International Journal of Healthcare Information Systems and Informatics
Volume 16 • Issue 2 • April-June 2021

A Secure IoT-Based Mutual Authentication for Healthcare Applications in Wireless Sensor Networks Using ECC

Deepti Singh, NSIT, New Delhi, India
Bijendra Kumar, Netaji Subhas University of Technology, Delhi, India
Samayveer Singh, National Institute of Technology, Jalndhar, India
Satish Chand, JNU, New Delhi, India

ABSTRACT

The role of wireless medical sensor networks (WMSNs) is very significant in healthcare applications of IoT. Online report generation and sharing the reports reduce the time and make the treatment of patients very fast. Here, the safety of patient data plays a crucial role. As there is a restriction of resources in sensor nodes, the design of authentication scheme for WMSNs is not an easy task in healthcare applications. Healthcare professionals are using their mobile to collect data from patients' bodies. To use WMSNs in healthcare applications, cryptanalysis of Li et al. is done and found that it suffers from various attacks. Hence, a new efficient privacy-preserving user authenticated scheme using elliptic curve cryptography (ECC) is proposed. The security analysis of scheme is performed using random oracle model, in addition to BAN logic. AVISPA is used for simulation to prove that the proposed scheme can resist passive and active attacks. Finally, the performance comparison of schemes shows that the proposed scheme performs better.

KEYWORDS

AVISPA, BAN Logic, ECC, IoT, Security, Session Key, User Authentication, WSNs

1. INTRODUCTION

WMSNs play a crucial role in internet of things (IoT) and are extensively used in a lot of healthcare applications to collect the information/data of the observing patients' body. IoT is an evolving technology that makes remote sensing a reality. But, owing to wireless network and limitation of resources in sensor nodes, it's difficult to assure that authorised user only reads the sensitive data is an essential task in IoT atmosphere (Zhu & Huang, 2017). Certain authentication schemes have been proposed to care for this problem. However, earlier schemes possess their flaws, such as susceptible to one or the other attacks or not providing feature like user anonymity. To have secure communication between user and sensor, user authentication scheme with security protection for healthcare applications is designed in this paper.

Usually, WMSNs is designed by a user or healthcare professionals like nurses or doctor, gateway node (GWN) and many sensor nodes through a wireless channel, in which sensors are used to gather data for a particular patient and then these data are to be forwarded to designated professional [(Singh, Singh, Kumar & Chand, 2018)]. Usually, sensor nodes have restricted resources like storage,

DOI: 10.4018/IJHISI.20210401.oa2

computing power etc. while GWN has no resource limitation (Singh & Singh, 2018). Hence, the authenticity of a user (or patient) is the main test for safety of IoT in WMSNs. Along with key management (Fakhrey, Tiwari, Johnston & Al-Mathehaji, 2016) authentication is also required for verification of legitimate user in WMSNs, as a main safety mechanism. The main idea is that user, GWN and the sensor should be mutually authenticated to each other. The user can start a session by doing user registration, followed by login to GWN, and then GWN may request a sensor node to gather information wished by user. At successful verification, user accepts message from GWN (Singh, Singh, Kumar, & Chand, 2018), (Singh, Kumar, Singh, Chand, 2019). But, wireless sensor network (WSN) is prone to security attacks due to its wireless channel. Due to the limited capability of sensor, it makes cryptography algorithms like RSA not appropriate for WSN. Because of size and cost restrictions on sensors, there is a limitation on resources such as computation power, storage space, computation cost, and communication bandwidth.

Furthermore, applications of WSNs are very delicate concerning security. At the same time, it is expected that authentication scheme should possess most of the functionality features like mutual authentication, key agreement and should be safe against most of the security attacks. Hence, to design an efficient authentication scheme for WMSNs considering limited resources as well as security from various attacks is a big challenge. In this paper, a novel user authentication protocol using ECC that provides all well-known security features is proposed.

1.1 Elliptic Curve Over Prime Field GF(p)

Assume P is a large prime number. An elliptic curve $E_p(a,b)$ over galois field $GF(p)$ is explained by equation $y^2 = x^3 + ax + b$, where $a,b \in Z_p$ and $4a^3 + 27b^2 \neq 0(modp)$. All points on $E_p(a,b)$ and point O called infinity form an additive group G. A Hasse's theorem (Mahto, & Yadav, 2018) declares that points on $E_p(a,b)$ denoted by $\neq E$, and it fulfils the following inequality $p+1-2\sqrt{p} \leq p+1+2\sqrt{p}$. It can also be explained as an elliptic curve $E_p(a,b)$ over Z_p has approximately p points on it. If $P=(x_P, y_P)$ and $Q=(x_Q, y_Q)$ be two points in $E_p(a,b)$, then addition of *P* and *Q* is calculated as $R=P+Q=(x_R, y_R)$ and it is computed as follows:

$x_R = (\mu^2 - x_P - x_Q)(modp)$, $y_R = (\mu(x_P - x_R)(modp)$, Where

$\mu = \frac{y_Q - y_P}{x_Q - x_P}(mod\, p)$, $if\ P \neq -Q$ and $\mu = \frac{3xp^2 + a}{2y_P}(mod\, p)$, $if\ P \neq -Q$. If P is a generator of G then scalar multiplication $kP = P + P + \ldots P(k\,times)$.

Definition 1 (Elliptic Curve Discrete Logarithm Problem (ECDLP)): Given a point $Q \in G$, it is difficult to calculate discrete logarithm k such that $Q = kP$.

Definition 2 (Elliptic Curve Computational Diffie-Hellman problem (ECCDHP)): If there are two points $xP, yP \in G$ for $x, y \in Z_P$, it is difficult to calculate $xyP \in G$.

Definition 3 (Elliptic Curve Decisional Diffie-Hellman problem (ECDDHP)): If there are three points $xP, yP, zP \in G$, it is difficult to find whether $xyP = zP$, here $x, y, z \in Z_p^*$.

1.2. Contribution and Organization of Paper

The contributions of the proposed scheme are as follows:

- We have cryptanalyzed Li et al. (Li, Niu, Bhuiyan, Wu, Karuppiah & Kumari, 2018) and found that the scheme suffers from attacks like (1) smart card loss attack (2) insider (3) forward secrecy attack.
- A lightweight mutual authentication scheme has been designed that allows only a legitimate user to access the data from sensor node.
- A secured session key is shared among user, gateway node and sensor node session key is limited ti these stakeholders only.
- The proposed scheme is based on ECC as ECC provides better security feature with smaller key size as compared to another public key cryptosystem like RSA. All the credentials of the user are secure in the proposed scheme.
- In the proposed scheme, it is not required to store any secret credentials in the smart card.
- The informal security analysis that is non-mathematical security analysis is further done to ensure security of the designed scheme.
- This scheme is suitable for constrained environment of healthcare in WMSNs. Use of hash function also provides integrity to the messages.
- BAN logic and Random oracle model is used to prove security feature of our scheme. AVISPA is used as a simulation tool to provide formal security analysis of proposed scheme.
- Performance analysis and comparison is done with the recent schemes. The proposed scheme has the ability to withstand various security attacks and also provide additional functionality like mutual authentication.

The rest of the paper is as follows. In section 2, a brief about literature review is given. Section 3 reviews and section 4 provide some vulnerabilities of Li et al's protocol. In section 5, the proposed scheme is presented. Formal and Informal security analysis is done in section 6. In section 7, the performance of proposed scheme is compared with other schemes. At last, conclusion is mentioned in section 8.

2. LITERATURE REVIEW

A review is performed to obtain useful authentication schemes for the research. As per the need we have read abstract, proposed scheme, results and their conclusion. Once the reading was done, a decision was made to include the paper or not according to our criteria. Our criteria are to find user authentication schemes in WSNs. A thorough analysis of various schemes is done to find their merits and demerits. The information like communication cost, computation cost, and their safety from attacks is analysed and used for performance analysis with the proposed scheme. We have also considered various factors for comparison between different schemes like mutual authentication, user anonymity, session key agreement and resilience to various attacks like impersonation, smart card loss, forward secrecy etc. The password-based authentication scheme is widely used. In this type identity of the authentic users is verified only with the help of passwords. To access real-time information, Base station or Gateway node need to authenticate user and sensor node at the same time (Singh, Kumar, Singh, Chand, 2019). As sensor nodes have limited communication and computation ability, so a lightweight user authentication scheme is preferred. Various two-factor authentication scheme (2FAS) for WSNs were proposed. For 2FAS password and smart card are used by the user to access real-time information from sensor nodes (Wang, Li & Wang, 2018).

Watro et al. (Watro, Kong, Cuti, Gardiner, Lynn & Kruus, 2004) suggested a 2FAS using RSA and Diffie-Hellman key exchange algorithm. Wong et al. (Wong, Zheng, Cao & Wang, 2006) suggested a lightweight and less complicated hash-based scheme. It is the first password-based dynamic authentication scheme for WSNs that permits authentic users to request delicate information at every sensor of the network. It uses a lightweight function like hash function and exclusive-or operations. However, it was found by Das et al. that it is not safe against various attacks like replay, forgery and

stolen-verifier. Das et al. (Das, 2009) proposed an enhanced scheme that uses smart card. They also used temporal-credential based 2FAS that need less complex function like hash and XOR operation. In this a valid user should possess smart card and password for the verification purpose. But later, He et al. (He, Gao, Chan, Chen, & Bu, 2010) find that Das et al. cannot provide mutual authentication and it is also not safe against attacks like denial-of-service and sensor node capture attack. It is also prone to impersonation and insider attack. Then they proposed an improved scheme considering the above issues. Unfortunately, Kumar et al. (Kumar, & Lee, 2011) find that He et al. suffers from some problems like no session key agreement, no user anonymity and the problem of mutual authentication persists. Turkanovic et al. (Turkanović, Brumen & Hölbl, 2014) proposed a lightweight, energy efficient and secure 2FAS based on hash function. Biswas et al. (Amin, Islam, Biswas, Khan, Leng & Kumar, 2016) find that scheme (Turkanović, Brumen & Hölbl, 2014) is vulnerable to security attacks like smart card loss attack, offline identity and password guessing attack.

Gope and Hwang (Gope & Hwang, 2016) proposed a lightweight real-time anonymous protocol by considering attacks found in various previous schemes. It ensures various properties like user untraceability and perfect forward secrecy. Luo et al. (Luo, Wen & Su, 2018) find that in (Gope & Hwang, 2016) problem of de-synchronisation exists between GWN and sensor node which leads to non-authentication between them. The problem of clone card attack also exists in the scheme (Gope & Hwang, 2016). Xue et al. (Xue, Ma, Hong & Ding, 2013) uses a temporary credential to design authentication scheme. The temporal credential is obtained by taking hash of shared key between user and GWN, identity of user and expiry time of temporal credential. Although Xue et al. maintains various security properties. But later, Jiang et al. (Jiang, Ma, Lu, & Tian, 2015) find that Xue et al. is vulnerable to multiple attacks like insider attack, identity and password guessing attack. Then it is proved by Das at al. (Das, 2016) that Jiang et al. is insecure against insider attack and problem of de-synchronisation persist.

Wu et al. (Wu, Xu, Kumari, & Li, 2018) find that Das et al. (Das, 2016) has some significant problem in their scheme like user impersonation attack and offline password guessing attack. Wu et al. then designed an authentication scheme recently using ECC. Ryu et al. (Ryu, Song, Moon, Kim & Won, 2019) find that Wu et al. is not safe against user impersonation attack and can also not provide user anonymity. It is also exposed to outsider attack. Wu et al. (Wu, Xu, Kumari & Li, 2017) proposed a scheme for WSNs, which can also be implemented for internet of things. But it also suffers from attacks like impersonation, sensor node anonymity attack and problem of user traceability persist. Later, Jiang et al. (Jiang, Ma, Wei, Tian, Shen & Yang, 2016) designed an ECC based untraceable authentication scheme. In this ECC multiplication operation is performed only by user and GWN, but sensor only performs a simple one-way hash operation. But later Li et al. (Li, Niu, Bhuiyan, Wu, Karuppiah & Kumari, 2018) find that scheme (Jiang, Ma, Wei, Tian, Shen & Yang, 2016) suffers from attacks like Known session-specific temporary information attack and the problem of synchronisation also exists. Sutrala et al. propounded (Sutrala, Das, Kumar, Reddy, Vasilakos, & Rodrigues, 2018) a user authentication and key agreement scheme and also provided the formal and informal analysis of the scheme. Based on the flaws of previous work, three-factor authentication scheme for IoT applications is proposed. Through performance analysis and comparison with other schemes it can be easily seen that proposed scheme not only attain computational efficacy but also achieves a lot of security and functionality features.

3. LI ET AL.'S PROTOCOL

In the year 2018, Li et al. (Li, Niu, Bhuiyan, Wu, Karuppiah & Kumari, 2018) presented a three-factor authentication scheme for WSNs. Though Li et al. provide various attractive features, like the facility of user anonymity and local password update. But on cryptanalysis, it fails to accomplish many of the claimed properties. This scheme cannot preserve forward secrecy and is also prone to an insider attack.

Table 1. Symbols used in Li et al

Symbol	Meaning
U_i	User
SC	Smart card
ID_i	Identity of user
b_i	Biometric of user
r_i, r_s, r_j	Random no genertaed by user,sensor and gateway node
PW_i	Password of user
C	Codeword
SID_j	identity of sensor node
$h(.)$	One way hash function
$\oplus$	XOR operation
$\|\|$	Concatenation of message

3.1. Li et al.'s Scheme

This subsection will provide a brief about Li et al.'s (Li, Niu, Bhuiyan, Wu, Karuppiah & Kumari, 2018). The symbols used are given in Table 1. Li et al's scheme comprises of four key phases: registration, login, authentication, and password change. The details of the phases are given below:

3.1.1. Registration

For registration phase of this scheme, GWN defines a cyclic group $G = \langle P \rangle$ of order n, where n is a large prime number. G could be an elliptic curve group or prime order subgroup of Z_p^*. The GWN chooses x and K as its master secret key and $X = xp$ as its public key. In the end, GWN publishes $\{E(F_p), G, P, X\}$ and stores x, K securely.

3.1.1.1 Sensor Registration Phase

GWN selects a sensor node having identity SID_j and calculate the secret key $K_s = h(SID_j \| K)$ for each node. And, GWN inserts $\{SID_j, K_s\}$ in the memory of S_j, then the sensor node is deployed in the desired area.

3.1.1.2 User Registration Phase

This phase is executed, when a user wants to obtain information from sensor nodes. The following steps are needed to perform for registration of user:

Step 1: User selects ID_i, PW_i, b_i and nonce a_i and computes $RPW_i = h(PW_i \| a_i)$.
Step 2: User send message { ID_i, RPW_i,b_i } to the GWN.

Step 3: GWN computes $F(c_i, b_i) = (,)$ where $= h(c_i)$, $= h(c_i b_i)$, c_i belongs to C where C is a codeword for U_i. After that GWN also calculates $A_i = h(ID_i \| RPW_i \| c_i)$, $B_i = h(ID_i \| K)h(RPW_i \| c_i)$ and stores $<,, A_i, B_i, X, F(.)>$ in the smart card (SC). GWN sends smart card to the user. GWN saves ID_i and U_i stores nonce into their databases respectively.

3.1.2 Login and Authentication

The following steps are needed to generate session key among user, base station and sensor node.

Step 1: User enters biometric information and also inserts SC into reader. Then SC computes the value of $h(c_i) = ?$, where $c_i = F(b_i)$. If it is equal, user inputs ID_i, PW_i and compute and compare the value of A_i. If it is equal, user's identity and password is verified. Then SC computes $M_1 = B_i \; h(h(PW_i \| a_i) | c_i)$, $M_2 = sP$, $M_3 = sX = sxP$, $M_4 = ID_i \quad M_3$, $M_5 = M_1 \; r_i$, $M_6 = h(ID_i \; | | r_i) SID_j$ and $M_7 = h(M_1 \| \text{SID}_j \| M_3 \; || \quad r_i)$. User sends message $< M_2, M_4, M_5, M_6, M_7 >$ to GWN.

Step 2: GWN then checks for the identity of user in their database, if it is available then it also calculates and compare the value of M_7. If it is equal, GWN choses a random number r_g and computes $K_s = h(SID_j \; || \; K)$, $M_8 = ID_i \; K_s, M_9 = r_g \; h(ID_i \; | | K_s), \quad M_{10} = r_g \quad r_i$ and $M_{11} = h(ID_i \| SID_j \| K_s \| r_i \| r_g)$. GWN sends message $\langle M_8, M_9, M_{10}, M_{11} \rangle$ to sensor node.

Step 3: Sensor node calculates and compares for the value of M_{11}. If it is equal, Sensor node choses random number r_j and calculates $M_{12} = r_j K_s, \quad SK_j = h(ID_i \| SID_j \| r_g \| r_j \| r_i)$, $M_{13} = h(K_s \| SK_j \| r_j)$.SN sends message $\langle M_{12}, M_{13} \rangle$ to GWN.

Step 4: GWN then calculates and compares the value of M_{13}. If it is equal, GWN computes $M_{14} = M_1 r_g$, $M_{15} = r_i \quad r_j$ and $M_{16} = h(ID_i \| SK \| r_g \; || \; r_j)$. GWN sends the message $< M_{14}, M_{15}, M_{16} >$.

Step 5: User computes session key and also checks for the value of M_{16}. If it is equal, user and sensor achieve a shared session key.

4. CRYPTANALYSIS OF LI ET AL.

4.1. Smart Card Loss Attack

This scheme permits the user to select its own identity and password. It is assumed that user usually chooses easy and low entropy identity/ password. An adversary A can easily guess these pairs and can calculate the value of $A_i^* = h(ID_i^* \| PW_i^* \| a_i \| c_i \;)$ where $c_i = f(b_i)$ and a_i is obtained by A from lost smart card. An adversary A repeats this process until $A_i^* = A_i$.

4.2. Insider Attack

In this scheme, user uses his biometric data in a plaintext format to login. The administrator can use this login message to impersonate as user and hence this scheme is prone to insider attack.

4.3. Forward Secrecy Attack

As sensor node performs critical operations and stores sensitive information; It is likely to have sensor node capture attack to extract its secret key (K_s). With the secret key, an adversary A can easily get the previous session key. A can calculate the value of ID_i, r_g, r_i by intercepting the message sent from $\langle M_8, M_9, M_{10}, M_{11} \rangle$ GWN to sensor node. An adversary A can also compute the value of $SID_k = M_6\, h\left(ID_i\, r_i\right)$ by intercepting the login message sent from user to GWN.

5. PROPOSED SCHEME

In this section, user authentication for WMSNs using ECC is proposed. The sensor node(SNo) senses the real-time data and sends the sensed data to user (Um). In this registration center (RCk) is used for registration of Um and SNo. RCk is also responsible for generating secret key of gateway node (Gn) and SNo. The authenticity of Um and SNo is verified before actually transmitting the data. After mutual authentication, the communicating parties generate a shared session key to communicate with each other securely manner. The important point is that RCk is not involved during the authentication phase of this scheme. The symbols and their description are given in Table 2.

5.1. System Initialization Phase

In this, Gn selects a non-singular elliptic curve $E_p\left(a,b\right)$ and a base point P in a finite field $E_p\left(a,b\right)$, where p is a prime number. Let $G = \left\{p, E_p\left(a,b\right), P\right\}$ be an elliptic curve group created by P. Gn computes public key $Q = SnP$, then it declares $\left\{G, Q, h\left(.\right)\right\}$, where h(.) is the used hash function.

5.2. User Registration

For user registration, Um sends the registration request to gateway node Gn .After verification, user is registered and Gn provides SC to the user. The SC contains various information in the encrypted form including user's credentials. The following steps are executed for registration purpose:

Step 1: User Um choses identity IDm, password PWm, biometric BRm and a nonce Xu and sends $B1 = h(IDm \,||\, Xu)$, $B2 = h\left(PWm \left\| Xu \right\|\right)$, $Gen\left(BRm\right) = \left(,\right)$ to Gn through a safe channel.

Step 2: Gateway node Gn computes the following:

$C1 = h(B1 \,||\, T1)$, $C2 = h\left(B1 \left\| B2 \right\| IDn\right)$, $C3 = h(C1 \,||\, Xs)$ where $T1$ is the registration request time, IDn is the identity of Gn and $C3$ is the secret key of Um.

Step 3: Gn stores $\left\langle T1, Xu, IDn, C2, C3, h\left(.\right), \right\rangle$ in smart card and sends this to the user. Um also computes $C0 = \left(h\left(IDm \left\| PWm \right\|\right)\ Xu\right)$ and stores it in smart card SC. This completes the registration of user.

5.3. Sensor and Gateway Node Registration Phase

In this, SNo and Gn register themselves with registration center RCk. The subsequent steps are followed for registration:

Table 2. Symbols used in proposed scheme

Symbol	Meaning
Um	User
Gn	Gatewaynode
Sno	Sensor node
RCk	Registration centre
IDm, IDn, IDo	Identity of Um,Gn,SNo
PWm	Password of user
BRm	Biometric of user
Qu	Public key of user
SC	Smart card
Src	Secret key of registration centre
Xu, Xs, Xo	Random nonce of Um,Gn,SNo
$T1$	Registration time
Sn	Secret key of Gn
So	Secret key between Gn,SNo
TSi	Timestamp
$\oplus$	XOR operation
$h(.)$	One way hash function
$\|\|$	Concatenation of message

Step 1: RCk calculates secret key for Gn: $Sn = h(IDn \,||\, Src)$. Here IDn is the identity of Gn and Src is the secret key of registration center.

Step 2: RCk calculates shared secret key between Gn and SNo: $So = h(IDo \,||\, Src)$. Here IDo is the identity of the sensor node.

Step 3: RCk stores $\langle IDo, So \rangle$ in the memory of SNo and $\langle IDn, Sn, IDo, So \rangle$ in the memory of SNo. This completes the registration phase of sensor node and gateway node with registration centre.

5.4. Login Phase

For login, user needs to enter its identity IDm, password *PWm* and biometric *BRm*. Then smart card SC verifies its correctness and after verification, it is sent to Gn for login. After registration, Um can log in using the following steps:

Step 1: User Um enters $< IDm, PWm, BRm >$ and inserts smart card into card reader.
Step 2: Um selects one Gn to get access to the data from the nearest sensor node to Gn.
Step 3: Then smart card calculates the following information for verification of user:

1. $Rep\left(BRm,\right) =$
2. $Xu^{'} = (h(IDm \,||\, PWm \,||\,)\, C0$
3. $B1^{'} = h(IDm \,||\, Xu')$
4. $B2^{'} = h\left(PWm \| \| Xu'\right)$
5. $C2^{'} = h\left(B1^{'} \| B2^{'} \| IDn\right)$

Step 4: SC then compares the stored value $C2$ with the calculated value $C2^{'}$. If it is equal, user is verified, else session is terminated.
Step 5: SC calculates the following value and msg_1 is transmitted to Gn through a public channel.

1. $B3 = h\left(TS1 \| Xu \| IDn\right)$
2. $B4 = h(C3 || TS1 || Xu \,||\, Qu\,)$
3. $B5 = E_{B4.x}\left\{IDm \| Qu \| TS1\right\}$

Here, $B4.x$ is the x-co-ordinate of ECC point that can be decrypted at base station and $Qu = C3P$, where $C3$ is secret key and Qu is public key of the user.

Step 6: SC transmits message msg_1 $< IDn, IDo, B3, B4, B5, TS1 >$ to Gn. Here TS1 is the current timestamp.

5.5. Authentication Phase

In this phase, gateway node Gn first checks the authenticity of user Um and once it is verified then Gn sends the message to sensor node SNo. Then sensor checks authenticity of Gn. Once it is verified, SNo sends the authentication message to Gn to prove its authenticity. Then Gn sends reply message to user to verify its authenticity. In between the verification process, session key is also calculated by the entities. The authentication and key agreement are shown in Fig.1. In this scheme mutual authentication is obtained between user and sensor using the following steps:

Step 1: Gn computes the following after receiving msg_1, Gn checks if $\left|TS2 - TS1\right| \leq \Delta T$. $\triangle$T is the maximum permissible delay between the sender and receiver. If it's correct, Gn moves to step 2 else session is terminated.
Step 2: Gn computes

1. $h\left(TS1 \| Xu \| IDn\right)$ and compare this with received value of B3. If it is equal then it goes to next step.

Gn decrypts the value of $B5$ to get IDm' and this obtained value is compared with the actual identity of base station (IDm) .
Step 3: If they are equal then the user is verified. Gn computes the following:

1. $C4 = h\left(IDo \| C1 \| So \| Xs \| TS2\right)$
2. $C5 = h\left(Sn \| Xs \| C3 \| TS2 \,||\, Qs\right)$
3. $C6 = h\left(C5 \| C3 \| TS2 \| Xu \| IDm \,||\, Qs\right)$
4. $C7 = h\left(Xu \| Xs \| TS2\right) \oplus So$

Step 4: The gateway node Gn transmits message msg_2 < $C4, C5, C6, C7, IDo >$ to sensor SNo.

Step 5: After receiving msg_2, SNo computes the following: checks if $\left|TS2 - TS1\right| \leq \Delta T$.

Step 6: Then sensor SNo computes and compares the value of C4, C6 and also checks if |TS3-TS2|≤⋀T.If equal, calculate the value of session key: $S\_K = h\left(Sn \| Xs \| C3 \| Xu \| Xo \| So \| P\right)$, where Xo is random nonce and So is secret key of sensor node

Step 7: Then SNo compute the following:

1. $D1 = h\left(TS3 \| Xo \| So \| IDo \| S\_K\right)$.
2. $D2 = h(Xo \,||\, TS3) \oplus IDo$

Step 8: Sensor SNo sends message msg_3 < $D1, D2$ > to Gn.

Step 9: Gn after receiving the message, compute and compare the following:

1. $\left|TS4 - TS3\right| \leq \Delta T$.
2. $D1' = h\left(TS3 \| Xo \| So \| IDo \| S\_K\right), compare\, D1' = ?\, D1$
3. If they both are equal, sensor node is authenticated by Gn and it moves to next step else session is terminated here.

Step 10: Gn computes

1. $S\_K = h(Sn \| Xs \| C3 \| Xu \| Xo \,||\, So)$
2. $C8 = h(S\_K \,||\, C1 \| Xs \| TS4)$
3. $C9 = h(Xu \| Xs \| Xo \,||\, Sn) \oplus C3$

Step 11: Gn sends message msg_4 $\left\langle C8, C9 \right\rangle$ to the authenticated user Um.

Step 12: After receiving the message, SC computes and compares the following:

1. $\left|TS5 - TS4\right| \leq \Delta T$.
2. $S\_K = h(Sn \| Xs \| C3 \| Xu \| Xo \,||\, So)$
3. Compute and compare the value of C8 then it means user Um authenticates gateway node Gn and it moves to next step else session is terminated here.

Step 13: User saves the value of session key.

The authentication and session key established has been summarized in figure 1.

5.6. Password Change Phase

In this phase user can change his/her password. Whenever user feels that intruder modified the password, he/she must change the password. This phase should not involve any other participant for the security reasons and it would also save communication cost. The following steps are required to modify the password:

Step 1: Um enters its original identity and password.

Step 2: The SC calculates the following values:

1. $B1 = h(IDm \,||\, Nm)$,

2. $B2 = h\left(PWm \| \| Nm\right)$,
3. $Nm = (h(IDm \,||\, PWm \,||\, BRm) \oplus C4)$
4. $C2' = h\left(B1 \| B2 \| IDn\right)$,

Step 3: Then SC compares $C2' = ?\, C2$. If they are equal, user is verified else session is terminated. Now user provides new password and identity to the SC and calculates the following:

1. $C2' = h(B1 \| B2 \| IDn)$

$C3' = h\left(C1 \| Nn \| Sn\right) h(B1 \,||\, B2)$

2. $C4' = (h(IDm \,||\, PWm^{new}) \oplus Nm)$

Smart card then updates the value of C2, C3 and C4 in the storage space of smart card. Finally, new password of user is successfully updated.

5.7. Dynamic Node Addition Phase

The case may arise at some point of time that after proper establishment of sensor network, we need some additional node to be added to the existing network. The following steps are given below:

Step 1: The registration centre RCk chooses a new identity for the sensor node and computes $So^{new} = h(IDo^{new} \,||\, Src)$. Here IDo^{new} is the identity of new sensor node. RCk stores $\left\langle IDo^{new}, So^{new} \right\rangle$ in the memory of SNo^{new}.

Step 2: RCk sends $\left\langle IDo^{new}, So^{new} \right\rangle$ to the GWN for the registration purpose. GWN updates its database with this newly added sensor node. In this manner, a new node is successfully added.

6. SECURITY ANALYSIS

In this section, the security analysis of the proposed scheme is done. Firstly, we provide session key security using the Random Oracle model and then mutual authentication is proved with the help of BAN logic. The Random Oracle model uses Real-Or-Random model to prove semantic security that is session key secrecy among the communicating entities against an adversary or intruder. The BAN logic is used to justify mutual authentication among user, GWN and sensor node. The AVISPA tool is used for formal security analysis of our scheme. This also ensures that the scheme is safe against replay and man-in-the-middle attacks. Finally, non-mathematical study that is informal security analysis of proposed scheme is done to prove security against various well-known attacks.

6.1. Adversary Model

For formal security analysis the Real-Or-Random model is used in the proposed scheme. In our scheme user (Um), gateway node (Gn) and sensor node (SNo) are the three participating entities. The brief analysis is given as follows.

Participants: Let ${}^{r}_{Um}$, ${}^{s}_{Gn}$ and ${}^{t}_{SNo}$ be the instance of of user, GWN and sensor node.

Partnering: The instance of ${}^{r}_{Um}$, ${}^{s}_{Gn}$ and ${}^{t}_{SNo}$ belonging to Um, Gn, SNo are the partners. Let PID^{r}_{Um}, PID^{s}_{Gn} and PID^{t}_{SNo} be the partner id and SID^{r}_{Um} be the session id of the current session.

Freshness: If any adversary (ADq) does not compromise session key, then ${}^{r}_{Um}$, ${}^{s}_{Gn}$ and ${}^{t}_{SNo}$ are said to be fresh.

Figure 1. Authentication and session key agreement

User/ Smart Card	Base Station	Sensor node

Insert smart card,
Input IDm, PWm, BRm
Compute $Xu' = (h(IDm||PWm||\alpha) \oplus C0$
$B1' = h(IDm||Xu')$
$B2' = h(PWm||\alpha||Xu')$
$C2' = h(B1'||B2'||IDn)$
Compare $C2'$ with $C2$,
If equal, compute
$B3 = h(TS1||Xu||IDn), Qu = C3.P$
$B4 = h(C3//TS1//Xu||Qu)$
$B5 = E_{B4.x}\{IDm||Qu||TS1\}$

Message 1 $<IDo, B3, B4, B5, IDn, TS1>$ →

Check if $/TS2\text{-}TS1/ \leq \Delta T$
Compute $h(TS1||Xu||IDn)$,
compare it with B3. Also decrypt B5 and compare IDm.
If they both are equal, Compute,
$C4 = h(IDo||C1||So||Xs||TS2)$
$Qs = Sn.P$
$C5 = h(Sn||Xs||C3||TS2||Qs)$
$C6 = h(C5||C3||TS2||Xu||IDm||Qs)$
$C7 = h(Xu||Xs||TS2) \oplus So$

Message 2 $< C4, C5, C6, C7, IDo >$ →

Check if $/TS3\text{-}TS2/ \leq \Delta T$
Compute and compare the value
Of $C4, C6$
If equal, Compute $S\_K = h(Sn||Xs||C3||Xu||Xo||So)$
$D1 = h(TS3||Xo||So||IDo||S\_K)$
$D2 = h(Xo||TS3) \oplus IDo$

← *Message 3* $< D1, D2 >$

Compute $S\_K = h(Sn||Xs||C3||Xu||Xo||So)$
Compute and compare the value of $D1$,
If equal compute
$C8 = h(S\_K||C1||Xs||TS4)$
$C9 = h(Xu||Xs||Xo||Sn) \oplus C3$

← *Message 4* $< C8, C9 >$

If $|TS5 - TS4| \leq \Delta T$
Compute $h(Xu||Xs||Xo||Sn) = C9 \oplus C3$
$S\_K = h(Sn||Xs||C3||Xu||Xo||So)$
Stores S_K as session key

1. **Adversary:** The adversary ADq can execute below given queries:

- *Execute(* ^{r}, ^{s}, ^{t}*)*: This query simulates the login and authentication phase. ADq can get the copy of message exchanged among Um, Gn and SNo.
- *Send(* ^{s},m) : With this, ADq gets a normal response message after sending any message(m).
- *Test(* ^{s}) : For semantic security of session key this query is used. For example, if a coin is flipped in the beginning and its value is 1, the session key is sent to ADq else if its value is 0, any random value is sent to ADq .

(v) **Session key security:** In this ADq is challenged to differentiate between actual session key and any random value. ADq wins the game, if it has received correct session key. ADq can violate the semantic security of any authenticated key agreement scheme(S) is defined by $ADV_S^{AKE} = \left|2.\Pr\left[success\right]-1\right|$. Here success is that ADq can win the game. S can be secure if $ADV_S^{AKE} \leq$, where α is a very small number.

(vi) **Random oracle:** All the participants and an adversary are provided with h(.) function, where h(.) is a collision-resistant hash function. A table consisting of the form (r, s) is used for simulation of oracle. When query h(r) is received, s is only returned if (r,s) exists in the table, else a random string is returned.

6.2. Analysis Using Random Oracle Model

The lemma used for analysis in Random Oracle model is as follows:

Lemma 1: Let A, B, C denote the events in some probability distribution. Let us assume AB CD, then $|\Pr\left[A\right]-\Pr\left[B\right] \leq \Pr\left[C\right]$

Theorem 1: Let an adversary ADq runs in polynomial time T against scheme(S) in random oracle. Then the probability of ADq breaking the session key security is given by:

$$ADV_S^{AKE} \leq \frac{q_h^2}{\left|Hash\right|} + 2.ADV_{Gq}^{ECDDHP}\left(T\right).$$

Here, q_h denotes the number of hash queries, $\left|Hash\right|$ is output range of hash function and $ADV_{Gq}^{ECDDHP}\left(T\right)$ is advantage of ADq to break ECDDHP.

Proof: We use a game (G_0 to G_3), Success_Ei is the probability of adversary of guessing coin b to complete our verification. The analysis starts with G_0 and terminates at G_3 that concludes the benefit to breaking the safety of S is insignificant.

Game G_0: ADq performs this game against scheme S. The value of bit b needs to be taken at the beginning of this game. We have,

$$ADV_S = |\ 2.\Pr[\text{Success\_E0}]\text{-}1\ | \quad (1)$$

Game G_1: After transforming G_0 this game is obtained. This game denotes eavesdropping attack performed by an adversary ADq. Execute and Test Query is executed at the end. The output of test oracle decides about the actual session key or random number. The session key is computed as follows: S_K=h(Sn||Xs||C3||Xu||Xo||So). Therefore, an ADq should know all these values

like random numbers etc. Thus, without these information probabilities of eavesdropping attack is decreased. As a result, this game is equivalent to the above one and hence,

$$\Pr\left[\text{Success}\_\text{E1}\right] = \Pr\left[Success\_E0\right] \tag{2}$$

Game G_2: The simulation of Send and Test oracle transform Game G_1 to G_2. This G_2 model represents active attacks in which ADq tries to decide that participant will accept fabricated message or not. ADq tries to find if there is a hash collision or not. The entire communicating message contains a random nonce. As random nonce is not possible to be known by others, chances of a collision are minimised when an adversary ADq sends a query. According to the birthday paradox, it gives the following results.

$$\left|Pr\left[Success\_E1\right] - Pr\left[Success\_E2\right]\right| \leq q_h^2 \ / 2\left(\left|HASH\right|\right) \tag{3}$$

Game G_3: In this game, an adversary generates real session key using the communicated message among the participants. As session key is calculated as It is very tough or impossible for to verify the value of session key. Therefore,

$$\left|Pr\left[Success\_E2\right] - Pr\left[Success\_E3\right]\right| \leq ADV_{Gq}^{ECDDHP}\left(T\right) \tag{4}$$

Since session keys are random and not dependent on each other, and no facts regarding the coin is known by.

$$Pr\left[Success\_E3\right] = 1/2 \tag{5}$$

Solving equation (1)-(5) and lemma

$$\frac{1}{2}.ADV_S^{AKE} = \left|Pr\begin{bmatrix}Success\\ -E0\end{bmatrix} - \frac{1}{2}\right| \tag{6}$$

Using triangular inequality,

$$\left|Pr\left[Success\_E1\right] - Pr\left[Success\_E3\right]\right| \leq q_h^2 \ / 2\left(\left|HASH\right|\right) + ADV_{Gq}^{ECDDHP}\left(T\right) \tag{7}$$

Using equation (2), (5) and (8),

$$ADV_S^{AKE} \leq q_h^2 \ /\left(\left|HASH\right|\right) + 2.ADV_{Gq}^{ECDDHP}\left(T\right)$$

Thus, theorem validates that the proposed scheme is safe against attacks like dictionary, impersonation, replay, stolen verifier and MITM attack.

6.3. Authentication Proof Using BAN Logic

In this section, the security evaluation of proposed scheme is done based on BAN logic (Burrows, Needham Abadi, 1990). The symbols R, S as principals, U, V as formulas, T as statement and SK1 as key.

- $R \mid \circ T$: R believes statement T.
- $R \lhd T$: R can see statement T.
- # (U): U is fresh.
- $R \mid\sim T$: R once said statement T.
- $R \rhd T$: R controls statement T.
- $R \overset{SK1}{\leftrightarrow} S$: R and S uses shared secret key to communicate with each other. Any third party does not know it.
- $\{ T \}_{SK1}$: T is encrypted using key (SK1).
- $< T >_{U}$: T combined with U.
- (T,U): The statement T or U is part of formula (T,U).

Rules: BAN logic use following rule to prove the security of proposed scheme:

- Rule R_1 (Message meaning rule): $\dfrac{\mathrm{R} \mid\equiv \mathrm{R} \overset{SK1}{\leftrightarrow} \mathrm{S},\quad \mathrm{R}\{\mathrm{U}\}_{SK1}}{\mathrm{R} \mid \equiv \mathrm{S} \mid \equiv \mathrm{U}}$
- Rule R_2 (Freshness-conjuncatenation rule): $\dfrac{\mathrm{R} \mid\equiv \#(\mathrm{U})}{\mathrm{R} \mid\equiv (\mathrm{U},\mathrm{V})}$
- Rule R_3 (Session key rule): $\dfrac{\mathrm{R} \mid\equiv \#(\mathrm{U}).\mathrm{R} \mid\equiv \mathrm{S} \mid \equiv \mathrm{U}}{\mathrm{R} \mid\equiv \mathrm{R} \overset{SK1}{\leftrightarrow} \mathrm{S}}$
- Rule R_4 (Jurisdiction rule): $\dfrac{\mathrm{R} \mid\equiv \mathrm{S}\ \ \mathrm{U},\ \mathrm{R} \mid \equiv \mathrm{S} \mid\equiv \mathrm{U}}{\mathrm{R} \mid\equiv \mathrm{U}}$
- Rule R_5 (Believe rule): $\dfrac{\mathrm{R} \mid\equiv \mathrm{S} \mid \equiv (\mathrm{U},\mathrm{V})}{\mathrm{R} \mid\equiv\ \mathrm{U},\ \mathrm{R} \mid \equiv \mathrm{V}}$
- Rule R_6 (Nonce verification rule): $\dfrac{\mathrm{R} \mid\equiv\ \#(\mathrm{U}),\ \mathrm{R} \mid \equiv (\mathrm{S} \mid\ \mathrm{U})}{\mathrm{R} \mid\equiv\ \mathrm{S} \mid \equiv \mathrm{U}}$
- Rule R_7 (Seeing rule): $\dfrac{\mathrm{R} \mid\equiv \overset{SK1}{\rightarrow}\ \mathrm{R},\quad \mathrm{R}\{\mathrm{U}\}_{SK1}}{\mathrm{R}\ \mathrm{U}}$

Goals: The authentication session needs to satisfy these goals to validate that our scheme provides mutual authentication. Here, the variables Um, Gn, SNo represents principals.

- Goal G_1: $\mathrm{Gn} \mid \circ\ \mathrm{Um} \overset{SK1}{\leftrightarrow} \mathrm{Gn}$
- Goal G_2: $\mathrm{Gn} \mid \circ\ \mathrm{Um} \mid\quad \mathrm{Um} \overset{SK1}{\leftrightarrow} \mathrm{Gn}$
- Goal G_3: $\mathrm{SNo} \mid \circ \mathrm{Gn} \overset{SK1}{\leftrightarrow} \mathrm{SNo}$
- Goal G_4: $\mathrm{SNo} \mid \circ \mathrm{Gn} \mid \circ \mathrm{Gn} \overset{SK1}{\leftrightarrow} \mathrm{SNo}$
- Goal G_5: $\mathrm{Gn} \mid \circ \mathrm{SNo} \overset{SK1}{\leftrightarrow} \mathrm{Gn}$

- Goal G_6: $\mathrm{Gn} \mid \circ \mathrm{SNo} \mid \mathrm{SNo} \overset{SK1}{\leftrightarrow} \mathrm{Gn}$
- Goal G_7: $\mathrm{Um} \mid \ \mathrm{Gn} \overset{SK1}{\leftrightarrow} \mathrm{Um}$
- Goal G_8: $\mathrm{Um} \mid \ \mathrm{Gn} \mid \circ \ \mathrm{Gn} \overset{SK1}{\leftrightarrow} \mathrm{Um}$

Assumption: The following assumptions are made to analyse the proposed authentication scheme:

Assumption A_1: $\mathrm{Um} \mid \ \#\left(\mathrm{Xu}, \mathrm{Xs}, \mathrm{Xo}\right)$

Assumption A _2: $\mathrm{Gn} \mid \ \#\left(\mathrm{Xu}, \mathrm{Xs}, \mathrm{Xo}\right)$

Assumption A _3: $\mathrm{SNo} \mid \ \#\left(\mathrm{Xu}, \mathrm{Xs}, \mathrm{Xo}\right)$

Assumption A _4: $\mathrm{Um} \mid \ \mathrm{Um} \overset{SNi}{\leftrightarrow} \mathrm{Gn}$

Assumption A _5: $\mathrm{Gn} \mid \ \mathrm{Gn} \overset{K}{\leftrightarrow} \mathrm{SNo}$

Assumption A _6: $\mathrm{SNo} \mid \ \mathrm{SNo} \overset{K}{\leftrightarrow} \mathrm{Gn}$

Assumption A _7: $\mathrm{Gn} \mid \ \mathrm{Gn} \overset{SNi}{\leftrightarrow} \mathrm{Um}$

Assumption A _8: $Gn \mid \circ \mathrm{Um}\ \mathrm{Xu}$

Assumption A _9: $\mathrm{SNo} \mid \ \mathrm{Gn}\ \mathrm{Xs}$

Assumption A _10: $Gn \mid \circ \mathrm{SNo}\ \mathrm{Xo}$

Assumption A _11: $\mathrm{Um} \mid \ \mathrm{Gn}\ \mathrm{Xs}$

The analysis of scheme is done usimg BAN logic rules and assumptions.

Msg_1: $\mathrm{UmGn} : <\ IDn, IDo, TS1, B3, B4 >$

According to R_7

S_1: Gn $<<\ IDn, IDo, TS1, B3: < TS1, Xu, IDn >, B4: < Xu, P >_{B1}$

According to A_7, R_1, S_1

S_2: Gn $\mid \ \mathrm{Um} \mid\sim \left(IDn, IDo, TS1, Xu, P\right)$

According to A_1, R_2, S_2

S_3: Gn$\mid \ \mathrm{Um} \mid \ \left(IDn, IDo, TS1, Xu, P\right)$

According to A_8, R_4, R_5, R_6, S_3

S_4: Gn$\mid \ \mathrm{Xu}$

According to A_2, R_3, S_4

S_5: Gn $\mid \ \mathrm{Um} \overset{SK1}{\leftrightarrow} \mathrm{Gn}$ (G_1)

According to A_2, R_6, S_5

S_6: Gn | Um| $\overset{SK1}{\text{Um} \leftrightarrow \text{Gn}}$ (G_2)
Msg_2: Gn SNo :< $\left\langle \text{C4}, C5, C6, IDo, \text{TS2} \right\rangle$

According to Rule_7

S_7:

$<< IDo, \text{TS2}, \ \text{C4} :< \text{IDo}, \text{So}, \text{Xs}, \text{TS2} >_{C1} , C5 :< Sn, TS2, Xs, P >_{B1}, C6 :< Xu, TS2, P, IDm, Sn >_{B1,C5,}$ >>

According to A_6, R_7, S_1

S_8: $\text{SNo}\left| \ \text{Gn} \right| \sim \left(IDo, \text{TS2}, \text{So}, \text{Xs}, Sn, IDm \right)$

According to A_2, R_1, S_8

S_9: $\text{SNo}\left| \ \text{Gn} \right| \sim \left(IDo, \text{TS2}, \text{So}, \text{Xs}, Sn, IDm \right)$

According to A_2, R_8, S_1, S_4

S_10: $\text{SNo} \mid \ \left(IDo, \text{TS2}, \text{So}, \text{Xs}, Sn, IDm \right)$

According to R_5, S_10

S_11: $\text{SNo} \mid \ Xs, \text{SNo} \mid \ \text{Xo}$

According to A_3, R_3, S_11

S_12: $\text{SNo} \mid \ \overset{SK1}{\text{Gn} \leftrightarrow \text{SNo}}$ (G_3)

According to A_3, R_6, S_12

S_13: $\text{SNo}\left| \ \text{Gn} \right| \ \overset{SK1}{\text{Gn} \leftrightarrow \text{SNo}}$ (G_4)
Msg_3: SNo Gn : <D1, TS3>

According to R_7

S_14: Gn $\left\langle \left\langle D1 : \left(\text{TS3}, \text{RSk}, \text{So}, \text{IDo}, \ \text{S\_K} \right), \ \text{TS3} \right\rangle \right\rangle$

According to A_5, R_1, S_14

S_15: Gn$\left|\ \mathrm{SNo}\right| \sim \left(\mathrm{TS3}, \mathrm{RSk}, \mathrm{So}, \mathrm{IDo}, \ \mathrm{S_K}\right)$

According to A_2, R_2, R_4, R_6, S_15

S_16: Gn$\left|\ \mathrm{SNo}\right|\ \left(\mathrm{TS3}, \mathrm{RSk}, \mathrm{So}, \mathrm{IDo}, \ \mathrm{S_K}\right)$

According to R_5, S_16

S_17: Gn$\left|\ \mathrm{Xo}\right.$

According to A_2, R_3, S_17

S_18: Gn$\left|\ \overset{\mathrm{SK1}}{\mathrm{SNo} \leftrightarrow Gn}\right.$ (G_5)

According to A_2, R_6, S_18

S_19: Gn$\left|\ \mathrm{SNo}\right|\ \overset{\mathrm{SK1}}{\mathrm{SNo} \leftrightarrow Gn}$ (G_6)
Msg_4: Gn $\mathrm{Um} : \left\langle\ \mathrm{C7}, \mathrm{TS4}\right\rangle$

According to R_7

S_20: $Um << C7 : (\mathrm{S\_K}, \mathrm{Xs}, \mathrm{TS4})_{C1}$, TS4 > >

According to A_4, R_1, S_20

S_21: $\mathrm{Um}\left|\ \mathrm{Gn}\right| \sim \left(\mathrm{S\_K}, \mathrm{Xs}, \mathrm{TS4}\right)$

According to A_1, R_6, S_21

S_22: $\mathrm{Um}\left|\ \mathrm{Gn}\right|\ \left(\mathrm{S\_K}, \mathrm{Xs}, \mathrm{TS4}\right)$

According to A_11, R_4, R_5, S_22

S_23: $\mathrm{Um}\ |\ \mathrm{Xs}$

According to A_1, R_3, S_23

S_24: $\mathrm{Gn}\ |\ \overset{\mathrm{SK1}}{\mathrm{Gn} \leftrightarrow Um}$ (G_7)

According to A_1, R_6, S_24

S_25: $\mathrm{Gn}\left|\ \mathrm{Gn}\right|\ \overset{\mathrm{SK1}}{\mathrm{Gn} \leftrightarrow Um}$ (G_8)

Finally, we achieved all the goals. Therefore, we can say that the proposed scheme has achieved mutual authentication.

6.4 Other Informal Security Attacks

6.4.1. User Anonymity

The identity of user is included in the message $B1 = h(IDm||Xu)$ and $C4 = \left(h\left(IDm \| PWm \| BRm\right)\ Xu\right)$. It is challenging for any attacker to get every value mentioned above in polynomial time. And the original identity IDm is not known to the GWN. Finally, we can say our scheme achieves this property.

6.4.2. Provides Mutual Authentication

From BAN logic rules, assumptions and goals, we can see that our proposed scheme achieves mutual authentication among the user, GWN and sensor node. This property also ensures that this scheme is safe against replay and MITM attack.

6.4.3. Session Key Agreement and Its Security

The authentication schemes are designed to provide secure communication among the communication parties. As mentioned above, our scheme achieves mutual authentication and we can also see that common session key is also generated among user, GWN and sensor node. In this scheme session key is calculated as S_K=h(Sn||Xs||C3||Xu||Xo||So). For an attacker, to get all these values is impossible. Hence it is tough for an adversary to generate session key. And we can also say if an adversary knows any session-specific temporary information or secret key, then also the adversary cannot derive session key due to the difficulty to solve ECDLP. Thus, secure session key agreement property is achieved.

6.4.4 User Impersonation Attack

The attacker can eavesdrop messages over a public channel to impersonate as a user. But we can see our scheme provides security against this attack. If the attacker gets the message containing IDn, IDo, *TS1, B3, B4,* where $B3 = h\left(TS1 \| Xu \| IDn\right)$, *B4 = h(C3||TS1|| Xu || Qu)* and $B5 = E_{B4.x}\left\{IDm \| Qu \| TS1\right\}$. To impersonate as a user, it needs to frame new message containing the above-mentioned values. But it is impossible for an intruder to get all these values in polynomial time. Therefore, an attacker cannot generate another message in polynomial time. Hence, we can say that our scheme is safe against this attack.

6.4.5. Gateway Node Impersonation Attack

There are two messages through which legitimacy of GWN can be compromised, the first message sends to sensor node. If attacker intercepts this message $\left\langle C4, C5, C6, C7, IDo, TS2\right\rangle$ here

$C4 = h\left(IDo \| C1 \| So \| Xs \| TS2\right)$,

$C5 = h\left(Sn \| Xs \| C3 \| TS2 \| Qs\right)$,

$C6 = h\left(C5 \| C3 \| TS2 \| Xu \| IDm \| Qs\right)$ and $C7 = h\left(Xu \| Xs \| TS2\right)So$. For this attack to be successful adversary needs to impersonate as a GWN and send another message containing the values present in C4, C5, C6,C7. But we can easily say that attacker cannot get the secret value nor random numbers due to the secrecy of one-way hash function. Hence our scheme is safe against this attack.

6.4.6. Sensor Node Impersonation Attack

If the attacker is able to compromise D1 during the execution of our scheme then this attack is possible. That is an adversary must know all the values present in $D1 = h\left(TS3 \| Xo \| So \| IDo \| S\_K\right)$. But it is not easy for an attacker cannot get all these values at the same time. Therefore, this scheme is safe against this attack.

6.4.7. Replay Attack

In this, attacker usuallysend the prior executed message to the desired receiver assuming that it is sent from the authorised sender. But in our scheme, we have used timestamp and for every message first the transmission delay that is $\triangle$T is checked. And the message is rejected by the receiver if the delay is invalid. And we have also used BAN logic rules and assumptions to prove that our scheme is safe against this attack.

6.4.8. Privileged Insider Attack

We assume that Gn does not have user's confidential information like a password. It is known found that maximum problems are because of insider attack. In our scheme, the user first masks its confidential information, and then sends it to the gateway node during registration phase. So, it is tough for an insider to extract the password because it is secured by one-way hash function. Therefore, our scheme is safe against this attack.

6.4.9. Security of Secret Keys

This scheme uses various secret keys like Src, Sn, So. During this phase, Src is used to calculate $Sn(Sn = h(IDn \,||\, Src))$ and $So(So = h(IDo \,||\, Src))$. As we can see Src is protected by hash function, the adversary cannot get that secret key. Hence attacker cannot retrieve the value of Sn. Hence, the secret key is secure in our scheme.

6.4.10 Smart Card Loss Attack

In case of this attack, an adversary can easily guess identity and password. But in the proposed scheme adversary will not be able to guess credentials of user because of the following facts: If an attacker gets all the sored information of smart card < IDo ,B3, B4, B5, IDn, TS1>. Attacker will not be able to calculate the values of $B3 = h\left(TS1 \| Xu \| IDn\right)$, $B4 = h\,(C3 \| TS1 \| Xu \,||\, Qu\,)$, $B5 = E_{B4.x}\left\{IDm \| Qu \| TS1\right\}$. In this, method it is difficult to guess these values without knowledge of identity and password. These identity and password are protected by hash function. And due to non-invertibility of hash it is not possible to get user credentials. Hence, we can say our scheme is safe against this attack.

6.4.11. Perfect Forward Secrecy

The session key depends on random nonce and the adversary cannot calculate its value. If the session key is attacked by an adversary, then it tries to calculate previous session key. But the adversary cannot get compute the confidential information present in the session key. So, he/she cannot compute previous session key. Therefore, our scheme preserves this perfect forward secrecy.

6.4.12. Efficient Password Change

If the password is attacked by an adversary or if he/she wants to modify his/her password, then this phase is executed. To change the password of user, neither there is a role of gateway node nor registration centre. It can be done independently by the user, hence load on the network is reduced

and it can resist denial of service attack. To change password, the user first enters its original identity and password. Hence authenticity of a user is also verified, that as a result reduces computational cost. As a result, we can say password change phase of this scheme is efficient.

6.4.13. Efficient Login

For login, the user provides information like identity and password. If these values are not correct, smart card reader detects this and terminates the connection. So, extra communication and computation is not required. Therefore, our proposed scheme provides an efficient login phase.

6.4.14. Efficient Authentication

As we know that sensor node has small battery and it is very difficult to recharge or replace its battery. To increase life of the sensor network, it is necessary to reduce computation cost performed by the sensor node. This cost can be either in the form of computations performed or the number of bits transmitted by sensor node. In this scheme, as sensor node first authenticates user and gateway node it reduces the unnecessary load of dealing with fake messages by an adversary. Hence, this scheme provides efficient authentication.

6.4.15 Offline Guessing Attack

Even if attacker gets all the messages message 1, message 2, message 3, message 4 an attacker will not be able to guess correct identity and password. Hence our scheme can resist this attack.

7. SIMULATION USING AVISPA TOOL

We apply widely accepted AVISPA tool for formal security verification of our proposed scheme and analyse its security features. This tool verifies whether an authentication scheme is safe against replay and MITM attack (Armando, Basin, Boichut, Chevalier, Compagna, Cuéllar, & Mödersheim, 2005). This tool is massively used during the design of authentication protocols because it can be used to verify whether the protocol is secure against active and passive adversaries. In this tool, a High-level protocol specification language (HLPSL) is used (Oheimb, 2005). The simulation is done using AVISPA for (i) OFMC (ii) CL-AtSe back-ends and the result is shown in figure 2 and figure 3 respectively. The intruder has been provided with all messages and can interact with other roles. Its main goal is to disclose secret keys, compromise the authenticity of different roles. The OFMC and CL-AtSe back-ends verify the attack (if any) can be found while implementing this scheme. If the scheme is safe, it will report SAFE else it will show which security attack is present in the scheme. We can see clearly in the summary of these two back-ends that our scheme is safe against attacks.

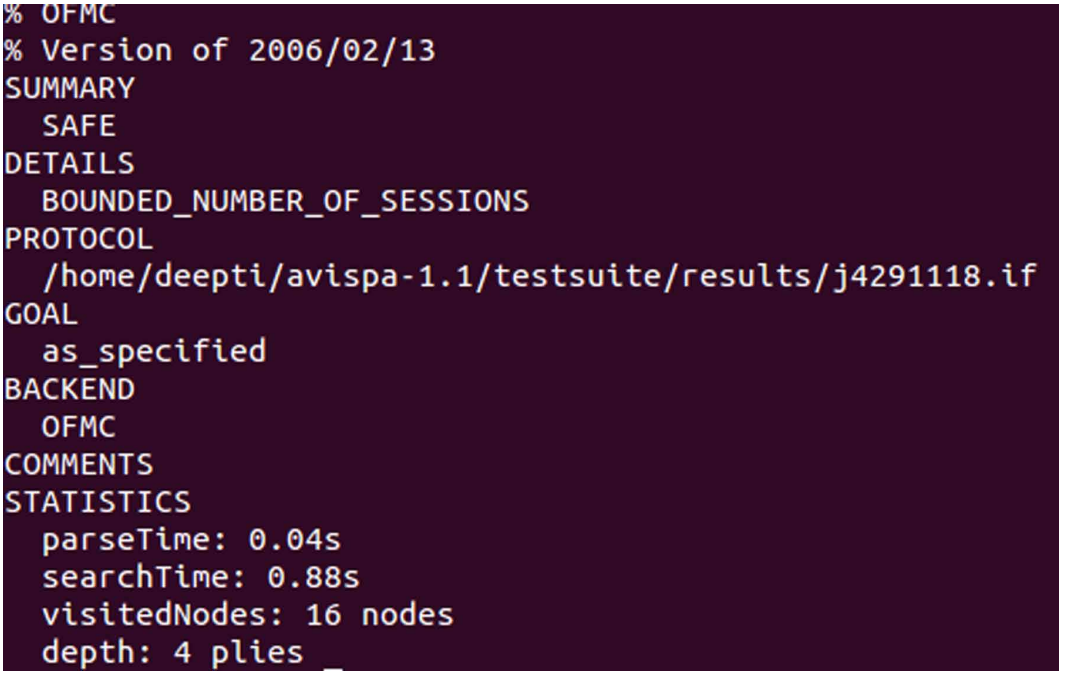
8. PERFORMANCE EVALUATION

In this section, we evaluate the security of our scheme with other schemes based on security features. Then the comparison is performed on the basis of communication and computation costs.

8.1. Comparison of Security Features

In Table 3, we have presented the security and functionality features of our scheme and other related schemes. Table 4 shows that the scheme (Li, Niu, Bhuiyan, Wu, Karuppiah, & Kumari, 2018),(Jiang, Ma, Wei, Tian, Shen & Yang, 2016)] are not safe against known session-specific temporary information attack and does not provide forward secrecy. Li et al. (Li, Niu, Bhuiyan, Wu, Karuppiah & Kumari, 2018) is not resistant to smart card loss attack. Jiang et al.(Jiang, Ma, Wei, Tian, Shen & Yang, 2016) also lacks the feature of untraceability and is not resistant to offline guessing attack. It also can't identify an unauthorized login. Park et al. (Park, Lee, Kim, & Park, 2016) cannot provide user

Figure 2. OFMC backend result for authentication and key agreement phase



anonymity and is not resilient to user impersonation attack. From this, we can easily analyse that none of the mentioned schemes are free from security attacks. But the proposed scheme is resistant to many attacks and provides additional security features compared to others.This scheme is also simulated formally with AVISPA tool that shows that it is safe against replay and MITM attack.

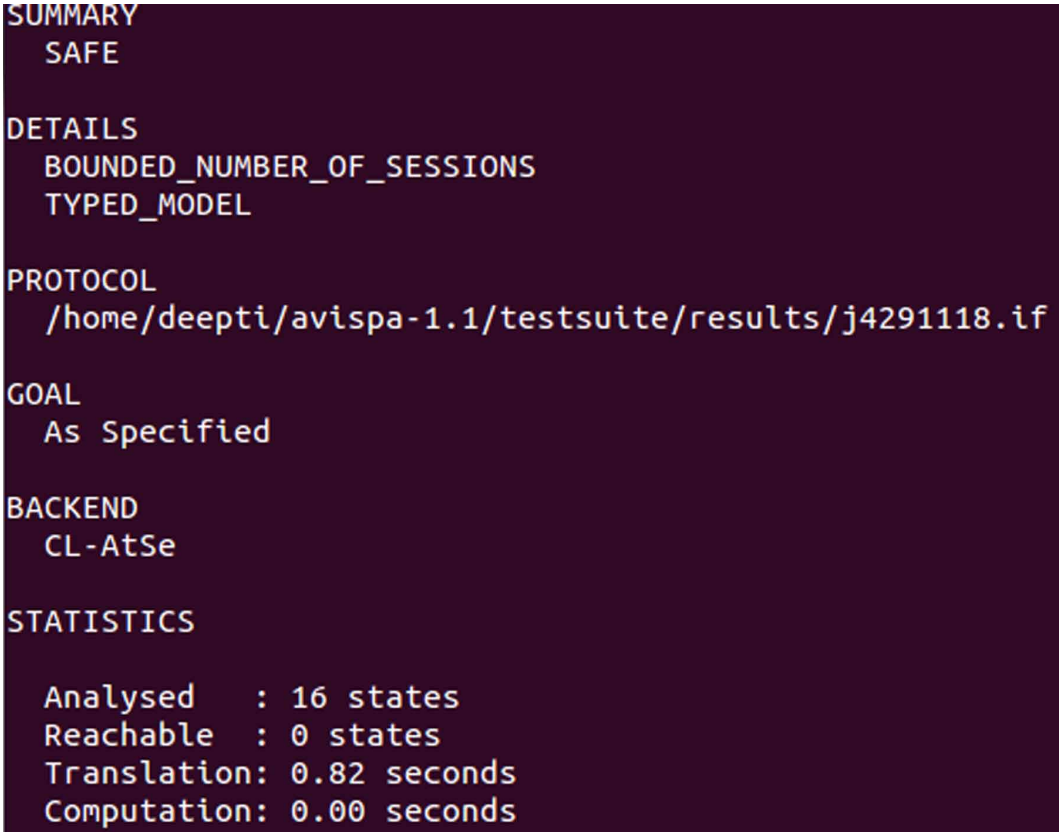
8.2. Comparison of Computational Cost

Table 5 facilitate the comparison of computational cost among different related scheme along with our scheme. $T_{ec/ed}$,T_{ecc} and T_h denotes time of encryption and decryption, ECC multiplication and hash operation respectively. T_{ecc} is larger than $T_{ec/ed}$ and T_h and according to paper (Xu & Wu, 2015) (Wu, Xu, Kumari, Li, Das, Khan, & Baliyan, 2016) value of $T_{ec/ed}$,T_{ecc} and T_h are 0.1303 ms, 0.4275ms and 0.0004ms. The computation time of login and authentication is more important due to resource constraint nature of sensors'. From the table we can see scheme Li et al. (Li, Niu, Bhuiyan, Wu, Karuppiah & Kumari, 2018) and Jiang et al. (Jiang, Ma, Wei, Tian, Shen & Yang, 2016) have approximately equal computation cost. And Park et al. has much higher computation overhead as compared to others. The proposed scheme is efficient as compared to other discussed schemes (Li, Niu, Bhuiyan, Wu, Karuppiah, & Kumari, 2018),(Jiang, Ma, Wei, Tian, Shen & Yang, 2016),28]. In our scheme, sensor node does not perform ECC multiplication operation. Our scheme is most efficient as compared to other discussed schemes.

8.3. Comparison of Communication Cost

Table 6 facilitate the comparison of communication cost among different related schemes along with our scheme. For simplicity of calculation, we have assumed the length of ECC point multiplication is 160 bits and for random number, timestamp, hash function, secret key, identity and password the length is 128 bits. From the table, we can see scheme Li et al. (Li, Niu, Bhuiyan, Wu, Karuppiah & Kumari, 2018) and Jiang et al. (Jiang, Ma, Wei, Tian, Shen & Yang, 2016) have higher communication

Figure 3. CL-AtSe backend result for authentication and key agreement phase



cost and they are efficient as compared to Park et al. (Park, Lee, Kim, & Park, 2016). The proposed scheme provides better communication efficacy compared to the other three schemes. Finally, from Table 4, 5 and 6 it can be concluded that this scheme provides better functionality features, less communication and computation costs compared to other schemes. It is also resistant to most of the security attacks. Hence, it is more suitable for designing any secure authentication scheme as compared to other schemes.

9. CONCLUSION

In this paper, cryptanalysis of Li et al. scheme is done and found some vulnerability. Then, a new scheme is designed to solve the security pitfall of Li et al. scheme. The proposed scheme is an ECC based revocable privacy-preserving scheme to authenticate the legitimate user and sensor node in WMSNs. It is also noted from the literature review that various schemes could not provide the necessary security features. One of the main requirements is to verify the authenticity of the user (or patient) and sensors present on patient's body to prevent them from security attacks. The mutual authentication and session key are generated in this scheme. This scheme also achieves various security features with low cost, which as a result save lifetime of deployed sensors in the patient's body. The proposed scheme helps to protect the online data from unauthorized entities in healthcare wireless medical sensor network. The security analysis validates that it is applicable in various applications. We also evaluated the performance of our scheme with other existing ECC based schemes. The evaluation results show that proposed scheme has less communication and computation overhead and hence can be successfully used for healthcare applications.

Table 3. Symbols used for security features

Mutual authentication	SF1
Resilience to impersonation attack	SF2
Key agreement between user and sensors'	SF3
Resist known session specific temporary information attack	SF4
User Anonymity	SF5
Resist Offline guessing attack	SF6
Resistant to Smart card loss attack	SF7
Resistant to forward secrecy	SF8
Untraceability	SF9
Freely Password change	SF10
Can detect unauthorized login	SF11

Table 4. Comparison of security feature of authentication schemes

Features	Proposed Scheme	Park et al.[28]	Jiang et al.[26]	Li et al.[24]
SF1	Yes	Yes	Yes	Yes
SF2	Yes	No	Yes	Yes
SF3	Yes	Yes	Yes	Yes
SF4	Yes	Yes	No	No
SF5	Yes	No	Yes	Yes
SF6	Yes	Yes	No	No
SF7	Yes	Yes	Yes	No
SF8	Yes	Yes	No	No
SF9	Yes	Yes	Yes	Yes
SF10	Yes	Yes	No	Yes
SF11	Yes	Yes	No	Yes

Table 5. Comparison of Computation cost of authentication schemes

	User	Base Station	Sensor node	Total Complexity	Total Running time
Park et al.[28]	$6T_{h+}2T_{ecc}$	$7T_{h+}2T_{ec}$	$4T_{h+}2T_{ecc}+T_{ed}$	$17T_{h+}4T_{ecc}+3T_{ec/ed}$	2.1077
Jiang et al.[26]	$8T_{h+}2T_{ecc}$	$9T_{h+}T_{ecc}$	$6T_h$	$19T_{h+}3T_{ecc}$	1.2901
Li et al.[24]	$8T_{h+}2T_{ecc}$	$9T_{h+}T_{ecc}$	$4T_h$	$21T_{h+}3T_{ecc}$	1.2909
Our scheme	$8T_h+T_{ecc}+T_{ec}$	$12T_h+T_{ecc}+T_{ed}$	$7T_h$	$27T_h+2T_{ecc}+2T_{ec/ed}$	0.9961

Table 6. Comparison of Communication cost of authentication schemes

	User	Base Station /Gateway node	Sensor node	Total cost(in bits)
Park et al.[28]	4*128+2*160	4*128	1*128+3*160	1952
Jiang et al.[26]	2*160+3*128	5*128	4*128	1856
Li et al.[24]	2*160+3*128	7*128	2*128	1856
Our scheme	5*128	7*128	2*128	1792

REFERENCES

Amin, R., Islam, S. H., Biswas, G. P., Khan, M. K., Leng, L., & Kumar, N. (2016). Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks*, *101*, 42–62. doi:10.1016/j.comnet.2016.01.006

Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuéllar, J., & Mödersheim, S. (2005, July). The AVISPA tool for the automated validation of internet security protocols and applications. In *International conference on computer aided verification* (pp. 281-285). Springer. doi:10.1007/11513988_27

Burrows, M., & Needham Abadi, R. (1990). A logic of authentication. *ACM Transactions on Computer Systems*, *8*(1), 18–36. doi:10.1145/77648.77649

Choi, Y., Lee, D., Kim, J., Jung, J., Nam, J., & Won, D. (2014). Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors (Basel)*, *14*(6), 10081–10106. doi:10.3390/s140610081 PMID:24919012

Das, A. K. (2016). A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *9*(1), 223–244. doi:10.1007/s12083-014-0324-9

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

Fakhrey, H., Tiwari, R., Johnston, M., & Al-Mathehaji, Y. A. (2016). The optimum design of location-dependent key management protocol for a WSN with a random selected cell reporter. *IEEE Sensors Journal*, *16*(19), 7217–7226. doi:10.1109/JSEN.2016.2594591

Gope, P., & Hwang, T. (2016). A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. *IEEE Transactions on Industrial Electronics*, *63*(11), 7124–7132. doi:10.1109/TIE.2016.2585081

He, D., Gao, Y., Chan, S., Chen, C., & Bu, J. (2010). An Enhanced Two-factor User Authentication Scheme in Wireless Sensor Networks. *Ad-Hoc & Sensor Wireless Networks*, *10*(4), 361–371.

Jiang, Q., Ma, J., Lu, X., & Tian, Y. (2015). An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *8*(6), 1070–1081. doi:10.1007/s12083-014-0285-z

Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J., & Yang, Y. (2016). An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. *Journal of Network and Computer Applications*, *76*, 37–48. doi:10.1016/j.jnca.2016.10.001

Kumar, P., & Lee, H. J. (2011, June). Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks. In Wireless Advanced (WiAd), 2011 (pp. 241-245). IEEE. doi:10.1109/WiAd.2011.5983262

Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M., & Kumari, S. (2018). A robust ECC-based provable secure authentication protocol with privacy preserving for industrial internet of things. *IEEE Transactions on Industrial Informatics*, *14*(8), 3599–3609. doi:10.1109/TII.2017.2773666

Luo, H., Wen, G., & Su, J. (2018). Lightweight three factor scheme for real-time data access in wireless sensor networks. *Wireless Networks*, 1–16.

Mahto, D., & Yadav, D. K. (2018). Performance Analysis of RSA and Elliptic Curve Cryptography. *International Journal of Network Security*, *20*(4), 625–635.

Park, Y., Lee, S., Kim, C., & Park, Y. (2016). Secure biometric-based authentication scheme with smart card revocation/reissue for wireless sensor networks. *International Journal of Distributed Sensor Networks*, *12*(7), 1550147716658607. doi:10.1177/1550147716658607

Ryu, J., Song, T., Moon, J., Kim, H., & Won, D. (2019). Cryptanalysis of Improved and Provably Secure Three-Factor User Authentication Scheme for Wireless Sensor Networks. In *Computational Science and Technology* (pp. 49–58). Springer. doi:10.1007/978-981-13-2622-6_5

Singh, D., Kumar, B., Singh, S., & Chand, S. (2019). SMAC-AS: MAC Based Secure Authentication Scheme for Wireless Sensor Network. *Wireless Personal Communications*, *107*(2), 1289–1308. Advance online publication. doi:10.1007/s11277-019-06336-8

Singh, D., Singh, S., Kumar, B., & Chand, S. (2018). An Efficient and Secure Authentication Scheme using Markov Chain for Wireless Sensor Networks. *IEEE 8th International Advance Computing Conference (IACC),* 33-38.

Singh, D., Singh, S., Kumar, B., & Chand, S. (2018). Anonymity Preserving Authentication and Key Agreement Scheme for Wireless Sensor Networks. In *International Conference on Futuristic Trends in Network and Communication Technologies* (pp. 484-495). Springer.

Singh, S., & Singh, P. K. (2018). Performance Investigation of Energy Efficient HetSEP for Prolonging Lifetime in WSNs. *International Conference on Futuristic Trends in Network and Communication Technologies*, 496-509.

Sutrala, A. K., Das, A. K., Kumar, N., Reddy, A. G., Vasilakos, A. V., & Rodrigues, J. J. (2018). On the design of secure user authenticated key management scheme for multigateway-based wireless sensor networks using ECC. *International Journal of Communication Systems*, *31*(8), e3514. doi:10.1002/dac.3514

Turkanović, M., Brumen, B., & Hölbl, M. (2014). A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks*, *20*, 96–112. doi:10.1016/j.adhoc.2014.03.009

Von Oheimb, D. (2005, September). The high-level protocol specification language HLPSL developed in the EU project AVISPA. In *Proceedings of APPSEM 2005 workshop* (pp. 1-17). Academic Press.

Wang, D., Li, W., & Wang, P. (2018). Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics*, *14*(9), 4081–4092. doi:10.1109/TII.2018.2834351

Watro, R., Kong, D., Cuti, S. F., Gardiner, C., Lynn, C., & Kruus, P. (2004, October). TinyPK: securing sensor networks with public key technology. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks* (pp. 59-64). ACM. doi:10.1145/1029102.1029113

Wong, K. H., Zheng, Y., Cao, J., & Wang, S. (2006, June). A dynamic user authentication scheme for wireless sensor networks. In *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on* (Vol. 1). IEEE. doi:10.1109/SUTC.2006.1636182

Wu, F., Xu, L., Kumari, S., & Li, X. (2017). A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security. *Journal of Ambient Intelligence and Humanized Computing*, *8*(1), 101–116. doi:10.1007/s12652-016-0345-8

Wu, F., Xu, L., Kumari, S., & Li, X. (2018). An improved and provably secure three-factor user authentication scheme for wireless sensor networks. *Peer-to-Peer Networking and Applications*, *11*(1), 1–20. doi:10.1007/s12083-016-0485-9

Wu, F., Xu, L., Kumari, S., Li, X., Das, A. K., Khan, M. K., & Baliyan, R. (2016). A novel and provably secure authentication and key agreement scheme with user anonymity for global mobility networks. *Security and Communication Networks*, *9*(16), 3527–3542. doi:10.1002/sec.1558

Xu, L., & Wu, F. (2015). Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health-care. *Journal of Medical Systems*, *39*(2), 1–9. doi:10.1007/s10916-014-0179-x PMID:25631840

Xue, K., Ma, C., Hong, P., & Ding, R. (2013). A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. *Journal of Network and Computer Applications*, *36*(1), 316–323. doi:10.1016/j.jnca.2012.05.010

Zhu, Z., & Huang, R. G. (2017, October). Study on the IOT Architecture and Access Technology. In *2017 16th International Symposium on Distributed Computing and Applications to Business, Engineering and Science (DCABES)* (pp. 113-116). IEEE.

Deepti Singh received her B.Tech. in Information Technology from Uttar Pradesh Technical University, Lucknow, India in 2009 and her M.Tech. in Computer Science & Engineering from Kamla Nehru Institute of Technology, Sultanpur, India, in 2013. She is pursuing her PhD in the Department of Computer Engineering, Netaji Subhas Institute of Technology, New Delhi, India. Her research interest includes wireless sensor networks.

Bijendra Kumar did his Bachelor of Engineering from H.B.T.I. Kanpur, India. He has done his Ph.D. in Delhi University, Delhi, India in 2011. Presently he is Professor in Computer Engineering Division at Netaji Subhas University of Technology (formerly, Netaji Subhas Institute of Technology), Delhi, India. His areas of research interests are Video applications, watermarking, and Design of algorithms, Wireless sensor networks, cloud computing and Topic Modeling.

Samayveer Singh received his B.Tech. in Information Technology from Uttar Pradesh Technical University, Lucknow, India in 2007, and his M.Tech. degree in Computer Science & Engineering from National Institute of Technology, Jalandhar, India, in 2010. He has done his PhD in Computer Engineering at Netaji Subhas Institute of Technology, New Delhi, (University of Delhi) India. Presently he is Assistant Professor in Computer engineering Division at NIT, Jalandhar India. His research interests are wireless sensor networks, Image processing.

Satish Chand did his M.Sc. in Mathematics from Indian Institute of Technology, Kanpur, India and M.Tech. in Computer Science from Indian Institute of Technology, Kharagpur, India and Ph.D. from Jawaharlal Nehru University, New Delhi, India. Presently he is Professor in School of computer and systems sciences at Jawaharlal Nehru University, New Delhi, India. Areas of his research interest are Multimedia Broadcasting, Networking, Video-on-Demand, Cryptography, and Image processing, Wireless sensor network.