in WSNs environment.

(1) As the entire communication takes place on insecure channel, an attacker possess the capability to intercept or modify any messages that are transmitted among the parties over public channel [6], [11].

(2) The transmitted messages can be eavesdropped by an attacker [25], [26].

TABLE 1. Notations of BAN-logic.

Symbol		Description
$M \mid\equiv X$	:	The principal M believes the announcement X.
$M \triangleleft X$	:	M considers X, which means that a message containing X is received by M where X can be read by M.
$M \mid\sim X$	:	M sometime stated X, which means that $M \mid\equiv X$ as M once stated it in sometime.
$M \mid\Rightarrow X$	:	M commands X, M has complete authority on X, and M considers X as trusted (Jurisdiction over X).
$\sharp(X)$	:	The message X is fresh, which means that no any entity sent a message containing X at whenever ahead of current round.
$M \mid\equiv N \overset{SK}{\longleftrightarrow} M$	:	M and N use SK (shared key) to communicate with each other.
$M \overset{SK}{\longleftrightarrow} N$	:	M and N use SK as a shared secret between them.
$< X >_Y$	:	The formula X is combined with the formula Y.
(X)	:	The formula X is hashed value.
(X, Y)	:	The formulas X and Y are combined and hashed .
$(X, Y)_k$	:	The formulas X and Y are combined and then hashed with the key k.

TABLE 2. Rules of BAN-logic.

Rules		Functionality Description
Message meaning rule	:	$\frac{M \mid\equiv N \overset{k}{\longleftrightarrow} M, M \triangleleft \{X\}_k}{M \mid\equiv N \mid\sim X}$.
Nonce verification rule	:	$\frac{M \mid\equiv \sharp(X), M \mid\equiv N \mid\sim X}{M \mid\equiv N \mid\equiv X}$.
Jurisdiction rule	:	$\frac{M \mid\equiv N \mid\equiv X, M \mid\equiv N \mid\Rightarrow X}{M \mid\equiv X}$.
Freshness rule	:	$\frac{M \mid\equiv \sharp(X)}{M \mid\equiv \sharp(X, Y)}$.
Belief rule	:	$\frac{M \mid\equiv N \mid\equiv (X, Y)}{M \mid\equiv N \mid\equiv (X)}$.
Session key rule	:	$\frac{M \mid\equiv \sharp(X), M \mid\equiv N \mid\equiv X}{M \mid\equiv M \overset{k}{\longleftrightarrow} N}$.

(3) By applying the power consumption analysis on the captured smartcards, an attacker can extract the valuable information stored on the smartcard [27], [41].
(4) Though the gateway nodes is secure, an attacker has the potential to capture the sensor node physically, due to the hostile environments [30].
(5) The low-entropy passwords and identities can be guessed in an off-line manner by an attacker [22], [40], [57].

III. REVIEW OF JUNG *et al.*'s scheme

A. USER'S REGISTRATION PHASE

A newly joined user U_i wishes to register with gateway to get the services. The details of this phase are as follows:

Reg1: The new user U_i chooses his ID_i, and PW_i. Computes a masked password $\overline{PW_i} = h(PW_i \| b)$ using the random nonce b. Further, sends $< ID_i, \overline{PW_i} >$ to GWN as a request message for the registration over a secure channel.

Reg2: The GWN computes $v = h(x_a), N_i = h(ID_i \| \overline{PW_i}) \oplus v$ and $M_i = h(\overline{PW_i} \| v)$, after getting the parameters from user. Moreover, stores the parameter v into its database. Then the parameters $\{N_i, M_i, h(\cdot)\}$ are stored into smart card memory and transmit it to the user over the secure channel .

Reg3: U_i stores b to the smart card's memory.

TABLE 3. Notations and their meanings.

Symbol	Description
U_i	i^{th} remote user
S_n	communicated sensor node
GWN	Gateway node (base station) in WSN
SC_i	Smartcard of user U_i
ID_i, PW_i	Identity and Password of user U_i
SID_n	Identity of sensor node S_n
x_a	The secret parameter generated by the GWN, $(U_i \overset{x_a}{\longleftrightarrow} GWN)$
x_s	The shared key between the GWN and S_n
$\mathcal{A}$	Attacker/Adversary
$h(\cdot)$	One-way hash function
R_i	Extracted string
B_i	Biometric characteristic
P_i	Auxiliary string
ΔT	Time interval for the allowed transmission delay
T_c	Time when a message received by an entity
SK	Session key shared between U_i and S_n
k	Symmetric key
E_k/D_k	Encryption/Decryption using symmetric key
$\alpha \| \beta$	Concatenation of data α with data β
$\alpha \oplus \beta$	Exclusive-OR of data α and data β

B. LOGIN AND AUTHENTICATION PHASES

The registered user U_i wishes to get some services from the sensor nodes. But, before that the validity of the user's credentials are verified on the basis of smartcard parameters and user's login credentials. The details of this phase is as follows:

L1 : U_i inputs his login credentials identity ID_i and password PW_i into the smartcard reader. Then computes the masked $\overline{PW_i}^* = h(PW_i \| b)$, $v* = h(ID_i \| \overline{PW_i}^*) \oplus N_i$.

L2 : Further computes, $M_i^* = h(\overline{PW_i}^* \| v^*)$. Verifies if $M_i \overset{?}{=} M_i*$ this hold with the stored value of smart card. Otherwise, terminates the process.

L3 : The smart card generates a random nonce R_1 and computes $DID_i = h(ID_i \| R_1)$, $k = h(DID_i \| v^* \| T_1)$ and $A_i = E_k(DID_i, R_1, T_1)$, where T_1 is the current timestamp.

L4 : U_i transmit the message $\{DID_i, A_i, T_1\}$ to the GWN.

A1 : GWN checks the timestamp's freshness T_1 as $|T_1' - T_1| < \Delta T$. On successful, GWN computes $k = h(DID_i \| h(x_a) \| T_1)$ and $D_k(A_i) = \{DID_i, R_1, T_1\}$. GWN verifies DID_i, T_1 with the received values. If succeed, GWN acknowledge the legitimacy of U_i and proceed with the next step. Otherwise, the process is terminated.

A2 : GWN selects a random nonce R_2 and computes $M_i = h(x_s \| SID_n) \oplus R_2$, $SK = h(DID_i \| h(x_s \| SID_n) \| R_2 \| T_2)$, and $B_i = h(DID_i \| SK \| h(x_s \| SID_n) \| SID_n \| T_2)$. Then, transmits the message $\{M_i, DID_i, B_i, T_2\}$ to S_n over the public channel.

A3 : S_n checks if $|T_2' - T_2| < \Delta T$. If this hold, S_n calculate $R_2 = M_i \oplus h(x_s \| SID_n)$, $SK = h(DID_i \| h(x_s \| SID_n) \| R_2 \| T_2)$, and verifies

$B_i \stackrel{?}{=} h(DID_i \| SK \| h(x_s \| SID_n) \| SID_n \| T_2)$. If this unsuccessful, S_n terminates the process. Else, believes GWN is authentic.

A4 : Further S_n computes $C_i = h(h(x_s \| SID_n) \| SK \| DID_i \| SID_n \| T_3)$. Sends the message $\{C_i, T_3\}$ to GWN.

A5 : GWN firstly verifies $|T_3' - T_3| < \Delta T$. If the verification fails, this phase is terminated. Otherwise, computes $C_i \stackrel{?}{=} h(h(x_s \| SID_n) \| SK \| DID_i \| SID_n \| T_3)$ from the received value. If this verification fails GWN terminates the process. Otherwise, believes S_n is legitimate and further computes $D_i = E_k(DID_i \| ID_n \| SK \| R_1 | T_4)$ and sends the response message $\{D_i, T_4\}$ to U_i over an insecure channel.

A6 : U_i first check the timestamp $|T_4' - T_4| < \Delta T$. If the verification fails, terminates the phase. Otherwise, computes $D_k(D_i) = \{DID_i, SID_n, SK, R_1, T_4\}$ and compares the decrypted DID_i, R_1, T_4 with the earlier computed values. If the verification holds, U_i authenticates GWN otherwise, terminates the process.

C. PASSWORD CHANGE PHASE

This phase takes action whenever U_i wishes to changes his/her old password to new password. This phase involves no assistance with GWN and S_n. The details are as follows:

P1 : U_i inserts his/her smartcard into the card reading device and inputs his personal login credentials $\{ID_i, PW_i\}$ to compute $\overline{PW_i}^{old} = h(PW_i^{old} \| b)$, $v^{old} = N_i \oplus h(ID_i \| \overline{PW_i}^{old})$, and verify $M_i \stackrel{?}{=} h(\overline{PW_i}^{old} \| v^{old})$. If this verification fails, it terminates the phase. Otherwise, the smartcard continues with the next step.

P2 : The smartcard compute $\overline{PW_i}^{new} = h(PW_i^{new} \| b)$, $N_i^{new} = v^{old} \oplus h(ID_i \| \overline{PW_i}^{new})$, and $M_i^{new} = h(\overline{PW_i}^{new} \| v^{old})$.

P3 : The smartcard replaces the older values of N_i and M_i with the new values N_i^{new} and M_i^{new}. Therefore, the smartcard finally contains $\{N_i^{new}, M_i^{new}, h(\cdot), b\}$.

IV. SHORTCOMINGS OF JUNG *et al.*'s scheme

Note.1: This designed scheme of Jung *et al.*'s faces many security flaws. Most importantly, the insider of the system creates many insecure problems to the other registered and legitimate users. The details are as follows [57]:

A. PASSWORD GUESSING ATTACK

Let us suppose that, the attacker $\mathcal{A}$ has registered as a legal user to the system. Now $\mathcal{A}$ also own's his own login credentials and other parameters to login into the system also makes use of the captured communication messages of U_i. The attack is performed as follows:

PG1: Attacker own's user's smartcard and gets the information $\{N_i, M_i, b\}$ by applying power analysis.

PG2: Attacker guess ID_i and PW_i as they are chosen from the low-entropy to compute $\overline{PW}_i$, attacker uses the parameter b and guessed password.

PG3: Further, computes $v = N_i \oplus h(ID_i^g \| \overline{PW}_i^g)$ and $M_i^g = h(\overline{PW}_i^g \| v^g)$.

PG4: Now verify $M_i \stackrel{?}{=} M_i^g$. If this verification is successful then the attacker is succeeded in guessing the login parameters right.

This entire process takes place off-line. No interaction is needed. i.e., All the users credentials are at risk. Since attacker is able to calculate v just by guessing ID_i/PW_i. In other words, attacker can make use of v whenever required to crash this entire network.

Note.2: In the design of Jung *et al.*'s scheme the parametric values such as $\{b, v\}$, where $v = h(x_a)$ and b is a random nonce chosen by user him/herself and stores in their smartcard. An active attacker $\mathcal{A}$ can easily extract these parametric values and perform valuable attacks and prove Jung *et al.*'s design insecure and impractical to use.

B. FORGERY ATTACK

The attack is performed as follows:

FA1: Attacker $\mathcal{A}$ uses his credentials and retrieve the value $v = h(x_a)$ as computed by GWN. But, $\mathcal{A}$ retrieves v using $\mathcal{A}$'s login credentials, as $v = N_i^{\mathcal{A}} \oplus h(ID_i^{\mathcal{A}} \| \overline{PW_i}^{\mathcal{A}})$.

FA2: Now from the earlier transmitted messages of the legitimate user U_i, attacker extracts the parameters $\{DID_i^{prev}, A_i^{prev}, T_1^{prev}\}$ and computes $k^{\mathcal{A}} = h(DID_i^{prev} \| v^{\mathcal{A}} \| T_1^{prev})$ and decrypts A_i with the computed $k^{\mathcal{A}}$ to retrieve $\{DID_i^*, R_1^*, T_1^*\}$.

FA3: After the decryption of A_i of the user U_i with the computed $k^{\mathcal{A}}$ verifies $DID_i^{prev} \stackrel{?}{=} DID_i^*$. If the verification is successful, the attacker $\mathcal{A}$ is successful in breaking the scheme. Then $\mathcal{A}$ proceeds with the next step to forge the user U_i. Otherwise, repeat the steps $FA1 - FA3$ until attacker is successful in breaking the scheme without the interference of the GWN.

FA4: Now, $\mathcal{A}$ modifies user's current message $\{DID_i, A_i, T_1\}$ as $\{DID_i^{\mathcal{A}}, A_i^{\mathcal{A}}, T_1\}$, where $A_i^{\mathcal{A}} = E_{k^{\mathcal{A}}}(DID_i^{\mathcal{A}}, R_1^{\mathcal{A}}, T_1)$ computed value of the attacker.

FA5: After the modification, attacker sends the request message $\{DID_i^{\mathcal{A}}, A_i^{\mathcal{A}}, T_1\}$ to GWN. Here GWN, just checks the validity of the timestamp and validate the request message by decrypting $A_i^{\mathcal{A}}$ using the symmetric key k and finds the parameters as legal on comparison.

FA6: Thus, attacker $\mathcal{A}$ can easily forge user's messages. This shows, Jung *et al.*'s scheme fails to resist forgery attack.

C. USER TRACABILITY ATTACK

In Jung *et al.*'s scheme, the user's valuable information is stored in user's smartcard so that the credentials can be used

to login into the system and get access to the information user trying to fetch. But in Jung *et al.*'s scheme, the parametric values like M_i, DID_i are transmitted from U_i to GWN and then from GWN to S_n. Attacker can fetch M_i from the user's smartcard by applying power analysis [6] and then from the captured messages attacker $\mathcal{A}$ can get the information of DID_i. Attacker can easily keep track of user and gain access of what user is trying to achieve.

D. PRIVACY OF THE SESSION KEY

In Jung *et al.*'s design the session key is computed by GWN and then by S_n. Although the session key is computed involving the parameters of user and sensor node, user has no part in computing the session key. Moreover, apart from user and sensor node session key is known and computable by third person which is GWN [28], [29]. If suppose, an insider sits at GWN, then the insider can easily eavesdrop on the session keys and compromise any session at his will. This shows, the privacy of the session key is not considered by Jung *et al.* which is a serious problem of Jung *et al.*'s scheme.

E. FAILS TO SUPPORT DYNAMIC NODE ADDITION

Basically, in WSNs, the sensor nodes are deployed in an hostile environment and are often captured physically [30]. Thus, the data of the captured sensor nodes contain the useful information. Sometimes, due to heavy computation burden sensor nodes fails to respond. In such cases, there should be a provision to add or delete sensor node according to the need of the system. It is evident that Jung *et al.*'s scheme fails to provide this essential feature.

F. NO PROVISION OF VERIFYING THE SCHEME TO ENSURE FORMAL SECURITY [31]

To evaluate and verify the efficiency of the proposed scheme there is a strictly necessary of formal security analysis. It is observed that, Jung *et al.*'s scheme just presented the informal security analysis and neglected the formal security verification for their scheme security.

TABLE 4. Comparison of security requirements/functional attributes.

Security attributes	[11]	[12]	[15]	[27]	[33]	[19]	[20]
Replay attack	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
User anonymity	*No*	*No*	*No*	*No*	*No*	*No*	*Yes*
Mutual authentication	*Yes*	*No*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Stolen smartcard attack	*Yes*	*No*	*Yes*	*No*	*No*	*No*	*No*
Impersonation attack	*Yes*	*No*	*No*	*No*	*No*	*Yes*	*No*
Lack of Dynamic node addition	*No*	*No*	*Yes*	*No*	*Yes*	*Yes*	*No*
Efficient Password/Biometric change	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*
Forgery attack	*No*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*No*
Session key agreement	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*No*
Man – in – the – middle attack	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*Yes*
Denial of Service	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*No*	*Yes*
Sensor node capturing	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Biometric/Password guessing attack	*No*	*No*	*No*	*Yes*	*No*	*Yes*	*No*
Privileged – insider attack	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*No*

The security pitfalls were highlighted in the Table 4, protected by the existing schemes. It is observed that many schemes in Table 4 fails to resist many important features for example; password guessing attack, user anonymity, impersonation attack. Moreover, the dynamic node addition feature is not considered in many of the cited schemes.

V. SUGGESTED COUNTER MEASURES

From the *Note*.1, every registered user uses the parameter b to compute the masked password $\overline{PW}_i = h(PW_i \| b)$ which is a static value and b is stored in "plaintext" form to every registered users smartcard. An active attacker $\mathcal{A}$ can bumble the system by capturing the legitimate user's smartcard. In the section IV-A, we have seen that when an attacker gains access to U_i's smartcard $\mathcal{A}$ can easily impose password guessing attack. To avoid this and improve Jung *et al.*'s scheme one can counter it as $L_i = b \oplus h(ID_i \| PW_i)$ and replace the smartcard with the parameter by L_i instead of b. For the best possible solution one can opt biometric features to avoid password guessing attack.

Moreover, as mentioned in *Note*.2, the masked master secret keys under the hash function couldn't ensure the user as unique. This shows that, any attacker can become a registered user and furthermore, instead of the legitimate user, $\mathcal{A}$ can anonymously login to the system. Thus there is a strict need to focus on differentiating the legitimate users from the attackers. Looking into the drawbacks of Jung *et al.*'s design, we focus on restricting such anonymous authentication. In Jung *et al.*'s scheme, in the section IV-B, it is observed that every registered user gets the same parametric value $v = h(x_r)$, which remains same in every session and every registered user can make use of it. This opens the doors for the intruders/attackers to gain access to the valuable information which the legitimate user trying to access. Instead of making use of $v = h(x_r)$ and give it to the users during registration by masking it as $v = h(x_r \| ID_i)$, where the improved parameter ensure the uniqueness of the user and also restrict attackers in imposing forgery attack on behalf of the legitimate user. This correction ensures each user is obtaining the unique secret value according to their registration. This countermeasure takes care of the dishonest user by producing honest user's identity to enjoy the services.

VI. THE PROPOSED SCHEME

In our scheme, the user makes use of his biometric feature to login in the system and establishes a secure connection with the sensor node via gateway node. The biometric fuzzy extractor is considered to extract the biometric key of the user to tackle with the password guessing attacks. The detailed description is discussed in four phases: user registration, login and authentication, biometric/password update, and node addition.

A. REGISTRATION PHASE

In this phase, user U_i registers with gateway. The details are as follows:

R1: The user U_i selects his ID_i, PW_i. Using fuzzy extractor, biometric feature $Gen(Bio_i) = < \alpha_i, \tau >$ is captured by the Generation function.

R2: Computes a masked password $\overline{PW_i} = h(PW_i \| b \| \alpha_i)$, $Reg_i = h(b \| \alpha_i)$ using the random nonce b. Further, sends $< Reg_i, ID_i, \overline{PW_i} >$ to GWN as a request message for the registration over a secure channel.

$User(U_i)$	Gateway Node(GWN)
inputs ID_i, PW_i	
and generate random nonce b	
imprints $Gen(Bio_i) =< \alpha_i, \tau >$	
Computes $\overline{PW_i} = h(PW_i \| b \| \alpha_i)$	
$Reg_i = h(b \| \alpha_i)$	
$< Reg_i, ID_i, \overline{PW_i} >$ $\longrightarrow$	
	$v = h(x_a \| ID_i)$
	$N_i = h(ID_i \| \overline{PW_i}) \oplus v$
	$M_i = h(\overline{PW_i} \| v)$
	$SC_i = \{N_i, M_i, h(\cdot), \tau\}$ $\longleftarrow$
$L_i = b \oplus h(ID_i \| \alpha_i)$	

FIGURE 2. User registration phase.

R3: On receiving the credentials from user, the *GWN* computes $v = h(x_a \| ID_i)$, $N_i = h(ID_i \| \overline{PW_i}) \oplus v$ and $M_i = h(\overline{PW_i} \| v)$, and stores v into the database against Reg_i. Then the parameters $\{N_i, M_i, h(\cdot), \tau\}$ are stored into smart card memory and transmit it to the user over the secure channel .

R4: On receiving the smart card, U_i computes $L_i = b \oplus h(ID_i \| \alpha_i)$ embeds L_i to the smart card's memory. The illustration of this phase is found in Fig. 2.

B. LOGIN AND AUTHENTICATION PHASES

The login phase is executed to validate the user credentials and restrict denial of service attack against attacker when U_i wants to gain access to WSN. The details are given below. The illustration of this phase is found in Fig. 3.

L1 : The user U_i inserts his smart card into the card reader. U_i inputs his login credentials such as identity ID_i, password PW_i and biometric feature by applying fuzzy extractor's reproduction function $\alpha_i = Rep(Bio_i, \tau)$. Then computes the masked $\overline{PW_i}^* = h(PW_i \| b \| \alpha_i)$, $v^* = h(ID_i \| \overline{PW_i}^*) \oplus N_i$.

L2 : Further computes, $M_i^* = h(\overline{PW_i}^* \| v^*)$. Verifies $M_i \stackrel{?}{=} M_i^*$ with the stored value of smart card. If this verification holds, the smart card acknowledges the legitimacy of the user and proceeds to the next step. Otherwise, terminates the process.

L3 : The smart card generates a random nonce R_1 and computes $Reg_i = h(b \| \alpha_i)$, $DID_i = h(ID_i \| R_1)$, $k = h(Reg_i \| DID_i \| v^* \| T_1)$ and $A_i = E_k(v^*, DID_i, R_1, T_1)$, where T_1 is the current timestamp.

L4 : U_i transmit the message $\{DID_i, Reg_i, A_i, T_1\}$ to the *GWN*.

A1 : Upon receiving the login request from U_i, *GWN* verifies the freshness of the user's time stamps T_1 as $|T_1' - T_1| < \Delta T$. If this holds, *GWN* extracts U_i's master secret key from its memory which is stored against to Reg_i. computes $k = h(Reg_i \| DID_i \| v \| T_1)$ and $D_k(A_i) = \{v^*, DID_i^*, R_1^*, T_1^*\}$. *GWN* verifies v^*, DID_i^*, T_1^* with the stored and received values. If the verification hold, *GWN* acknowledge the legitimacy of U_i and proceed with the next step. Otherwise, GWN assumes there is some fault in the message and the process is terminated.

A2 : *GWN* selects a random nonce R_2 and computes $MM_i = h(x_s \| SID_n) \oplus R_2$, and $B_i = h(DID_i \| R_2 \| h(x_s \| SID_n) \| SID_n \| T_2)$. Then, transmits the message $\{MM_i, DID_i, B_i, T_2\}$ to S_n over the public channel.

A3 : On receiving the message, S_n checks if $|T_2' - T_2| < \Delta T$. If the verification holds,

User U_i	Gateway node GWN	Sensor node S_n
Inserts SC into a terminal.		
Inputs ID_i and PW_i.		
imprints his biometric key Bio_i		
$\alpha_i = Rep(Bio_i, \tau)$		
$\overline{PW_i}^* = h(PW_i \| b \| \alpha_i)$,		
$v^* = h(ID_i \| \overline{PW_i}^*) \oplus N_i$		
$M_i^* = h(\overline{PW_i}^* \| v^*)$		
Verifies $M_i \stackrel{?}{=} M_i*$		
generates a random nonce R_1		
$Reg_i = h(b \| \alpha_i)$,	$\|T1' - T_1\| < \Delta T$	
$DID_i = h(ID_i \| R_1)$,	$k = h(Reg_i \| DID_i \| v \| T_1)$	
$k = h(Reg_i \| DID_i \| v^* \| T_1)$	$D_k(A_i) = \{v^*, DID_i^*, R_1^*, T_1^*\}$	
$A_i = E_k(v^*, DID_i, R_1, T_1)$	verifies v^*, DID_i^*, T_1^*	
$Message_1 = \{DID_i, Reg_i, A_i, T_1\}$ $\longrightarrow$	generates random nonce R_2	$\|T_2' - T_2\| < \Delta T$
		$R_2^* = MM_i \oplus h(DID_i \| h(x_s \| SID_n))$
	$MM_i = h(DID_i \| h(x_s \| SID_n)) \oplus R_2$,	$B_i \stackrel{?}{=} h(DID_i \| R_2^* \| h(x_s \| SID_n) \| SID_n \| T_2)$
	$B_i = h(DID_i \| R_2 \| h(x_s \| SID_n) \| SID_n \| T_2)$	$SK = h(DID_i \| h(x_s \| SID_n) \| R_2 \| T_2)$
	$Message_2 = \{MM_i, DID_i, B_i, T_2\}$ $\longrightarrow$	$F_i = SK \oplus DID_i \oplus h(DID_i \| h(x_s \| SID_n) \| R_2^*)$,
		$C_i = h(h(x_s \| SID_n) \| SK \| DID_i \| SID_n \| T_3)$
	$\|T_3' - T_3\| < \Delta T$	$Message_3 = \{C_i, F_i, T_3\}$ $\longleftarrow$
	$SK = F_i \oplus DID_i \oplus h(DID_i \| h(x_s \| SID_n) \| R_2^*)$	
	$C_i \stackrel{?}{=} h(h(x_s \| SID_n) \| SK \| DID_i \| SID_n \| T_3)$	
	$D_i = E_k(DID_i \| SID_n \| SK \| R_1 \| T_4)$	
$\|T_4' - T_4\| < \Delta T$	$Message_4 = \{D_i, T_4\}$ $\longleftarrow$	
$D_k(D_i) = \{DID_i, SID_n, SK, R_1, T_4\}$		
compares the decrypted DID_i, R_1, T_4		

FIGURE 3. Login and authentication phases of the proposed scheme.

S_n computes $R_2^* = MM_i \oplus h(x_s \| SID_n)$, and verifies $B_i \stackrel{?}{=} h(DID_i \| R_2^* \| h(x_s \| SID_n) \| SID_n \| T_2)$. If the verification fails, S_n terminates the process. Otherwise, believes GWN is authentic.

A4 : Further S_n computes $SK = h(DID_i \| h(x_s \| SID_n) \| R_2 \| T_2)$, $F_i = SK \oplus DID_i \oplus R_2^*$, $C_i = h(h(x_s \| SID_n) \| SK \| DID_i \| SID_n \| T_3)$. Sends the message $\{C_i, F_i, T_3\}$ to GWN.

A5 : GWN firstly verifies $|T_3' - T_3| < \Delta T$. If the verification fails, this phase is terminated. Otherwise, computes $SK = F_i \oplus DID_i \oplus R_2^*$, $C_i \stackrel{?}{=} h(h(x_s \| SID_n) \| SK \| DID_i \| SID_n \| T_3)$ from the received value. If this verification fails, GWN terminates the process. Otherwise, believes S_n is legitimate and further computes $D_i = E_k(DID_i \| SID_n \| SK \| R_1 | T_4)$ and sends the response message $\{D_i, T_4\}$ to U_i over an insecure channel.

A6 : U_i first check the timestamp $|T_4' - T_4| < \Delta T$. If the verification fails, terminates the phase. Otherwise, computes $D_k(D_i) = \{DID_i, SID_n, SK, R_1, T_4\}$ and compares the decrypted DID_i, R_1, T_4 with the earlier computed values. If the verification holds, U_i authenticates GWN otherwise, terminates the process.

C. BIOMETRIC/PASSWORD CHANGE PHASE

This phase takes action whenever U_i wishes to changes his/her old password to new password. This phase involves no assistance with GWN and S_n. The details are as follows:

P1 : U_i inserts his/her smartcard into the card reading device and inputs his personal login credentials $\{ID_i, PW_i\}$ to compute $\overline{PW_i}^{old} = h(PW_i^{old} \| b)$, $v^{old} = N_i \oplus h(ID_i \| \overline{PW_i}^{old})$, and verify $M_i \stackrel{?}{=} h(\overline{PW_i}^{old} \| v^{old})$. If this verification fails, it terminates the phase. Otherwise, the smartcard continues with the next step.

P2 : The smartcard compute $\overline{PW_i}^{new} = h(PW_i^{new} \| b)$, $N_i^{new} = v^{old} \oplus h(ID_i \| \overline{PW_i}^{new})$, and $M_i^{new} = h(\overline{PW_i}^{new} \| v^{old})$.

P3 : The smartcard replaces the older values of N_i and M_i with the new values N_i^{new} and M_i^{new}. Therefore, the smartcard finally contains $\{N_i^{new}, M_i^{new}, h(\cdot), b\}$.

P4 : The illustration of this phase is given in Fig. 4.

D. DYNAMIC SENSOR NODE ADDITION PHASE

Some sensor nodes may lapse due to their battery utilization or they can be physically caught by an attacker. A provision for deployment of newly arrival sensor node S_n^{new} be deployed in the current WSN. The details are as follows:

DA1: A new unique identity SID_n^{new} need to be selected for S_n^{new} by the GWN.

DA2: The GWN then performs computation $P_n^{new} = h(SID_n^{new} \| x_s)$, and the parameters SID_n^{new} is written into the sensor node's memory before deploying S_n^{new} into the network.

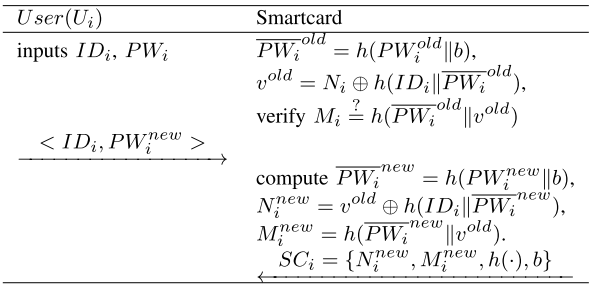

FIGURE 4. Biometric/Password change phase.

VII. SECURITY ANALYSIS

In this section, the security of the proposed scheme is demonstrated using the BAN-logic proof which ensures the mutual authentication among the participants. Furthermore, using AVISPA tool, we demonstrated the security of the proposed scheme against replay and man-in-the-middle attacks. Moreover, to ensure the other security requirements and functionalities we performed an informal security analysis. The details are as follows:

A. BAN-LOGIC PROOF TO DEMONSTRATE THE MUTUAL AUTHENTICATION

This method of formal security analysis is recommended to demonstrate the mutual authentication and session key establishment between U_i and SN_j using the widely-accepted BAN-logic [32] and the details of notation and rules can be seen in Table 1 and Table 2.

Goals: To prove the method demonstrated successful, few goals need to be set and the design must satisy the analytic procedures of the BAN-logic [24]. The test goals can be formulated as follows:

$G_1 : S_n \mid\equiv (U_i \stackrel{SK}{\longleftrightarrow} S_n)$. $G_2 : U_i \mid\equiv S_n \mid\equiv (U_i \stackrel{SK}{\longleftrightarrow} S_n)$.

$G_3 : U_i \mid\equiv (U_i \stackrel{SK}{\longleftrightarrow} S_n)$. $G_4 : S_n \mid\equiv U_i \mid\equiv (U_i \stackrel{SK}{\longleftrightarrow} S_n)$.

Idealized form:

- Message M_1, $U_i \rightarrow S_n : \{U_i \stackrel{ID_i}{\longleftrightarrow} S_n, T_1, ID_i\}_{h(x_a \| ID_i)}$;
- Message M_2, $U_i \rightarrow S_n : \{U_i \stackrel{ID_i}{\longleftrightarrow} S_n, R_1, T_1, ID_i, U_i \stackrel{R_1}{\longleftrightarrow} S_n\}_{h(x_a \| ID_i)}$;
- Message M_3, $GWN \rightarrow S_n : (T_2, SID_n, GWN \stackrel{SID_n}{\longleftrightarrow} S_n)_{h(x_s \| SID_n)}$;
- Message M_4, $GWN \rightarrow S_n : (T_2, SID_n, GWN \stackrel{SID_n}{\longleftrightarrow} S_n, R_2, GWN \stackrel{R_2}{\longleftrightarrow} S_n)_{h(x_s \| SID_n)}$;
- Message M_5, $S_n \rightarrow GWN : (GWN \stackrel{SID_n}{\longleftrightarrow} S_n, T_3, GWN \stackrel{R_1}{\longleftrightarrow} S_n)_{h(x_s \| SID_n)}$;
- Message M_6, $U_i \rightarrow GWN : (GWN \stackrel{SID_n}{\longleftrightarrow} S_n, T_3, R_1, GWN \stackrel{R_1}{\longleftrightarrow} S_n, U_i \stackrel{SK}{\longleftrightarrow} GWN)_{h(x_a \| ID_i)}$;
- Message M_7, $S_n \rightarrow U_i : \{U_i \stackrel{ID_i}{\longleftrightarrow} S_n, R_2, T_3, ID_i, U_i \stackrel{R_2}{\longleftrightarrow} S_n\}_{h(x_a \| ID_i)}$;

TABLE 5. Assumptions.

A_1: $S_n|\equiv \sharp(T_1)$;
A_2: $S_n|\equiv \sharp(T_2)$;
A_3: $GWN|\equiv \sharp(T_3)$;
A_4: $U_i|\equiv \sharp(T_3)$;
A_5: $U_i|\equiv \sharp(T_4)$;
A_6: $S_n|\equiv \sharp(R_1)$;
A_7: $S_n|\equiv \sharp(R_2)$;
A_8: $GWN|\equiv \sharp(R_1)$;
A_9: $U_i|\equiv \sharp(R_2)$;
A_{10}: $U_i|\equiv (U_i \overset{h(x_a\|ID_i)}{\longleftrightarrow} S_n)$;
A_{11}: $S_n|\equiv (U_i \overset{h(x_a\|ID_i)}{\longleftrightarrow} S_n)$;
A_{12}: $S_n|\equiv (GWN \overset{h(x_s\|SID_n)}{\longleftrightarrow} S_n)$;
A_{13}: $GWN|\equiv (GWN \overset{h(x_a\|ID_i)}{\longleftrightarrow} S_n)$;
A_{14}: $GWN|\equiv (GWN \overset{h(x_s\|SID_n)}{\longleftrightarrow} S_n)$;
A_{15}: $S_n|\equiv U_i \Rightarrow (U_i \overset{ID_i}{\longleftrightarrow} S_n)$;
A_{16}: $S_n|\equiv U_i \Rightarrow (U_i \overset{R_1}{\longleftrightarrow} S_n)$;
A_{17}: $S_n|\equiv GWN \Rightarrow (GWN \overset{SID_n}{\longleftrightarrow} S_n)$;
A_{18}: $S_n|\equiv GWN \Rightarrow (GWN \overset{R_2}{\longleftrightarrow} S_n)$;
A_{19}: $GWN|\equiv S_n \Rightarrow (GWN \overset{R_1}{\longleftrightarrow} S_n)$;
A_{20}: $U_i|\equiv S_N \Rightarrow (U_i \overset{R_2}{\longleftrightarrow} S_n)$;
A_{21}: $GWN|\equiv U_i \Rightarrow (U_i \overset{SK}{\longleftrightarrow} GWN)$;
A_{22}: $U_i|\equiv GWN \Rightarrow (U_i \overset{SK}{\longleftrightarrow} GWN)$;

- Message M_8, $GWN \rightarrow U_i : (U_i \overset{ID_i}{\longleftrightarrow} S_n, R_2, T_4, ID_i, U_i \overset{h(x_a\|ID_i)}{\longleftrightarrow} S_n, U_i \overset{SK}{\longleftrightarrow} GWN)_{h(x_a\|ID_i)}$;

Considering the BAN-logic rules as presented in Table 2 and taking the assumptions(see Table 5) into account, the analysis is carried out to prove the mutual authentication among the communicated parties as follows:

From the message 1, we can see:

S-1: $S_n \triangleleft \{U_i \overset{ID_i}{\longleftrightarrow} S_n, T_1, ID_i\}_{h(x_a\|ID_i)}$

From the step S-1 and assumption A_{11}, we take the message meaning rule to derive:

S-2: $S_n|\equiv U_i|\sim (U_i \overset{ID_i}{\longleftrightarrow} S_n, T_1, ID_i)$.

From the step S-2 and taking A_1, the freshness conjuncatenation rule is applied to get:

S-3: $S_n|\equiv \sharp(U_i \overset{ID_i}{\longleftrightarrow} S_n, T_1, ID_i)$.

Using the steps S-2 and S-3, the nonce-verification rule is applied to derive:

S-4: $S_n|\equiv U_i|\equiv (U_i \overset{ID_i}{\longleftrightarrow} S_n)$.

Considering S-4, the belief rule is applied to obtain:

S-5: $S_n|\equiv U_i|\equiv (U_i \overset{ID_i}{\longleftrightarrow} S_n)$.

Taking the step S-5 and A_{15} into consideration, jurisdiction rule is applied to get:

S-6: $S_n|\equiv (U_i \overset{ID_i}{\longleftrightarrow} S_n)$.

From the message 2, we can write:

S-7: $S_n \triangleleft \{U_i \overset{ID_i}{\longleftrightarrow} S_n, U_i \overset{R_1}{\longleftrightarrow} S_n, T_1, R_1, ID_i\}_{h(x_a\|ID_i)}$

From the step S-7 and assumption A_{11}, we take the message meaning rule to derive:

S-8: $S_n|\equiv U_i|\sim (U_i \overset{ID_i}{\longleftrightarrow} S_n, U_i \overset{R_1}{\longleftrightarrow} S_n, T_1, R_1, ID_i)$.

From step S-8 and assumption A_1, A_6, the freshness conjuncatenation rule is applied to get:

S-9: $S_n|\equiv \sharp(U_i \overset{ID_i}{\longleftrightarrow} S_n, U_i \overset{R_1}{\longleftrightarrow} S_n, T_1, R_1, ID_i)$.

Using the steps S-8 and S-9, the nonce-verification rule is applied to derive:

S-10: $S_n|\equiv U_i|\equiv (U_i \overset{ID_i}{\longleftrightarrow} S_n, U_i \overset{R_1}{\longleftrightarrow} S_n, T_1, R_1, ID_i)$.

Considering S-10, the belief rule is applied to obtain:

S-11: $S_n|\equiv U_i|\equiv (U_i \overset{R_1}{\longleftrightarrow} S_n)$.

Taking the step S-11 and A_{16}, into consideration, jurisdiction rule is applied to get:

S-12: $S_n|\equiv (U_i \overset{R_1}{\longleftrightarrow} S_n)$.

From the message 3, we can infer:

S-13: $S_n \triangleleft (T_2, SID_n, GWN \overset{SID_n}{\longleftrightarrow} S_n)_{h(x_s\|SID_n)}$

From the step S-13 and assumption A_{12}, we take the message meaning rule to derive:

S-14: $S_n|\equiv GWN|\sim (T_2, SID_n, GWN \overset{SID_n}{\longleftrightarrow} S_n)$.

From S-14 and assumption A_2, the freshness conjuncatenation rule is applied to get:

S-15: $S_n|\equiv \sharp(T_2, SID_n, GWN \overset{SID_n}{\longleftrightarrow} S_n)$.

Using the steps S-14 and S-15, the nonce-verification rule is applied to derive:

S-16: $S_n|\equiv GWN|\equiv (T_2, SID_n, GWN \overset{SID_n}{\longleftrightarrow} S_n)$.

Considering S-16, the belief rule is applied to obtain:

S-17: $S_n|\equiv GWN|\equiv (GWN \overset{SID_n}{\longleftrightarrow} S_n)$.

Taking the step S-17 and A_{17}, into consideration, jurisdiction rule is applied to get:

S-18: $S_n|\equiv (GWN \overset{SID_n}{\longleftrightarrow} S_n)$.

From the message 4, we could derive:

S-19: $S_n \triangleleft (T_2, SID_n, GWN \overset{SID_n}{\longleftrightarrow} S_n, R_2, GWN \overset{R_2}{\longleftrightarrow} S_n)_{h(x_s\|SID_n)}$

From S-19 and A_{12}, we take the message meaning rule to derive:

S-20: $S_n| \equiv GWN| \sim (T_2, SID_n, GWN \overset{SID_n}{\longleftrightarrow} S_n, R_2, GWN \overset{R_2}{\longleftrightarrow} S_n)$.

From S-20 and assumption A_2, A_7, the freshness conjuncatenation rule is applied to get:

S-21: $S_n|\equiv \sharp(T_2, SID_n, GWN \overset{SID_n}{\longleftrightarrow} S_n, R_2, GWN \overset{R_2}{\longleftrightarrow} S_n)$.

Using the steps S-20 and S-21, the nonce-verification rule is applied to derive:

S-22: $S_n| \equiv GWN| \equiv (T_2, SID_n, GWN \overset{SID_n}{\longleftrightarrow} S_n, R_2, GWN \overset{R_2}{\longleftrightarrow} S_n)$.

Considering S-22, the belief rule is applied to obtain:

S-23: $S_n|\equiv GWN|\equiv (GWN \overset{R_2}{\longleftrightarrow} S_n)$.

Taking the step S-23 and A_{18}, into consideration, jurisdiction rule is applied to get:

S-24: $S_n|\equiv (GWN \overset{R_2}{\longleftrightarrow} S_n)$.

From the message 5, we could derive:

S-25: $GWN \triangleleft (GWN \overset{SID_n}{\longleftrightarrow} S_n, T_3, GWN \overset{R_1}{\longleftrightarrow} S_n)_{h(x_s\|SID_n)}$

From S-25 and A_{14}, we take the message meaning rule to derive:

S-26: $GWN|\equiv S_n|\sim (GWN \overset{SID_n}{\longleftrightarrow} S_n, T_3, GWN \overset{R_1}{\longleftrightarrow} S_n)$.

From S-26 and assumption A_3, the freshness conjuncatenation rule is applied to get:

S-27: $GWN|\equiv \sharp(GWN \overset{SID_n}{\longleftrightarrow} S_n, T_3, GWN \overset{R_1}{\longleftrightarrow} S_n)$.

Using the steps S-26 and S-27, the nonce-verification rule is applied to derive:

S-28: $GWN|\equiv S_n|\equiv (GWN \overset{SID_n}{\longleftrightarrow} S_n, T_3, GWN \overset{R_1}{\longleftrightarrow} S_n)$.

Considering S-28, the belief rule is applied to obtain:

S-29: $GWN|\equiv S_n|\equiv (GWN \overset{R_1}{\longleftrightarrow} S_n)$.

Taking the step S-29 and A_{19}, into consideration, jurisdiction rule is applied to get:

S-30: $GWN|\equiv (GWN \overset{R_1}{\longleftrightarrow} S_n)$.

From the message 6, we could derive:

S-31: $GWN \triangleleft (GWN \overset{SID_n}{\longleftrightarrow} S_n, T_3, R_1, GWN \overset{R_1}{\longleftrightarrow} S_n, U_i \overset{SK}{\longleftrightarrow} GWN)_{h(x_a\|ID_i)}$

From S-31 and assumption A_{13}, we take the message meaning rule to derive:

S-32: $GWN|\equiv U_i|\sim (GWN \overset{SID_n}{\longleftrightarrow} S_n, T_3, R_1, GWN \overset{R_1}{\longleftrightarrow} S_n, U_i \overset{SK}{\longleftrightarrow} GWN)$.

From S-32 and assumption A_3, A_8, the freshness conjuncatenation rule is applied to get:

S-33: $GWN|\equiv \sharp(GWN \overset{SID_n}{\longleftrightarrow} S_n, T_3, R_1, GWN \overset{R_1}{\longleftrightarrow} S_n, U_i \overset{SK}{\longleftrightarrow} GWN)$.

Using the steps S-32 and S-33, the nonce-verification rule is applied to derive:

S-34: $GWN|\equiv U_i|\equiv (GWN \overset{SID_n}{\longleftrightarrow} S_n, T_3, R_1, GWN \overset{R_1}{\longleftrightarrow} S_n, U_i \overset{SK}{\longleftrightarrow} GWN)$.

Considering S-17, S-18, S-29 and S-34, the belief rule is applied to obtain:

S-35: $GWN|\equiv U_i|\equiv (U_i \overset{SK}{\longleftrightarrow} GWN)$. **(Goal 4)**

Taking the step S-35 and A_{21}, into consideration, jurisdiction rule is applied to get:

S-36: $GWN|\equiv (U_i \overset{SK}{\longleftrightarrow} GWN)$. **(Goal 3)**

From the message 7, we could derive:

S-37: $U_i \triangleleft \{U_i \overset{ID_i}{\longleftrightarrow} S_n, R_2, T_3, ID_i, U_i \overset{R_2}{\longleftrightarrow} S_n\}_{h(x_a\|ID_i)}$

From S-37 and assumption A_{10}, we take the message meaning rule to derive:

S-38: $U_i|\equiv S_n|\sim (U_i \overset{ID_i}{\longleftrightarrow} S_n, R_2, T_3, ID_i, U_i \overset{R_2}{\longleftrightarrow} S_n)$.

From S-38 and assumption A_4, A_9, the freshness conjuncatenation rule is applied to get:

S-39: $U_i|\equiv \sharp(U_i \overset{ID_i}{\longleftrightarrow} S_n, R_2, T_3, ID_i, U_i \overset{R_2}{\longleftrightarrow} S_n)$.

Using the steps S-38 and S-39, the nonce-verification rule is applied to derive:

S-40: $U_i|\equiv S_n|\equiv (U_i \overset{ID_i}{\longleftrightarrow} S_n, R_2, T_3, ID_i, U_i \overset{R_2}{\longleftrightarrow} S_n)$.

Considering the steps S-5, S-6, and S-39, the belief rule is applied to obtain:

S-41: $U_i|\equiv S_n|\equiv (U_i \overset{R_2}{\longleftrightarrow} S_n)$.

Taking the step S-41 and A_{20}, into consideration, jurisdiction rule is applied to get:

S-42: $U_i|\equiv (U_i \overset{R_2}{\longleftrightarrow} S_n)$.

From the message 8, we could derive:

S-43: $U_i \triangleleft (U_i \overset{ID_i}{\longleftrightarrow} S_n, R_2, T_4, ID_i, U_i \overset{h(x_a\|ID_i)}{\longleftrightarrow} S_n, U_i \overset{SK}{\longleftrightarrow} GWN)_{h(x_a\|ID_i)}$

From S-43 and assumption A_{10}, we take the message meaning rule to derive:

S-44: $U_i|\equiv S_n|\sim (U_i \overset{ID_i}{\longleftrightarrow} S_n, R_2, T_4, ID_i, U_i \overset{h(x_a\|ID_i)}{\longleftrightarrow} S_n, U_i \overset{SK}{\longleftrightarrow} GWN)$.

From S-44 and assumption A_5, A_9, the freshness conjuncatenation rule is applied to get:

S-45: $U_i|\equiv \sharp(U_i \overset{ID_i}{\longleftrightarrow} S_n, R_2, T_4, ID_i, U_i \overset{h(x_a\|ID_i)}{\longleftrightarrow} S_n, U_i \overset{SK}{\longleftrightarrow} GWN)$.

Using the steps S-44 and S-45, the nonce-verification rule is applied to derive:

S-46: $U_i|\equiv GWN|\equiv (U_i \overset{ID_i}{\longleftrightarrow} S_n, R_2, T_4, ID_i, U_i \overset{h(x_a\|ID_i)}{\longleftrightarrow} S_n, U_i \overset{SK}{\longleftrightarrow} GWN)$.

Considering the steps S-5, S-6, S-41 and S-46, the belief rule is applied to obtain:

S-47: $U_i|\equiv GWN|\equiv (U_i \overset{SK}{\longleftrightarrow} GWN)$. **(Goal 2)**

Taking the step S-47 and A_{22}, into consideration, jurisdiction rule is applied to get:

S-48: $U_i|\equiv (U_i \overset{SK}{\longleftrightarrow} GWN)$. **(Goal 1)**

In view of the Steps 35, 36, 47, and 48, the proposed scheme provides the mutual authentication and key agreement by achieves all the goals (Goals 1-4).

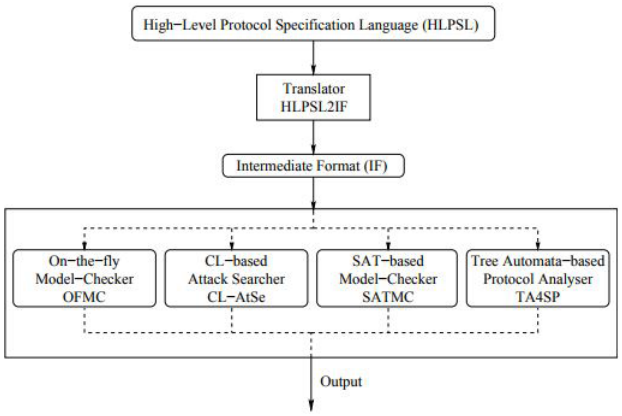

FIGURE 5. Architecture of the AVISPA tool.

B. FORMAL SECURITY VERIFICATION USING AVISPA SIMULATION TOOL

Inspite of the examination regarding the formal security, we give the reenactment results using the [33] tool to our proposed scheme. In recent years, the formal security verification using the AVISPA tool becomes one of the powerful analysis to check the security of a scheme. This AVISPA tool [33] uses the High Level Protocol Specification Language(HLPSL) for implementing the security protocol, which is a role-oriented language. The HLPSL2IF translator makes the HLPSL code into the intermediate form (IF) which is given as input to one of the comprises one of the four variant backends (Fig. 5):

(i) On-the-fly Model-Checker (OFMC)
(ii) CL-based Attack Searcher (CL-AtSe)

(iii) AT-based Model-Checker (SATMC)
(iv) Tree-Automata-based Protocol-Analyzer (TA4SP)

In these backends, an implementation is done in which a variety of state-of-art-automatic analysis techniques are carried out. HLPSL consists of basic roles which are executed according to the network for the entities involved. In addition, the session roles are considered as a mandatory role to enhance the concrete arguments which indulge to all the basic roles for the involved entities. Furthermore, the top-level role is considered as the environment which is again another mandatory role which can be compared and included for one or more sessions involving the global constants.

```
%%% Role for user Ui
role user (Ui, GWN, Sn : agent,
SKuigwn : symmetric_key,
% H is one-way hash function
H: hash_func,
Snd, Rcv: channel(dy))
% Player: the user Ui
played_by Ui
def=
local State: nat,
IDi, PWi, Alphai, B, V, Regi, Ni, Mi, Tau, Li: text,
PWi1, DIDi, K, Ai : text,
T1, R1 : text,
E, F: hash_func
Xa, Xs: text,
const sp1, sp2, ui_gwn_t1, gwn_ui_t2, gwn_ui_r2: protocol_id
init State := 0
transition
%%% User registration phase
1. State = 0 /\ Rcv(start) =|>
State' := 1 /\ Alphai' := new() /\ B' := new()
/\ PWi1' := H(PWi.B'.Alphai')
/\ Regi' := H(B'.Alphai')
/\ secret({IDi,PWi, B', Alphai'}, sp1, {Ui})
% Send the registration request to GWN securely
/\ Snd({H(B.Alphai').IDi.H(PWi.B.Alphai')_SKuigwn)
% Receive the registration reply from BRC securely
2. State = 1 /\ Rcv({xor(V',H(IDi.H(PWi.B.Alphai'))).
H(H(PWi.B.Alphai').V').Tau'.H}_SKuigwn) =|>
State' := 2 /\ secret({Xa',V}, sp2, {GWN})
%%% Login and authenticate phase
/\ T1' := new()
/\ Regi':= H(B.Alphai)
/\ DIDi':= H(IDi.R1')
/\ K':= H(Regi'.DIDi'.xor(H(IDi.H(PWi.B'.Alphai')),
xor(H(Xa'.IDi),H(IDi.H(PWi.B.Alphai'))) ).T1')
/\ Ai':= E(xor(H(IDi.H(PWi.B'.Alphai')),xor(H(Xa'.IDi),
H(IDi.H(PWi.B.Alphai'))) ),DIDi',R1',T1')
% Send login request message Message1 to GWN openly
/\ Snd(DIDi'.Regi'.Ai'.T1')
% Ui has freshly generated the values R1 and T1 for GWN
/\ witness(Ui, GWN, ui_gwn_r1, R1')
/\ witness(Ui, GWN, ui_gwn_t1, T1')
% Receive authentication reply Message4 from GWN openly
3. State = 2 /\ Rcv(E(DIDi'.IDsnj'.SK'.R1'.T4').T4') =|>
% Ui's acceptance of the values R2 and T4 generated for Ui by GWN
State' := 3 /\ request(GWN, Ui, gwn_ui_r2, R2')
/\ request(GWN, Ui, gwn_ui_t3, T3')
end role
```

FIGURE 6. Role for a user U_i.

In HLPSL, the intruder (always denoted by i) takes some roles as legitimate users; hence, it also participates in the execution of protocol as a concrete session. The Dolev-Yao threat model [23] is implemented so that the replay and man-in-the-middle attacks can be verified against the attacker. The AVISPA and HLPSL specifications can be found in detail in [34]. Various roles including the basic roles for user U_i (see Fig. 6), *GWN* (see Fig. 7) and SN_j (see Fig. 8), and the mandatory roles for the session, goal and environment (see Fig. 9) are implemented in HLPSL for the proposed scheme.

The implementation of our scheme is done on the basis of HLPSL [34] used in AVISPA. The more detailed information regarding AVISPA architecture and HLPSL are available [33].

```
%%% Role for GWN
role gwn (Ui, GWN, Sn : agent,
H: hash_func,
Snd, Rcv: channel(dy))
% Player: the GWN
played_by GWN
def= local State: nat,
IDi, PWi, Alphai, B, V, Regi, Ni, Mi, Tau, Li: text,
PWi1, DIDi, K, Ai : text,
T1, R1, R2, T2, T3, T4 : text,
Bi, SK, Ci, Fi : text,
E, F: hash_func
Xa, Xs: text,
const sp1, sp2, gwn_sn_r2, gwn_sn_t2,
sn_gwn_t3, gwn_ui_t3, gwn_ui_t4: protocol_id
init State := 0
transition
% Receive the login request message from Ui openly
1. State = 0 /\ Rcv(H(IDi.R1').H(B.Alphai).E(xor(H(IDi.H(PWi.B'.Alphai')),
xor(H(Xa'.IDi),H(IDi.H(PWi.B.Alphai'))) ),DIDi',R1',T1').T1') =|>
State' := 2 /\ secret({IDi,PWi, B', Alphai'}, sp1, {Ui})
/\ secret({Xa}, sp2, {Ui,GWN})
/\ R2' := new() /\ T2' := new()
/\ Mi' := xor(H(Xs.IDsnj),R2')
/\ Bi' := H(DIDi'.R2'.H(Xs.IDsnj).IDsnj.T2')
% Send authentication request message Message2 to Sn openly
/\ Snd(Mi'.DIDi.Bi.T2')
% GWN has freshly generated the values R2 and T2 for Sn
/\ witness(GWN, Sn, gwn_sn_r2, R2')
/\ witness(GWN, Sn, gwn_sn_t2, T2')
% receive authentication request message Message3 from Sn openly
/\ Rcv(H(H(Xs.IDsnj).H(DIDi'.H(Xs.IDsnj).R2.T2).
DIDi.IDsnj'.T3').xor(xor(SK',DIDi'),R2').T3')
% Sn has freshly generated the value T3 for GWN
/\ witness(Sn, GWN, sn_gwn_t3, T3')
/\ request(Ui, GWN, ui_gwn_t1, T1')
end role
```

FIGURE 7. Role for the *GWN*.

```
%%% Role for sensor node Sn
role sensor (Ui, GWN, Sn : agent,
H: hash_func,
Snd, Rcv: channel(dy))
% Player: sensor node Sn
played_by Sn
def= local State: nat,
IDi, PWi, Alphai, B, V, Regi, Ni, Mi, Tau, Li: text,
PWi1, DIDi, K, Ai : text,
T1, R1, R2, T2, T3, T4 : text,
SK, Ci, Fi : text,
E : hash_func
Xa, Xs: text,
const sp1, sp2, gwn_sn_r2, gwn_sn_t2, sn_gwn_t3: protocol_id
init State := 0
transition
% Receive authentication request message Message2 from GWN openly
1. State = 0 /\ Rcv(xor(H(Xs.IDsnj),R2').DIDi'.H(DIDi'.R2'.
H(Xs.IDsnj).IDsnj.T2').T3') =|>
State' := 3 /\ secret({IDi,PWi, B', Alphai'}, sp1, {Ui})
/\ secret({Xs}, sp2, {GWN,Sn})
/\ T3' := new()
/\ SK' := H(DIDi'.H(Xs.IDsnj).R2.T2)
/\ Fi' := xor(xor(SK',DIDi'),R2')
/\ Ci' := H(H(Xs.IDsnj).H(DIDi'.H(Xs.IDsnj).R2.T2).DIDi.IDsnj'.T3')
% Send authentication reply message Message3 to GWN openly
/\ Snd(Ci'.Fi'.T3')
% Sn has freshly generated the value T3 for GWN
/\ witness(Sn, Ui, sn_ui_t3, T3')
% Sn's acceptance of the values R2 and T2 generated for Sn by GWN
/\ request(GWN, Sn, gwn_sn_r2, R2')
/\ request(GWN, Sn, gwn_sn_t2, T2')
end role
```

FIGURE 8. Role for sensor nodes SN_j.

The proposed scheme is simulated with the help of the Security Protocol ANimator for AVISPA (SPAN) [50], [51], and using the widely-accepted OFMC and CL-AtSe back-ends. At present, both SATMC and TA4SP back-ends do not support bitwise XOR operation. Thus, the simulation results

```
%%% Role for the session
role session (Ui, GWN, Sn : agent,
SKuigwn : symmetric_key,
H: hash_func)
def=
local Sn1, Sn2, Sn3, Sn4, Rv1, Rv2, Rv3, Rv4 : channel (dy)
composition
GWN (Ui, GWN, Sn, SKuigwn, H, Sn1, Rv1)
/\ user (Ui, GWN, Sn, SKuigwn, H, Sn2, Rv2)
/\ gwn (Ui, GWN, Sn, H, Sn3, Rv3)
/\ sensor (Ui, GWN, Sn, H, Sn4, Rv4)
end role
%%% Role for the goal and environment
role environment()
def=
const ui, gwn, sn: agent,
skuigwn : symmetric_key,
h, f : hash_func,
didi,regi,ai,mi,bi,ci,di,fi,
t1, t2, t3, t4: text,
sp1, sp2, sp3, sp4, ui_gwn_r1, ui_gwn_t1, gwn_snj_r2,
gwn_sn_t2, sn_gwn_t3, gwn_ui_t4 : protocol_id
intruder_knowledge = {ui, gwn, sn, h, f,
didi,regi,ai,mi,bi,ci,di,fi,
t1, t2, t3, t4}
composition
session(ui, gwn, sn, skuigwn, h)
/\ session(i, gwn, sn, skuigwn, h)
/\ session(ui, i, sn, skuigwn, h)
/\ session(ui, gwn, i, skuigwn, h)
end role
goal
%%% Confidentiality (privacy)
secrecy_of sp1, sp2, sp3, sp4
%%% Authentication
authentication_on ui_gwn_r1, ui_gwn_t1
authentication_on gwn_sn_r2, gwn_sn_t2, gwn_ui_t4
authentication_on sn_gwn_t3
end goal
environment()
```

FIGURE 9. Role for the session, goal and environment.

```
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite\results\proof_wsn_scheme.if
GOAL
  as specified
BACKEND    OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 54.43s
  visitedNodes: 9327 nodes
  depth: 6 plies
```

FIGURE 10. The result of OFMC backend.

of the proposed scheme under these SATMC and TA4SP back-ends are reported as inconclusive. Therefore, we omitted the simulation results for these backends in this paper. Fig. 10 represents the results under OFMC gives out to be 9327 nodes are visited with the search time is 54.43 seconds, and the depth is 6 *plies*. From the result, it is clear that our scheme demonstrates safe and secure. The simulation results provided in Fig. 10 assure that the proposed scheme satisfies the design properties, and is secure against both replay and man-in-the-middle attacks.

C. INFORMAL SECURITY ANALYSIS

Here, this section deals with rigorous analysis where we demonstrate our scheme is capable of handling the following attacks.

1) PRIVILEGED-INSIDER ATTACK [47]

In the registration phase, as a part of registration the user U_i submits $< Reg_i, ID_i, \overline{PW_i} >$ to GWN, where $\overline{PW_i} = h(PW_i||b||\alpha_i)$, $Reg_i = h(b||\alpha_i)$. So, the privileged insider at GWN does not come to know the password of the user applying for registration, he cannot obtain PW_i from $\overline{PW_i}$ due to the colliion resistant one-way property of the hash function, and he cannot guess PW_i from $\overline{PW_i}$ without knowing the random strings b, α_i. Hence, our scheme resists the privileged insider attack.

2) USER ANONYMITY [46], [47]

Considering the threat model into account, we suppose $\mathcal{A}$ captures the communicated messages from U_i, GWN, and S_n, respectively. The messages $\{DID_i, Reg_i, A_i, T_1\}$, $\{MM_i, DID_i, B_i, T_2\}$, $\{C_i, F_i, T_3\}$ and $\{D_i, T_4\}$ consist of user's identity information, which is masked using the hash function as $DID_i = h(ID_i||R_1)$. Thus, without the knowledge of R_1 and biometric value α_i (which only the legitimate user can know/compute), it is computationally infeasible for any $\mathcal{A}$ to derive the valid user's identity ID_i. As a result, our scheme holds the user anonymity property.

3) BIOMETRIC/PASSWORD GUESSING ATTACK [40], [48], [52]

We have made use of biometric fuzzy extractor to get α_i value and make use of it in the computation of $\overline{PW}_i = h(PW_i||b||\alpha_i)$. Furthermore, the verification of $M_i \stackrel{?}{=} h(\overline{PW}_i||v)$. This shows that $\mathcal{A}$ cannot gain any advantage, as guessing and computation of α_i and PW_i in M_i is like solving the inverting hash function values. Thus, it is computationally infeasible for an $\mathcal{A}$ to guess the user's credentials. Thus, our scheme is free from the password guessing and biometric key guessing attack.

4) USER IMPERSONATE ATTACK [44], [45]

From the practical point-of-view an active attacker can traps the login message $Message_1 = < DID_i, Reg_i, A_i, T_1 >$ of U_i during the execution of the protocol, where $DID_i = h(ID_i||R_1)$, $Reg_i = h(b||\alpha_i)$, $A_i = E_k(DID_i, R_1, T_1)$. $\mathcal{A}$ may tries to extract or produce some valid message/information in order to make GWN believe $\mathcal{A}$ as authentic. In order to do so, $\mathcal{A}$ needs to compute valid message $Message_1$. As $\mathcal{A}$ cannot compute $< DID_i, Reg_i, A_i >$, without the knowledge of $< ID_i, \alpha_i, b, R_1 >$ and secret parameters $< v, k >$. This results in computationally infeasible for $\mathcal{A}$ to forge/guess the trapped message in a polynomial time. Thus, our scheme resists user impersonation attack.

5) GATEWAY NODE IMPERSONATION ATTACK [20], [53]

Suppose that the attacker obtains all transmitted message such as $\{DID_i, Reg_i, A_i, T_1\}$ and $\{MM_i, DID_i, B_i, T_2\}$ and tries to impersonate as a legal gateway node. However, It is not feasible to decrypt the $A_i = E_k(DID_i, R_1, T_1)$ without the symmetry key k. Therefore, the attacker cannot impersonate as a valid gateway node.

6) RESIST THE NODE CAPTURE ATTACK [42], [43], [49]

Suppose that the attacker captures the sensor node. Every sensor S_j has its own identity SID_n and secret number x_s. There is no relation among the identities and secret numbers of the sensors. So even if some sensors are captured by $\mathcal{A}$, it is hard for $\mathcal{A}$ to pretend to be other sensors.

7) DENIAL-OF-SERVICE ATTACKS [20], [48], [54]

Let us assume, an attacker captures user's smart card, and apply the power analysis and extract the stored information from it. To deliver denial of service attack, attacker tries to modify the password. But, the attacker fails to update/ modify the user's password as a secure verification steps are performed during password change phase. If the attacker needs to login using user's credentials, the attacker has to guess/know both user ID_i and PW_i. Therefore, our proposed scheme is secure for denial of service attack.

8) MUTUAL AUTHENTICATION AND SESSION KEY AGREEMENT [40], [41], [55]

We divide this property into three cases:

1. GWN checks W_i to authenticate U_i.
2. SN_j checks W_g to authenticate GWN directly and U_i indirectly.
3. U_i checks V_s to authenticate SN_j directly and GWN indirectly.

Thus, this is clear from the above, our proposed scheme perfectly implement mutual authentication and agree on a session key $SK = h(h(ID_i\|R_1)\|h(x_s\|SID_n)\|R_2\|T_2)$.

9) KNOWN SESSION SPECIFIC RANDOM NUMBER LEAKAGE ATTACK [50], [52], [56]

We suppose that, attacker $\mathcal{A}$ captures the transmitted messages $\{DID_i, Reg_i, A_i, T_1\}$, $\{MM_i$,DID_i,B_i,$T_2\}$, $\{C_i, F_i, T_3\}$ and $\{D_i, T_4\}$ and tries to compute the session key $SK = h(h(ID_i\|R_1)\|h(x_s\|SID_n)\|R_2\|T_2)$. Here $\mathcal{A}$ needs to possess the required parameters such as $ID_i, R_1, R_2, x_s, SID_n$. By some means, the attacker may get the session specific random numbers R_1 and R_2 but only knowing R_1 and R_2 will not give any advantage to the attacker as $\mathcal{A}$ cannot compute the required session key with R_1 and R_2. It is observed that, $\mathcal{A}$ may also require the long-term secret x_s of the cloud server and cloud sensor identity SID_n. This shows, it is computationally infeasible for an attacker to compute the session key $SK = h(h(ID_i\|R_1)\|h(x_s\|SID_n)\|R_2\|T_2)$. This shows, that our scheme has the potential to resist known session specific random number leakage attack.

10) MAN-IN-THE-MIDDLE AND REPLAY ATTACKS [38], [39]

We suppose that, attacker $\mathcal{A}$ captures the transmitted messages $\{DID_i, Reg_i, A_i, T_1\}$, $\{MM_i$,DID_i,B_i, $T_2\}$, $\{C_i, F_i, T_3\}$ and $\{D_i, T_4\}$ and tries to replay it in order to launch a valid session on behalf of a legal user U_i with S_n. Due to the applicability of timestamp and dynamic parameters, replaying the transmitted message is invalid as they fail to clear the verification of timestamp threshold. On receiving the messages a verification of the timestamp is done, which restrict the replay attack. This shows, that our scheme has the potential to resist replay attack. Furthermore, as the attacker $\mathcal{A}$ does not have the knowledge of the parameter $< ID_i, \alpha_i, b, R_1 >$ and secret parameters $< v, k >$, $\mathcal{A}$ fails to compute a valid session key. Thus, our scheme has the potential to resist man-in-the-middle attack.

VIII. RESULTS: PERFORMANCE COMPARISON WITH RELATED SCHEMES

This section talks about the performance of our proposed scheme based on the security and functional features, the storage cost utilized by the smartcard and communication cost taken during the transmission of messages. The details are as follows:

TABLE 6. Comparison of security requirements/functional attributes.

Security attributes	[11]	[12]	[15]	[27]	[33]	[19]	[20]	Our
Replay attack	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*Yes*
User anonymity	*No*	*No*	*No*	*No*	*No*	*No*	*Yes*	*Yes*
Mutual authentication	*Yes*	*No*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*Yes*
Stolen smartcard attack	*Yes*	*No*	*Yes*	*No*	*No*	*No*	*No*	*Yes*
Impersonation attack	*Yes*	*No*	*No*	*No*	*No*	*Yes*	*No*	*Yes*
Lack of Dynamic node addition	*No*	*No*	*Yes*	*No*	*Yes*	*Yes*	*No*	*Yes*
Efficient Password/Biometric change	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Forgery attack	*No*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*No*	*Yes*
Session key agreement	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*No*	*Yes*
Man − in − the − middle attack	*Yes*	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*Yes*
Denial of Service	*Yes*	*Yes*	*No*	*Yes*	*Yes*	*No*	*Yes*	*Yes*
Sensor node capturing	*Yes*	*No*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Biometric/Password guessing attack	*No*	*No*	*No*	*Yes*	*No*	*Yes*	*No*	*Yes*
Privileged − insider attack	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*Yes*

A. COMPARISON OF SECURITY REQUIREMENTS/ FUNCTIONAL ATTRIBUTES

As shown in Table 6, our scheme preserves and resists many of the existing attacks in WSNs. Moreover, in comparison we have also shown that the earlier existing schemes like [9], [11], [12], [17], [19], [20], [26], and [35] fails to achieve/resist the important security attributes to ensure the security of their proposed schemes. Thus, our scheme proves to be efficient in terms of security and functional attributes.

B. COMMUNICATION COST AND SMART CARD STORAGE COST COMPARIONS AND ANALYSIS

In Table 8, we have presented the communication cost and the smart card storage of the proposed scheme along with other related schemes [9], [11], [12], [17], [19], [20], [26], [35]. For computing the smart card storage cost and communication cost, we consider the output of 20 bytes for $h(\cdot)$, if we choose SHA-1 hashing algorithm [36]. And for timestamp, random nonce/random number, identity of user/sensor node we consider 19 bytes. For acknowledgement 20 bytes.

The schemes [9], [19], [20], [26] require less communication cost and [19], [20] require less smart card storage cost over the proposed scheme. But, we have seen in security features section that these schemes [9], [19], [20], [26] are vulnerable to various security attacks and also do not provide the tabled security attributes. To pay some extra cost for better security features and functionalities is well justified and hence our protocol is better and suitable for real life applications. A graphical representation of communication cost and storage cost is shown in Fig. 11.

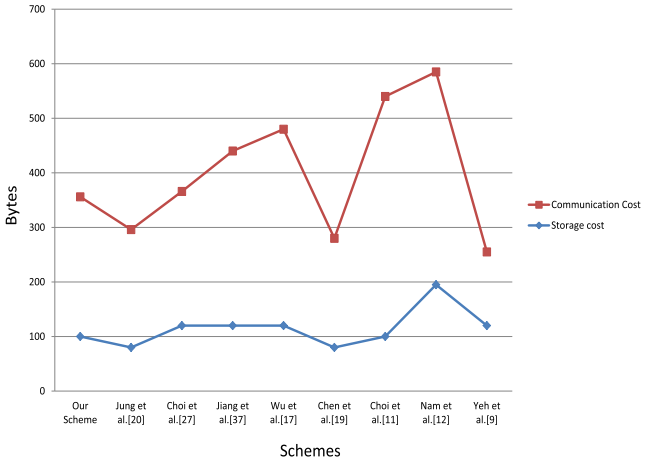

FIGURE 11. Communication cost and smart card storage cost comparison.

TABLE 7. Approximate time required for various operations [37].

Notation	Description (Time to compute)	Approximate computation time (in ms)
T_h	Hash function	0.0004
$T_{E/D}$	Symmetric key encryption/decryption AES-128	0.1303
T_{ECCM}	ECC point multiplication	7.3529
$T_{MAC} \approx T_h$	Message Authentication Code	0.0004

TABLE 8. Comparison of smart card storage cost and communication cost.

Scheme	Smartcard Storage cost	Messages during AKA	Communication cost
Our scheme	100 Bytes	4	256 Bytes
[20]	80 Bytes	4	216 Bytes
[27]	120 Bytes	3	246 Bytes
[37]	120 Bytes	4	320 Bytes
[17]	120 Bytes	4	360 Bytes
[19]	80 Bytes	4	200 Bytes
[11]	100 Bytes	4	440 Bytes
[12]	195 Bytes	5	390 Bytes
[9]	120 Bytes	3	135 Bytes

C. COMPARISON OF COMPUTATION COST

We have followed, the experimental results [37] which were applied using MIRACL C/C++ Library over the system compatible to 32-bit Windows 7 operating systems, Visual C++ 2008 Software.

The experiment results shows that, for symmetric key encryption/decryption AES-128 $T_{E/D} \approx 0.1303$ ms, for elliptic curve point multiplication over the finite prime field F_p it took $T_{ECC} \approx 7.3529$ ms, and for SHA-1 $T_h \approx 0.0004$ ms, respectively. An illustration of the experimental results are shown in Table 7.

In comparison to earlier proposed schemes, the proposed scheme consumes much lesser computation cost, such as 0.5219ms as discussed in Table 9. It is very clear from the comparison our scheme results more efficient than [9], [11], [12], [17], [26], and [35] with computation cost 29.9432 ms, 44.1242 ms, 29.9432 ms, 44.125 ms, 44.5131 ms, and 58.8264 ms. Though our scheme takes a bit slightly more computations than Chen *et al.*'s and Jung *et al.*'s scheme, our scheme preserves and resists the attacks which exists in the network, whereas the other schemes were proven to be vulnerable to achieve security requirements as shown in the Table 4. A graphical representation of the comparison is given in Fig. 12. Thus, our scheme proves to be more reliable due to the security and performance.

TABLE 9. Computation costs comparison during the login and authentication phases.

Scheme	Gateway node	Sensor node	User	Total	Time(ms)
Our scheme	$5T_h + 2T_{E/D}$	$3T_h$	$6T_h + 2T_{E/D}$	$14T_h + 4T_{E/D}$	0.5219
[20]	$5T_h + 2T_{E/D}$	$3T_h$	$5T_h + 2T_{E/D}$	$13T_h + 4T_{E/D}$	0.5215
[27]	$10T_h + 2T_{E/D}$	$6T_h + T_{E/D} + 2T_{ECC}$	$10T_h + T_{E/D} + 2T_{ECC}$	$26T_h + 4T_{E/D} + 4T_{ECC}$	29.9432
[37]	$8T_h + T_{ECC}$	$4T_h + 2T_{ECC}$	$5T_h + 3T_{ECC}$	$17T_h + 6T_{ECC}$	44.1242
[17]	$11T_h + 2T_{E/D}$	$4T_h + T_{E/D} + 2T_{ECC}$	$11T_h + T_{E/D} + 2T_{ECC}$	$26T_h + 4T_{E/D} + 4T_{ECC}$	29.9432
[19]	$5T_h + 2T_{E/D}$	$3T_h$	$2T_h + 2T_{E/D}$	$10T_h + 4T_{E/D}$	0.5217
[11]	$5T_h + T_{ECC}$	$6T_h + 2T_{ECC}$	$8T_h + 3T_{ECC}$	$19T_h + 6T_{ECC}$	44.125
[12]	$4T_h + 2T_{E/D} + T_{ECC}$	$3T_h + 2T_{ECC}$	$4T_h + T_{E/D} + 3T_{ECC}$	$12T_h + 3T_{E/D} + 6T_{ECC}$	44.5131
[9]	$4T_h + 4T_{ECC}$	$3T_h + 2T_{ECC}$	$1T_h + 2T_{ECC}$	$8T_h + 8T_{ECC}$	58.8264

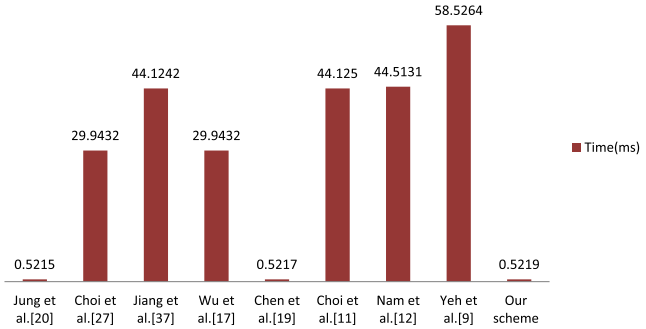

FIGURE 12. Comparison of computation cost.

IX. CONCLUSION

Overall, this paper discusses about newly proposed Jung *et al.*'s symmetric cryptosystem based authentication and key agreement scheme and analyzes the shortcomings of Jung *et al.*'s scheme. The vulnerabilities such as Forgery attack, Password guessing attack, Traceability attack, and uninterested in preserving the Privacy of the session key draws out to be the security weaknesses in Jung *et al.*'s scheme. As a remedial measure we come up with suitable countermeasures applicable to Jung *et al.*'s scheme and also, we have presented a suitable biometric and symmetric cryptosystem based authentication and key agreement scheme for WSNs, which has the potential to resist the shortcoming in the aforementioned compared schemes as well as has the ability to preserve the other security attributes. Furthermore, our proposed scheme is facilitated with dynamic node addition feature, and an user-friendly password/biometric update facility. In addition, the security of our scheme is shown using the formal analysis procedures like BAN-logic and AVISPA. BAN-logic validates mutual authentication, and AVISPA simulation tool verifies for replay attack and man-in-the-middle attack. Furthermore, the informal security analysis is also presented to show our scheme can satisfy desired security attacks. Finally, the performance of our scheme is compared with the aforementioned schemes.

REFERENCES

[1] C.-Y. Chong and S. P. Kumar, "Sensor networks: Evolution, opportunities, and challenges," *Proc. IEEE*, vol. 91, no. 8, pp. 1247–1256, Aug. 2003.

[2] Y.-X. Li, L. Qin, and Q. Liang, "Research on wireless sensor network security," in *Proc. Int. Conf. Comput. Intell. Secur.*, Dec. 2010, pp. 493–496.

[3] C. Buratti, A. Conti, D. Dardari, and R. Verdone, "An overview on wireless sensor networks technology and evolution," *Sensors*, vol. 9, no. 9, pp. 6869–6896, Aug. 2009.

[4] X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 8, pp. 1390–1397, Aug. 2011.

[5] J. Srinivas, D. Mishra, S. Mukhopadhyay, and S. Kumari, "Provably secure biometric based authentication and key agreement protocol for wireless sensor networks," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 4, pp. 875–895, 2017.

[6] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "A self-verifiable password based authentication scheme for multi-server architecture using smart card," *Wireless Pers. Commun.*, vol. 96, no. 4, pp. 6273–6297, 2017.

[7] S. Kumari, M. K. Khan, and M. Atiquzzaman, "User authentication schemes for wireless sensor networks: A review," *Ad Hoc Netw.*, vol. 27, pp. 159–194, Apr. 2015.

[8] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[9] H. Yeh, T. Chen, P. Liu, T. Kim, and H. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, May 2011.

[10] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 4, p. 730831, 2013.

[11] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10081–10106, 2014.

[12] J. Nam, M. Kim, J. Paik, Y. Lee, and D. Won, "A provably-secure ECC-based authentication scheme for wireless sensor networks," *Sensors*, vol. 14, no. 11, pp. 21023–21044, 2014.

[13] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016, doi: 10.1016/j.adhoc.2015.05.014.

[14] R. Amin and G. Biswas, "A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks," *Ad Hoc Netw.*, vol. 36, pp. 58–80, Jan. 2016.

[15] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Oct. 2016.

[16] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Netw.*, vol. 20, pp. 96–112, Sep. 2014.

[17] F. Wu, L. Xu, S. Kumari, and X. Li, "A new and secure authentication scheme for wireless sensor networks with formal proof," *Peer-Peer Netw. Appl.*, vol. 10, no. 1, pp. 16–30, 2015.

[18] Q. Jiang, J. Ma, X. Lu, and Y. Tian, "An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 8, no. 6, pp. 1070–1081, Jun. 2014.

[19] L. Chen, F. Wei, and C. Ma, "A secure user authentication scheme against smart-card loss attack for wireless sensor networks using symmetric key techniques," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 4, p. 704502, 2015.

[20] J. Jung, J. Kim, Y. Choi, and D. Won, "An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 8, p. E1299, 2016.

[21] J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," *Ad Hoc Netw.*, vol. 54, pp. 147–169, Jan. 2017.

[22] S. Jangirala, S. Mukhopadhyay, and A. K. Das, "A multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards," *Wireless Pers. Commun.*, vol. 95, no. 3, pp. 2735–2767, 2017.

[23] D. Dolev and A. Yao "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[24] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990.

[25] C. T. Li, C. Y. Weng, and C. C. Lee, "An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks," *Sensors*, vol. 13, pp. 9589–9603, Jul. 2013.

[26] Y. Choi, Y. Lee, and D. Won, "Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 1, p. 8572410, 2016.

[27] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology-CRYPTO* (Lecture Notes in Computer Science), vol. 1666. 1999, pp. 388–397.

[28] S. Kalra and S. K. Sood, "Advanced password based authentication scheme for wireless sensor networks," *J. Inf. Secur. Appl.*, vol. 20, pp. 37–46, 2015.

[29] Q. Mi, J. A. Stankovic, and R. Stoleru, "Practical and secure localization and key distribution for wireless sensor networks," *Ad Hoc Netw.*, vol. 10, no. 6, pp. 946–961, 2012.

[30] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 35, no. 5, pp. 1646–1656, 2012.

[31] M. Abdalla, M. Izabachène, and D. Pointcheval, "Anonymous and transparent gateway-based password-authenticated key exchange," in *Cryptology and Network Security*. Springer, 2008, pp. 133–148.

[32] M. Burrows, M. Abadi, and F. R. S. R. M. Needham, "A logic of authentication," *Operating Syst. Rev.*, pp. 1–13, 1989.

[33] AVISPA. *Automated Validation of Internet Security Protocols and Applications*. Accessed: Jan. 2015. [Online]. Available: http://www.avispa-project.org/

[34] D. von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proc. APPSEM Workshop*, 2005, pp. 1–17.

[35] Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He, and N. Chilamkurti, "A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks," *Int. J. Netw. Manage.*, vol. 27, no. 3, p. e1937, 2016.

[36] *Secure Hash Standard*, Standard FIPS PUB 180-1, U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Apr. 1995. Accessed: Jul. 2015. [Online]. Available: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

[37] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security," *J. Ambient Intell. Humanized Comput.*, vol. 98, no. 1, pp. 101–116, 2016.

[38] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K.-K. R. Choo, "A robust and energy efficient authentication protocol for industrial Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1606–1615, Jun. 2017.

[39] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2017.

[40] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and A. K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018.

[41] X. Li, J. Niu, J. Liao, and W. Liang, "Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update," *Int. J. Commun. Syst.*, vol. 28, no. 2, pp. 374–382, 2015.

[42] S. Challa *et al.*, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 69, pp. 534–554, Jul. 2017.

[43] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks," *Wireless Pers. Commun.*, vol. 94, no. 3, pp. 1899–1933, 2017.

[44] F. Wu *et al.*, "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment," *J. Netw. Comput. Appl.*, vol. 89, pp. 72–85, Jul. 2017.

[45] S. Kumari *et al.*, "On the design of a secure user authentication and key agreement scheme for wireless sensor networks," *Concurrency Comput., Pract. Exper.*, vol. 29, no. 23, pp. 1–24, 2017.

[46] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Secure Commun. Netw.*, vol. 9, no. 16, pp. 3670–3687, 2016.

[47] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Gener. Comput. Syst.*, vol. 63, pp. 56–75, Oct. 2016.
[48] A. K. Das, A. K. Sutrala, S. Kumari, V. Odelu, M. Wazid, and X. Li, "An efficient multi-gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 2070–2092, 2016.
[49] F. Wu, L. Xu, S. Kumari, and X. Li, "An improved and provably secure three-factor user authentication scheme for wireless sensor networks," *Peer-Peer Netw. Appl.*, vol. 11, no. 1, pp. 1–20, 2018.
[50] J. Srinivas, A. K. Das, N. Kumar, and J. Rodrigues "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2018.2828306.
[51] *AVISPA-SPAN. The Security Protocol ANimator for AVISPA*. Accessed: Sep. 2018. [Online]. Available: http://www.avispa-project.org
[52] S. Kumari, X. Li, F. Wu, A. K. Dasm, K.-K. R. Choo, and J. Shen, "Design of a provably secure biometrics-based multi-cloud-server authentication scheme," *Future Gener. Comput. Syst.*, vol. 68, pp. 320–330, Mar. 2017.
[53] S. Kumari, "Design flaws of 'an anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography,'" *Multimedia Tools Appl.*, vol. 76, no. 11, pp. 13581–13583, 2017.
[54] S. Kumari, M. K. Khan, and X. Li, "An improved remote user authentication scheme with key agreement," *Comput. Elect. Eng.*, vol. 40, no. 6, pp. 1997–2012, 2014.
[55] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *J. Supercomput*, pp. 1–26, 2017.
[56] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things," *IEEE Trans. Dependable Secure Comput.*, to be published, doi: 10.1109/TDSC.2018.2857811.
[57] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 708–722, Jul./Aug. 2016.

MAJID ALOTAIBI received the Ph.D. degree from The University of Queensland, Brisbane, QLD, Australia. He is currently an Assistant Professor with the Department of Computer Engineering, Umm al-Qura University. His current research interests include mobile computing, mobile and sensor networks, wireless technologies, ad hoc Networks, computer networks (wired/wireless), RFID, and nano electronics.