A Secure Biometric-Based User Authentication Scheme for Cyber-Physical Systems in Healthcare

Khushboo Jha*, Aruna Jain and Sumit Srivastava

Department of Computer Science and Engineering, Birla Institute of Technology, Ranchi-835215, Jharkhand, India

E-mail/Orcid Id:
KJ, kjha.phd@gmail.com, https://orcid.org/0000-0003-1062-8128; AJ, arunajain@bitmesra.ac.in;
SS, sumit.srivs88@gmail.com, https://orcid.org/0009-0003-6880-2958

DOI: https://doi.org/10.52756/ijerr.2024.v39spl.012

Abstract: The effectiveness and advantages of Cyber-Physical Systems (CPS) are significantly influenced by the interconnectivity of individual devices or nodes, such as Internet of Things (IoT) devices. The exchange of data that is pertinent to a comprehensive job or capability plays a crucial role in numerous CPS applications, including healthcare monitoring in smart cities and homes and many more. Data exploitation in remote healthcare systems may have catastrophic consequences for patients; hence, a safe cryptographic technique is necessary. To address these security difficulties, a highly effective biometric based three-factor mutual authentication along with a key agreement scheme has been put forth that leverages the lightweight Elliptic Curve Cryptosystem (ECC). This scheme has been specifically designed to cater to the unique requirements of remote healthcare systems. The approach has been validated utilizing the Burrows-Abadi-Needham (BAN) logic, which verifies the effectiveness of mutual authentication. Also, the resistance to active and passive attacks was demonstrated through the use of the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. Furthermore, a preliminary security evaluation is conducted to verify the resilience of the proposed system against several cryptographic attacks. Additionally, the suggested method is evaluated against existing state-of-the-art schemes and demonstrates superior performance in various security dimensions.

Introduction

In the present times, when people manage their routine work single-handedly in a nuclear family, there is a big challenge for elderly people when they are left alone in their twilight years. They face social exclusion, loneliness, isolation and even negligence, which in turn have negative impacts on their emotional and physical wellbeing. These elderly and medically challenged people are left by their families and friends for some reason and live alone for the majority of their time. Therefore, experts are working to provide services remotely, particularly for elderly people (Pal et al., 2018). To overcome aforesaid challenges, a based IoT environment for remote healthcare monitoring (Mondal et al., 2023; Jain et al., 2023) using wireless sensor networks (WSNs) (Alghamdi et al., 2023) is one of the eminent solutions for helping older people independently manage good health and safely age in place. It is regarded as a novel paradigm within the realm of the Internet of Things (IoT), facilitated by the proliferation of Machine-to-Machine communication, Wireless Sensor Networks, ubiquitous computing technology, Radio Frequency Identification (RFID), network communication infrastructure and evolving control methodologies (Rai et al., 2023; Dawn et al., 2023).

Moreover, CPS-based applications such as smart cities (Jha and Singh, 2024), smart homes for remote healthcare systems, etc. have the potential to leverage the proliferation of smart devices and wireless networks, enabling them to provide intelligent services which are driven by data from the physical environment. Further, IoT sensor device-based home care is becoming an integral part of the healthcare monitoring system (Mondal et al., 2023). Aiming to prevent elder and disabled people from being confined to institutions unnecessarily, this policy encourages people to age in
place. The environment integrates medical sensors, modern communication, actuators, and information technology, thereby enabling continuous and remote monitoring to forecast the behaviour of the elderly based on wireless sensor data. In such IoT-based environments, WSNs (Soni et al., 2019a; Soni et al., 2019b) are considered the most significant component as they collect the real-time data sensed by the sensor. The gateway node sends these data in the form of regular health reports to family members and healthcare professionals. These reports, enable complete monitoring and surveillance of the health condition of elderly people in real-time and provide remote feedback and support.

There are some existing IoT sensor device-based services, such as fall detection, outdoor positioning, obstacle recognition, fitness tracker, medicine reminder, smart audio communication devices, smart television, emergency support, abnormal behaviour detection, sleep monitoring, smart mobility platforms (like walker, wheelchair) and so on. Such IoT-based applications involve networking on every device and exchanging data via public channels. During the study of several IoT-based authentication schemes, one or the other schemes had pitfalls like sensor node capture attacks (Ahlawat and Bathla, 2023; Jha et al., 2024b), session key leak attacks, sensor node impersonation attacks, user impersonation attacks and gateway node impersonation attack, smart card loss attack and violation of forward secrecy. Also, the latest developments and applications of remote healthcare systems rely on the efficacy of cryptographic techniques to boost security standards (Chetry et al., 2023). These results necessitated the introduction of an efficient biometric-based authentication (Jha et al., 2023a; Jha et al., 2023b; Jha et al., 2024a) scheme using lightweight ECC cryptosystem and fuzzy extractor to protect the biometric template for secure communication between the involved parties in remote health care system.

The structure of this document is as follows: Section 2 demonstrates related works. Section 3 describes the proposed scheme. Section 4 describes the authentication proof using BAN logic, while Section 5 offers an informal security analysis. The suggested method is subjected to simulation verification using the AVISPA tool in Section 6, while the result and discussion is presented in Section 7. Section 8 addresses the conclusion.

Related works

CPSs (Hemalatha et al., 2023) based remote healthcare systems are an instance of an IoT-based application in gerontechnology, which plays a significant role in transforming the healthcare system for the elders. Nevertheless, network security threats increase with internet evolution (Chetry et al., 2023). Moreover, the transfer of data from the sensor node is susceptible to many security threats, including network infiltration, data tampering, and sensor node capture attacks (Ahlawat and Bathla, 2023). As a result, numerous authentication techniques have been proposed to safeguard the confidentiality of medical data and personal information about the involved parties. In 2019, Liu et al. (Liu et al., 2019) introduced an ID-MAKA approach that primarily accomplishes biometrics-oriented remote authentication, single login, and centerless functionality for mobile cloud computing services. However, the anonymity of users is not ensured (Cho et al., 2022).

In 2020, Vinoth et al. (2020) suggested a key agreement mechanism for the Industrial Internet of Things (IIoT) that incorporates secure multi-factor authentication. Vinoth’s solution has a lightweight characteristic and employs access structure and secret sharing techniques to establish the session key between users and sensors. Far et al. (2021) carried the cryptanalysis on Vinoth et al.’s approach and inferred that the system is susceptible to various forms of attacks, including the denial-of-service (DoS) attack, replay attack, sensor node capture attack, during the fourth stage of their protocol, and desynchronization attack. Also, it offers a direct link between the sensor node and the user, even in the presence of the gateway node. The utilisation of long-distance communication in the context of IIoT, particularly in expansive areas, results in significant power consumption within the sensor node. Consequently, their proposed scheme is deemed unsuitable for implementation in IIoT. Therefore, Far et al. (2021) enhanced and developed a lightweight anonymous privacy-preserving three-factor authentication technique for WSN-based IIoT referred to as LAPTAS. Within the LAPTAS system, individuals who have completed the registration process are granted the ability to utilize their secure smart card as a means of establishing communication with various sensors and obtaining access to the corresponding data. Unfortunately, Nyangaresi et al. (2022) performed a cryptanalysis of Far et al. and claimed that their approach is prone to user anonymity, backward and forward key secrecy, secret key and temporary information leakage. Thereby unsuitable for the IoT environment.

In 2021, Wu et al. (2021) proposed a lightweight ECC-based three-factor multiserver authentication scheme to improve the efficiency of mobile network
services. Similarly, in 2022, Saqib et al. (2022) suggested a three-factor authentication system for IoT-driven critical applications using identity, password, and digital signatures. The framework uses a publish-subscribe structure with lower hash chains and elliptical curve cryptography (ECC). Mutual authentication of gateway nodes with remote user and sensor nodes and dynamic session key generation are major features of the proposed system. However, in 2022, Mirsaraei et al. (2022) found that the approach of Saqib et al. (2022) lacks the crucial characteristic of user access level determination, which is crucial for authentication procedures. Additionally, Mirsaraei et al. (2022) exposed that the approach of Wu et al. (2021) fails to provide data integrity, data confidentiality, authorization and secured password updation. Also, it is prone to Denial-of-service (DoS) and brute force attacks. Based on the approaches, it can be inferred that all previous schemes exhibit certain security flaws, rendering them vulnerable. This inspired us to formulate a secure three-factor user authentication approach based on an elliptic curve cryptosystem utilizing IoT sensor nodes through WSNs for healthcare monitoring (Lekha et al., 2023). The proposed scheme demonstrates greater suitability for implementation in the remote healthcare system when compared with previous contemporary schemes.

Proposed scheme

We have devised a highly effective and reliable authentication scheme for remote healthcare monitoring in an IoT environment, especially for older people. The proposed scheme leverages ECC (Sarkar et al., 2019), a public key cryptosystem that generates keys using elliptic curves. It is more secure and implies a smaller key size than other cryptosystems (Soni et al., 2019a). Furthermore, the integration of a fuzzy extractor in the authentication system has enhanced the security of the user's biometric parameter. The proposed scheme consists of six phases, i.e., system initialization, registering sensor nodes, registering users, logging in, authenticating users, and changing passwords. In our scheme, three parties are involved, namely the user (elderly, caregivers, medical representatives and family members) $U_i$, gateway node denoted as $GWN$ and the IoT sensor nodes $SN_j$. In our scheme, a user will retrieve data from the sensor node via the gateway node. First of all, to form the environments of WSNs, the user and the sensor nodes have to register on $GWN$. To access healthcare records, the user will send a login request to $GWN$. Then $GWN$ will authenticate the user as a legitimate one, then it will forward the authentication message to the sensor node. Now, the sensor node will verify the authenticity of $GWN$ and send the response back to $GWN$. Likewise, $GWN$ will send a message to a user to verify the authenticity of $GWN$. Finally, mutual authentication communication will be established among all involved parties, sharing a common session key. In support of the GWN, a sensor node employs encryption using the session key to secure the patient's data before transmitting it to the user. Now, a doctor or family member as a user can monitor an elder person in a care centre or home and collect health data from the GWN stored in the private blockchain (Mirsaraei et al., 2022). Figure 1 represents the basic architecture of our proposed scheme.

Figure 1. Proposed WSN-based model for the healthcare system.
System initialization phase

At first, gateway node GWN determines the system attributes necessary to implement the proposed scheme. Therefore, it selects G as an additive group over the finite field \( F_p \), on an elliptic curve where point \( P \) is the generator of order large prime \( n \). Then it produces a nonce \( x \in Z_n^* \) as a private key and computes respective \( X = xP \) as a public key. A master secret key \( K_{GWN} \) of 1024 bits is chosen, which is kept secretly along with \( x \).

At the last GWN broadcast the parameters \( \{E(F_p), G, P, X\} \).

Sensor node registration phase

The integrity of the system's service relies on the legitimacy of all its constituent parts. Consequently, all sensor nodes in the system ought to be registered to GWN. The GWN selects an identity \( SID_j \) for the concerned sensor node. It then evaluates a secret key, \( K_{GWN-S} = h(SID_j \parallel K_{GWN}) \) and stores these values i.e., \( \{SID_j, K_{GWN-S}\} \) in sensor node \( N_j \)'s memory and deploys in the concerned area.

<table>
<thead>
<tr>
<th>Table 1. User registration phase.</th>
</tr>
</thead>
<tbody>
<tr>
<td>( U_i ) selects ( ID_i, PW_i )</td>
</tr>
<tr>
<td>produce a nonce ( a_i )</td>
</tr>
<tr>
<td>calculates ( RPW_i = h(a_i \parallel PW_i) )</td>
</tr>
<tr>
<td>stamps the biometric ( b_i ) on a specific gadget and</td>
</tr>
<tr>
<td>gets ( F_i ) as ( H(b_i) )</td>
</tr>
<tr>
<td>Stores ( a_i ) as ( V_i = a_i \oplus F_i )</td>
</tr>
<tr>
<td>( SC_i ) contains {A_i, B_i, h(\cdot), H(\cdot), X, P, V_i}</td>
</tr>
</tbody>
</table>

User registration phase

The user, who may be a member of the family or a medical professional, desires to access the service provided by the system. He/she must register themselves with GWN. Therefore, user registration involves the following procedures shown in Table 1.

Login phase

During this stage, a reliable system verifies the authenticity of a user by conducting a verification process that requires the submission of necessary credentials. The user executes the subsequent procedures to achieve successful completion of the login phase.

Step 1: \( U_i \) loads the \( SC_i \) into a card reader, provides \( ID_i, PW_i \), provides biometric \( b_i' \) on a specific gadget and receives \( F_i' = H(b_i') \). Then, \( SC_i \) evaluates \( a_i' = V_i = a_i \oplus F_i \oplus F_i' = a_i \oplus F_i \oplus F_i' = h(a_i' \parallel PW_i) \), \( h(RPW_i' \parallel ID_i \parallel F_i') \) and check \( A_i' = A_i \), if unequal then the session is terminated by the \( SC_i \) else user's identity, password and biometric altogether are verified.

Step 2: Now, \( SC_i \) computes \( C_i = B_i \oplus h(F_i' \parallel RPW_i') = h(ID_i \parallel K_{GWN}) \oplus h(F_i \parallel RPW_i) \oplus h(RPW_i' \parallel F_i') \oplus h(ID_i \parallel K_{GWN}) \). The \( SC_i \) selects a nonce \( r \) and \( U_{SK} \in Z_n^* \) and computes, \( M_r = rP, M_1 = rX = rxP \), and \( M_2 = ID_i \oplus M_1 = ID_i \oplus rxP \), \( M_3 = SID_j \oplus h(C_i \parallel M_2), M_4 = h(C_i \parallel SID_j) \parallel M_1 \parallel T_i \) and \( M_5 = U_{SK} \oplus h(M_3) \oplus C_i \). At the last, the login (request) message \( \{M_0, M_2, M_3, M_4, M_5, T_i\} \) is transmitted by \( U_i \) to GWN via the public channel.

Authentication phase

At this stage, the entities are required to verify each other’s identities, i.e., mutual authentication. In addition, they must generate a shared session key to securely exchange sensitive information over the Internet. In this study, we implement authentication in the manner described below.

Step 1: Presume that GWN gets the login request message \( \{M_0, M_2, M_3, M_4, M_5, T_i\} \) at \( T_2 \). And checks

\( h(RPW_i' \parallel ID_i \parallel F_i') \) and check \( A_i' = A_i \), if unequal then the session is terminated by the \( SC_i \) else user's identity, password and biometric altogether are verified.

\( M_1 = ID_i \oplus rxP \), \( M_2 = ID_i \oplus rP \), \( M_3 = SID_j \oplus h(C_i') \parallel M_1 \parallel T_i \) and \( M_4 = h(C_i' \parallel SID_j') \parallel M_1 \parallel T_i \) and checks if \( M_4 = M_4 \), if not then the session is rejected else \( U_i \) is authenticated to GWN. And computes \( U_{SK}' = M_5 \oplus h(M_1') \oplus C_i', MID_i = h((ID_i') \parallel T_i) \). Then compute the required message for \( SN_j \) as \( M_6 = ID_i \oplus h((ID_i') \parallel K_{GWN}) \parallel T_3 \) and chooses a nonce \( G_{SK} \in Z_n^* \) and compute \( M_7 = G_{SK} \oplus MID_i, M_8 = G_{SK} \oplus U_{SK}' \), \( M_9 = h(G_{SK} \parallel U_{SK}') \parallel h((ID_i') \parallel K_{GWN}) \parallel MID_i \parallel T_3 \). At last, GWN transmits the communication \( \{M_6, M_7, M_9, M_9, T_3\} \) to \( SN_j \) through the public medium.
Step 2: Presume that $SN_j$ receives the messages $(M_6,M_7,M_8,M_9,T_3)$ at $T_4$ and checks if $(T_4 - T_3) \leq \Delta T$ is in an allowed interval or not. If not then the session is rejected by $SN_j$ else computes $M'_6 = M_6 \oplus h(K_{GWN-S} \parallel T_3) = MID_t,G_{SK} = M_7 \oplus MID_t = G_{SK},U'_j = M_8 \oplus G_{SK} = G_{SK} \oplus U'_j \oplus G_{SK} = U_{SK},M'_6 = h(G_{SK} \parallel U_{SK} \parallel K_{GWN-S} \parallel MID_t \parallel T_3)$ and checks $M'_6 \neq M_6$, if not session is terminated by $SN_j$. Otherwise $SN_j$ chooses a nonce $S_{SK} \in Z_n^*$ and evaluates the session key as $SK_j = h(MID_t \parallel SID_j \parallel U'_j \parallel G_{SK} \parallel S_{SK}),M_{10} = S_{SK} \oplus h(G_{SK} \parallel K_{GWN-S}),M_{11} = h(G_{SK} \parallel S_{SK} \parallel U'_j \parallel MID_t \parallel T_3)$. At the last, $SN_j$ sends response $(M_{10},M_{11},T_3)$ to $GWN$ via the public channel.

Step 3: Presume that $GWN$ receives the message as $(M_{10},M_{11},T_3)$ at $T_6$ and checks if $(T_6 - T_5) \leq \Delta T$ in an acceptable interval or not. If not then the session is rejected otherwise $GWN$ computes and retrieves $S_{SK} = M_{10} \oplus h \left( G_{SK} \parallel h(SID_j \parallel K_{GWN}) \right) = S_{SK},M'_11 = h(G_{SK} \parallel S'_{SK} \parallel U'_j \parallel MID_t \parallel T_3)\text{ and checks } M'_11 \neq M_{11} , \text{ if not the session is rejected by the } GWN.$ Otherwise, $GWN$ computes the session key as $SK_g = h(MID_t \parallel SID_j \parallel U'_j \parallel G_{SK} \parallel S_{SK}),M_{12} = G_{SK} \oplus M_1,M'_{13} = S'_{SK} \parallel MID_t,M_{14} = h(G_{SK} \parallel S'_{SK} \parallel U'_j \parallel MID_t \parallel T_7)$. At the last, $GWN$ sends a message $(M_{12},M_{13},M_{14},T_7)$ to $U_i$ via public channels.

Step 4: Presume that $U_i$ accepts the message $(M_{12},M_{13},M_{14},T_7)$ at $T_8$ and checks if $(T_8 - T_7) \leq \Delta T$ is in an acceptable interval or not. If not, session is terminated else $U_i$ computes and retrieves $G_{SK} = M_{12} \oplus M_1 = G_{SK} \oplus xrP \oplus xrP = G_{SK},S'_{SK} = M_{13} \parallel MID_t$. Computes session key $SK_i = h(MID_t \parallel SID_j \parallel U'_j \parallel G_{SK} \parallel S'_{SK}),M'_14 = h(G_{SK} \parallel S'_{SK} \parallel U'_j \parallel MID_t \parallel T_7)$ . Checks $M'_14 \neq M_{14}$. If unequal then the session is rejected by the user else mutual authentication is performed successfully based on the session key generation i.e., $SK_i = SK_j = SK_g$. Finally, $U_i$ being the legitimate user is permitted to access the sensory data of $SN_j$ through the $GWN$.

Table 2 illustrates a summary of the devised login and authentication phase, including the session key agreement.

### Password change phase

Here, $U_i$ can freely modify passwords as many times as they want without the intervention of $GWN$. This updation procedure is performed locally and in offline mode by using only the $SC_i$. This phase is described below:

---

### Step 1: The $U_i$ loads the $SC_i$ into a specific gadget and input $ID_i, PW_i$ and gives biometric $b'_i$, and gets $F'_i = H(b'_i)$. Then $SC_i$ computes $a'_i = V_i \oplus a_i, RPW'_i = h(a'_i \parallel PW_i)$ and $A'_i = h(RPW'_i \parallel ID \parallel F'_i)$. Verifies $A'_i = A_i$ if the unequal session is rejected otherwise legitimacy of $U_i$ is ensured, thus permission for password update $PW_{\text{new}}$ is granted.

### Step 2: Now, $SC_i$ computes $RPW_{\text{new}} = h(PW_{\text{new}} \parallel a'_i), A_{\text{new}} = h(ID_i \parallel RPW_{\text{new}} \parallel F'_i)$ and $B_{\text{new}} = B_i \oplus h(RPW_i \parallel F'_i) \oplus h(RPW_{\text{new}} \parallel F'_i) = h(ID_i \parallel K_{GWN}) \oplus h(RPW_{\text{new}} \parallel F'_i)$ and updates $A_i, B_i$ by $A_{\text{new}}, B_{\text{new}}$ respectively.

### Authentication verification utilizing BAN logic

The Burrows-Abadi-Needham (BAN) logic is considered a formal model to test the session key and mutual authentication negotiation among legitimate parties. A formal BAN logic (Ali et al., 2018; Soni et al., 2021) analysis of the proposed scheme's security goals is presented below:

### Goal 1: $GWN \equiv U_i \rightarrow SK GWN$

### Goal 2: $GWN \equiv U_i \rightarrow SK GWN$

### Goal 3: $SN_j \equiv GWN \rightarrow SK SN_j$

### Goal 4: $SN_j \equiv GWN \rightarrow SK SN_j$

### Goal 5: $GWN \equiv SN_j \rightarrow SK GWN$

### Goal 6: $GWN \equiv SN_j \rightarrow SK GWN$

### Goal 7: $U_i \equiv GWN \rightarrow SK U_i$

### Goal 8: $U_i \equiv GWN \equiv SK U_i$

### Step 2: Conversion of communication messages into Idealized form:

$\text{Msg1: } U_i \rightarrow GWN: \{M_0, M_2, M_3, M_4, M_5, T_1\}$

$M_0: < r \rightarrow p, M_2: < ID_i \rightarrow r, X, M_3: < SID_j \rightarrow h(h(ID_i \parallel K_{GWN}) \parallel ID \parallel r, X), M_4: < SID_j \rightarrow h((ID_i \parallel K_{GWN}), r, X, T_1), M_5: < U_{SK} \rightarrow h((ID_i \parallel K_{GWN}), X)$

$\text{Msg2: } GWN \rightarrow SN_j: \{M_6, M_7, M_8, M_0, T_3\}$

$M_6: < MID_i \rightarrow h(K_{GWN-S}), T_3, M_7: < G_{SK} > MID_i, M_8: < U'_j > G_{SK}, M_9: h(G_{SK}, U_{SK}, K_{GWN-S}, MID_i, T_3)$

$\text{Msg3: } SN_j \rightarrow GWN: \{M_{10}, M_{11}, T_5\}$

$M_{10}: < S_{SK} > h(c'_i, K_{GWN-S}), M_{11}: h(G_{SK}, S_{SK}, U'_{SK}, MID_i, T_5)$

---

DOI: https://doi.org/10.52756/jerr.2024.v39sp1.012
Step 3: Further, certain assumptions to validate the reliability of the proposed system include:

A1: $U_i \equiv \#(U_{SK}, r, T_1, T_T) \quad (U_{W}, T_1)$

A2: $GW \equiv \#(U_{SK}, G_{SK}, T_3, T_5, T_T)$

A3: $SN_j \equiv \#(U_{SK}, G_{SK}, T_3, T_5, T_T)$

A4: $U_i \equiv SN_j \quad (SN_j) \quad (GW)$

A5: $GW \equiv (SN_j)$

A6: $SN_j \equiv SN_j \quad (SN_j) \quad GW$}

Step 4: BAN logic analysis demonstrates that the approach proposed achieves the goals depending on Steps 2 and 3:

According to the idealized form of Msg1:

$$\text{Msg1:} \quad U_i \rightarrow GW: \{M_{12}, M_{13}, M_{14}, T_T\}$$

$M_{12}: G_{SK} > rX, M_{13}: < S'_{SK} > M_{ID_T}$

$M_{14}: h(G_{SK}, S'_{SK}, U_{SK}, M_{ID_T}, T_T)$

Step 4: By seeing Msg1, we get

S1: $GW \rightarrow h(\langle rX, S'_{SK}, U_{SK}, M_{ID_T}, T_T \rangle)$

S2: $GW \equiv U_i \sim U_{SK}$
According to nonce verification rule, freshness concatenation, A2 and S2, we procure:

\[ S3: GWN \equiv U_i \equiv U_{SK}, \text{ here } U_{SK} \text{ is the required parameter for the session key of the proposed scheme.} \]

According to jurisdiction rule, S3 and A8, we procure

\[ S4: GWN \equiv U_{SK} \]

According to S3, A2 and session key rule, we procure

\[ S5: GWN \equiv U_i \xrightarrow{SK} GWN \]

**Goal 1 is achieved**

As per S5, A2 and nonce verification rule we procure

\[ S6: GWN \equiv U_i \equiv U_{SK} \xrightarrow{SK} GWN \]

**Goal 2 is achieved**

According to the idealized form of Msg2:

\[ \text{Msg2: } GWN \rightarrow SN_j: \{M_6, M_7, M_8, M_9, T_3\} \]

where \( M_6: \{MID_i > h(k_{GWN-S}), T_3\}, \)

\( M_7: < G_{SK} > MID_i, M_8: < U_{SK} > G_{SK}, \)

\( M_9: h(G_{SK}, U_{SK}, K_{GWN-S}, MID_i, T_3) \)

By seeing Msg2, we get

\[ S7: SN_j \equiv < MID_i > h(k_{GWN-S}), T_3, < G_{SK} > \]

\( MID_i < U_{SK} > G_{SK}, h(c^*), T_3 \)

where \( c^* = G_{SK}, U_{SK}, K_{GWN-S}, MID_i, T_3 \)

Using S7, A5 and message meaning rule we procure

\[ S8: SN_j \equiv GWN \sim G_{SK} \]

As per S8, A3, nonce verification and freshness concatenation rules, we get

\[ S9: SN_j \equiv GWN \equiv G_{SK}, \text{ here } G_{SK} \text{ is the required component for the proposed scheme's session key.} \]

As per S9, A9 and jurisdiction rules, we procure

\[ S10: SN_j \equiv G_{SK} \]

As per S9, A3 and the session key rule we procure

\[ S11: SN_j \equiv GWN \xrightarrow{SK} SN_j \]

**Goal 3 is achieved**

As per the nonce verification rule, S11 and A3, we procure

\[ S12: SN_j \equiv GWN \equiv GWN \xrightarrow{SK} SN_j \]

**Goal 4 is achieved**

According to the idealized form of Msg3:

\[ \text{Msg3: } SN_j \rightarrow GWN: \{M_{10}: < \}

\[ S_{SK} > h(g_{SK}^{i'}, K_{GWN-S}), M_{11}: h(e^*), T_5 \}

where \( e^* = G_{SK}, S_{SK}, U_{SK}^{i'}, MID_i, T_5 \)

By seeing Msg3, we get

\[ S13: GWN \equiv < \]

\[ S_{SK} > h(g_{SK}^{i'}, K_{GWN-S}), h(G_{SK}, S_{SK}, U_{SK}^{i'}, MID_i, T_5), T_5 \]

Based on the principle of message meaning, A6 and S13, we procure

\[ S14: GWN \equiv SN_j \equiv S_{SK} \]

As per S14, A2, nonce verification and freshness concatenation rules, we get

\[ S15: GWN \equiv SN_j \equiv S_{SK}, \text{ here } S_{SK} \text{ is the required component for the proposed scheme's session key.} \]

From jurisdiction rule, S15 and A10, we get

\[ S16: GWN \equiv S_{SK} \]

As per session key rule, S15 and A2, we procure

\[ S17: GWN \equiv SN_j \xrightarrow{SK} GWN \]

**Goal 5 is achieved**

As per the nonce verification rule, S17 and A2, we procure

\[ S18: GWN \equiv SN_j \equiv SN_j \xrightarrow{SK} GWN \]

**Goal 6 is achieved**

According to the idealized form of Msg4:

\[ \text{Msg4: } GWN \rightarrow U_i: \{M_{12}: < G_{SK} > rX, M_{13}: < S_{SK} > MID_i, M_{14}: h(f^*), T_7 \}

where \( f^* = G_{SK}, S_{SK}, U_{SK}^{i'}, MID_i, T_7 \)

By seeing Msg4, we get

\[ S19: U_i \equiv < G_{SK} > rX, < S_{SK} > \]

\( MID_i, h(G_{SK}, S_{SK}, U_{SK}^{i'}, MID_i, T_7), T_7 \)

Using message meaning rules, S19 and A7 we procure

\[ S20: U_i \equiv GWN \sim G_{SK} \]

As per S20, A1, nonce verification and freshness concatenation rules, we get

\[ S21: U_i \equiv GWN \equiv G_{SK}, \text{ here } G_{SK} \text{ is the required component for the proposed scheme's session key.} \]

From S21, A11 and jurisdiction rule, we procure

\[ S22: U_i \equiv G_{SK} \]

As per session key rules, A1 and S21 we procure

\[ S23: U_i \equiv GWN \xrightarrow{SK} U_i \]

**Goal 7 is achieved**

As per nonce verification rule, A1 and S23, we procure

\[ S24: U_i \equiv GWN \equiv GWN \xrightarrow{SK} U_i \]

**Goal 8 is achieved**

Hence, mutual authentication as well as the session key \( SK_i = SK_j = SK_{ij} \) are mutually created between \( U_i \) and \( S_j \) via \( GWN \).

**Informal security analysis**

The informal security analysis of the proposed approach shows that the protocol is capable of resisting many types of known attacks.

**Sensor node capture attack**

When \( U_i \) accesses the data of sensor node \( SN_j \), all the information exchanged during the authentication process with \( SN_j \) are stored in its memory like \( SID_j, K_{GWN-S} = h(SID_j \parallel K_{GWN}), SK_j \), messages \( \{M_6, M_7, M_8, M_9, T_3\} \) sent by \( GWN \) to \( SN_j \) and sent by \( SN_j \) to
where, $M_{10} = S_{SK} \oplus h(G'_{SK} \parallel K_{GWN-S}), M_{11} = h(G'_{SK} \parallel S_{SK} \parallel U_{SK}' \parallel S_{SK} \parallel MID_{T})$. Thus, we infer that the proposed scheme is resistant to sensor node impersonation attacks.

Resists user impersonation attack

Suppose $\hat{A}$ tries to impersonate a registered user $U_a$ to a legal sensor node $SN_k$ and $GWN$, based on some disclosed secret data from previous attacks. In the proposed scheme, as per the sensor node capture attack (Alhawat and Bathla, 2023), only $U_1's$ and $SN_k's$ data are known to $\hat{A}$ and fails to retrieve other legal users' and sensor node's data. Here to access sensor node $SN_k$, $\hat{A}$ tries to impersonate as $U_a$ to $GWN$ and $SN_k$ (non-captured) and for that, he/she computes the login request message $\{M_0, M_2, M_3, M_4, M_5, T_1\}$ to be sent to $GWN$ through a public channel. First $\hat{A}$ chooses a nonce $r$ and $U_{SK} \in Z_{n}$. As P and X are the public parameters of $GWN$ so $\hat{A}$ can compute $M_3 = rP$ and $M_4 = rX$. But fails to compute $M_2 = ID_a \oplus M_1$ as $ID_a$ is not known. Similarly a value of $SID_t, h(ID_{a} \parallel K_{GWN})$ are unknown so could not compute $M_3 = SID_t \oplus h(C_{a} \parallel M_1)$, $M_4 = h(C_{a} \parallel SID_{t} \parallel M_1 \parallel T_1)$ and $M_5 = U_{SK} \oplus h(M_1) \parallel C_{a}$. Thus, as $\hat{A}$ fails to evaluate the login request message, so we infer that the proposed approach is resilient to user impersonation attacks.

Resists gateway node impersonation attack

A Gateway node impersonation attack is feasible if any paired user and sensor node like $U_a$ and $SN_k$, whose data were leaked due to sensor node capture (Alhawat and Bathla, 2023; Jha et al., 2024b) in continuation of a few more attacks discussed above. But, as we have seen the proposed scheme contains data in highly encrypted form, which resists all the aforesaid attacks as well as resists the gateway node impersonation attack.

Resists replay attack

The proposed scheme transmits five messages $M_4 = h(C_{a} \parallel SID_{t} \parallel M_1 \parallel T_1)$, $M_7 = G_{SK} \parallel MID_{T}$, $M_9 = h(G_{SK} \parallel U_{SK}' \parallel h(SID_{t} \parallel K_{GWN}) \parallel MID_{T} \parallel T_3)$, $M_{11} = (G'_{SK} \parallel S_{SK} \parallel U_{SK}' \parallel MID_{T} \parallel T_5)$ and $M_{14} = h(G_{SK} \parallel S_{SK} \parallel U_{SK}' \parallel MID_{T} \parallel T_7)$ through public channels. As these messages contain a nonce and timestamp so whenever any of the legitimate parties get the above messages, first, it confirms the freshness of the timestamp. In case the timestamp is not valid, the current session is rejected. Hence, the inclusion of timestamps and nonce prevents unauthorized parties from replaying these messages. Therefore, we infer that the proposed approach is resilient to replay attacks.

Resists stolen smart card attack

A smart card contains $\{A_i, B_i, h(\cdot), H(\cdot), X, P, V_i\}$ where, $A_i = h(ID_i \parallel B_i \parallel h(RPW_{i} \parallel F_i))$, $B_i = h(ID_i \parallel K_{GWN}) \oplus h(RPW_{i} \parallel F_i)$, $X = xP$ is a public key of $GWN$. $P$ is the generator point on an elliptic curve and $V_i = a_i \parallel F_i$. From above values $\hat{A}$ cannot reveal the password or ID of a legitimate user as personal data are in highly encrypted form. Thus $\hat{A}$ cannot use the stored data in the SC for further evaluation so we deduce that the proposed scheme is resistant to stolen smart card attack.
Resists insider attack

To resist insider attack, user ID and password are not saved in any of the databases, not even GWN, in the proposed scheme. Personal information like user ID is in highly secured encrypted form \( MID_i = h(h(ID_i) \parallel T_n) \), where \( T_n \) is the timestamp which makes it random each time and also it’s hard to reveal ID from \( M_k = h(C_i \parallel SID \parallel M_1 \parallel T_1) \) and \( RPW_i = h(PW_i \parallel a_i) \), where \( a_i \) does the user choose the nonce at the time of registration.

Resists denial of service (DoS) attack

\( U_i \) inserts SC into a card reader and provides \( ID_i, PW_i \) gives the biometric \( b'_i \) on the particular device and gets \( F'_i = H(b'_i) \). Then, SC computes \( a'_i \) as \( V_i \oplus F'_i = a'_i \oplus F'_i \oplus i'_t = a_i, RPW'_i = h(a'_i \parallel PW'_i), A'_i = h(RPW'_i \parallel ID_i \parallel F'_i) \) and check \( A'_i = A_i \), if unequal then the session is rejected by the SC else user’s ID, password and biometric altogether are verified and allowed to send login requests to GWN. Hence, from above we infer that the proposed scheme is resistant to the denial-of-service attack as the login process begins only after \( ID_i, PW_i \) and biometrics of the user \( F_i \) is verified as a legitimate user by the system.

Mutual authentication

The proposed scheme allows users to access the sensory data only after fruitful authentication among the participating entities. At first, as per the login request message received \{\( M_0, M_2, M_3, M_4, M_5, T_1 \}\), GWN authenticates the user. After that, as per the received message \{\( M_6, M_7, M_8, M_9 \}\) sensor node authenticates the GWN. Similarly, GWN authenticates the sensor node based on the received response message \{\( M_{10}, M_{11}, T_3 \}\) sent by the sensor node. At last, the user authenticates the GWN based on the message \{\( M_{12}, M_{13}, M_{14}, T_7 \)\}. Therefore, all the entities mutually authenticate one another, to validate their legitimacy using their respective messages.

Resists known session-specific temporary information attack

In this proposed scheme, a secret session key \( SK_i = h(MID_i \parallel SID \parallel U_{SK} \parallel G_{SK} \parallel S_{SK}) \) is evaluated by the user, GWN and the sensor node using the nonce \( U_{SK}, G_{SK} \) and \( S_{SK} \) respectively and unidentified \( SID \) and \( ID_i \). Suppose an adversary can disclose \( SID_j \). But it’s impossible to evaluate the session key without knowing \( MID_i = h(h(ID_i) \parallel T_2) \) as this parameter is in highly encrypted form in combination with the timestamp. And it’s infeasible to disclose or guess the nonce \( U_{SK}, G_{SK} \) and \( S_{SK} \). So, we deduce that the proposed scheme resists this attack.

Simulation evaluation of the proposed scheme based on the AVISPA tool

Here we see the security proof for the proposed system, demonstrated with the help of the Automated Validation Information Security Protocols and Applications (AVISPA) tool (Soni et al., 2019a; Soni et al., 2019b; Armando et al., 2005) whose simulation in Figure 2, 3 and 4 result verifies the resistance of the proposed scheme towards replay attack and man-in-the-middle attack. Furthermore, security analyses are done for the On-the-Fly Model Checker (OFMC) and the Constraint Logic-based Attack Searcher (CL-AtSe). The implementation of the simulation code is done using High-Level Protocol Specification Language (HLPSL) for \( U_i \), GWN and \( SN_j \). Figure 5 (a) and (b) demonstrate the result in OFMC and CL-AtSe, respectively, as a back end. The simulation outcome is “SAFE”, validating the safety and resistance of the proposed approach against replay attacks and man-in-the-middle attacks.

Results & Discussion

This section includes a performance comparison of the proposed approach with various relevant schemes regarding functional features and security, computational overhead in terms of seconds and communication overhead including smart card storage in bits. Table 3 shows the comparisons of functional features and security of the proposed scheme in comparison to other relevant schemes (Liu et al., 2019; Vinoth et al., 2020; Far et al., 2021; Wu et al., 2021; Saqib et al., 2022; Wang et al., 2023). The schemes (Liu et al., 2019; Vinoth et al., 2020; Far et al., 2021; Wu et al., 2021) are suffering from user anonymity. The schemes (Saqib et al., 2022; Mirsaraei et al., 2022) lack unauthorized login detection features, thereby being unsuitable for the IoT environment.

As a corollary, compared with the relevant schemes mentioned above, our proposed scheme outperforms and achieves superior security and functional features. Moreover, the proposed approach repels attacks like insider attacks, smart card stolen attacks, sensor node impersonation attacks, user impersonation attacks, etc. Table 4 represents the computational and communication overhead in the login and authentication phase of the proposed approach and the relevant schemes (Liu et al., 2019; Vinoth et al., 2020; Far et al., 2021; Wu et al., 2021; Saqib et al., 2022; Wang et al., 2023) along with smart card storage. The computation cost is only related to the login and authentication phase as the resource limitation features of the gateway node and sensor nodes. Here, we assume \( T_{EC} \) and \( T_{H} \) represent the execution time of elliptic curve point multiplication and hash function.

DOI: https://doi.org/10.52756/jerr.2024.v39sp1.012
respectively. The values of the computational cost of $T_{EC}$ and $T_H$ are 0.063075s and 0.0005s (Das et al., 2016), respectively. Additionally, for computing smartcard storage and communication cost, i.e., the total bits transmitted in the login and authentication phase, we have assumed that the length of the password, identity, nonce and time stamps are 64 bits (Soni et al., 2019b) each. The length of the secret key of GWN is 1024 bits (Soni et al., 2019b), the length of a hash function is 160 bits (Soni et al., 2019b) and the length of ECC point $P$ is 320 bits (Soni et al., 2019b).

![Figure 2. HLPSL code for user](Image)

```hlpsl
role user (Ui, SNj, GWN : agent,
          SK1 : symmetric_key,
          SK2 : symmetric_key,
          Xor, Mul, H, H1 : hash_func,
          Snd, Rcv : channel (dy))
play_by
 def local State: nat,
    SIDj, KGWNS, RPWi, B1, Fi,
    Fi, Ai, Ci, Bi, X1, A1i, Bi, Ci, XP, Vi, A1, USK, GSK, SSK, PWi, IDi, RB21, MDi,
    M19, SKj, UISK, RPWi, i, Bi, SiSK, SK, Mi14, KGWN, IDii, V, SIDjj,
    Mi, M1, Mi11, SKGWNS, Ti1, Ui, Si, Mi6, T1, T3, T5, T7 : text,
    M0, M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, M12, M13, M14 : message,
    Inhash_func
 const user_gway_usk, gway_user_gsk, snode_user_gsk, user_snake_usk,
    snode_gway_gsk, gway_snake_gsk,
    subs1, subs2, subs3, subs4, subs5, subs6 : protocol_id
init State := 0

transition
% Start of registration phase of the user
1. State := 0/Rcv(start) =>
   State := 1/Fi := H1(B1)
   /RPWi := H(PWi, A1)
   % Send registration request message to GWN
   /Snd ((IDi, RPWi, Fi)_SK )
   /secret ((PWi, A1, B1), subs1, Ui)
   /secret ((RPWi, Fi), subs2, {Ui, GWN})
2. State := 1/Rcv ((Ai, Bi, X, P)_SK ) =>
   % Receives smart card information from GWN
   State := 2/Ri := new()
   /Vi := Xor(A1, Fi)
   /B21 := Xor(Vi, Fi)
   /RPWi := H(PWi, A1 )
   /Ai := H(IDi, RPWi, Fi)
   /Ci := Xor(Bi, H(RPWi, Fi))
   /Ti := new()
   /USK := new()
   /M0 := Mul(R, P)
   /M1 := Mul(R, X)
   /M2 := Xor(IDi, M1)
   /M3 := Xor(SIDj, H1(Ci, M1))
   /M4 := H(Ci, SIDj, M1, T1)
   /M5 := Xor(U, SKH, H1(Ci, M1))
   /Snd(M0, M2, M3, M4, M5, T1)
% Send login message to the GWN
   /secret ((IDi, USK, SIDj), subs3, {Ui, GWN, SNj})
   /witness(Ui, GWN, user_gway_usk, USK)
3. State := 2/Rcv(M12, M13, M14, T7) =>
   State := 3/Gi := Xor(M12, M1)
   /SiSK := Xor(M13, M12)
   /SK := H(M13, SIDj, USK, GSK, SiSK)
   /Mi14 := H(Gi, SK, SiSK, USK, Mi14, T7)
   /request(GWN, Ui, gway_user_gsk, GSK)
   /request(SNj, Ui, snode_user_gsk, SK)
end role
```
Therefore, the overall communication cost of the proposed scheme is 2880 bits and to store the parameters, a smart card requires 1440 bits of memory. Similarly, the total computation overhead of the proposed scheme for the login and authentication phase is $27T_H + 3T_{EC}$ which takes 0.202725s to execute. Thus, from the performance comparison point of view, the low communication overhead, computation cost, and smartcard storage indicate that our scheme is highly applicable to IoT devices and offers enhanced security.

**Figure 3. HLPSL code for gateway node**
role sensor(Ui,GWN,SNj:agent,
SK1:symmetric_key,
SK2:symmetric_key,
Xor,Mul,H,HL:hash_func,
Snd.Rcv:channel(dy))
played_by SNj
def=
local State:mat,
SIDj:KGWNS,RPWi,B1,B2,Ai,Bi,X,Xi,P,V,F1i,Cii,Fi,Ci,Aii,Bii,Biii,SIDi,A1,
USK,GSK,SSK,RPWi,DIi,R,B21,MIDi,M19,SKj,UiSk,RPWij,B1i,SiSK,
SK,Mi14,KGWNS,DIiV,SIDj,Mi4,Mi1,Mi11,SKGWNS,TiI,Usk,Mi6,GiSK,T1,
T3,T5,T7:text,
M0,M1,M2,M3,M4,M5,M6,M7,M8,M9,M10,M11,M12,M13,M14:message,
Inc:hash_func
const user_gway_usk,gway_user_gsk,snode_user_ssk,snode_snode_usk,
snode_gway_ssk,gway_snode_gsk,
subs1,subs2,subs3,subs4,subs5,subs6:protocol_id
init State:0
transition
1.State=0/Rcv(M6,M7,M8,M9,T3) =>
?State'=1/SSK':=new()
?/Mi6'=Xor(M6,H(KGWNS.T3))
?/GiSk'=Xor(M7,MIDI)
?/UiSK'=Xor(M8,GSK)
?/M19'=H(GSK.Usk.T3.KGWNS.MIDI)
?/T5'=new()
?/SKj'=H(MIDI.SIDj.USK.GSK.SSK)
?/M10'=Xor(SSK.H(GSK.KGWNS))
?/M11'=H(GSK.USk.Usk.MIDI.T5)
?/Snd(M10'.M11'.T5')
?/secret({SSK},subs6, (GWN,SNj,Uij))
?%request(Ui,SNj,snode_usk,USK)
?/request(GWN,SNj,gway_snode_gsk,GSK)
?/witness(SNj,GWN,snode_gway_ssk,SSK)
end role

**Figure 4.** HLPSL code for sensor node.

**Figure 5(a).** Simulation output in CL-AtSe back-end.
Table 3. Comparison of functional features and security.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SP1</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP3</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP4</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP5</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SP6</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP7</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP8</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP9</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP10</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SP11</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 4. Computational and communication overhead comparison.

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Computation cost (in second)</th>
<th>Smart card storage (in bits)</th>
<th>Communication Cost (in bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liu et al., 2019</td>
<td>$14T_{Ii} + 12T_{EC} \approx 0.764$</td>
<td>1248</td>
<td>2880</td>
</tr>
<tr>
<td>Vinoth et al., 2020</td>
<td>$19T_{Ii} + 1T_{EC} \approx 0.730$</td>
<td>2048</td>
<td>3040</td>
</tr>
<tr>
<td>Far et al., 2021</td>
<td>$24T_{Ii} + 4T_{EC} \approx 0.264$</td>
<td>2400</td>
<td>2216</td>
</tr>
<tr>
<td>Wu et al., 2021</td>
<td>$27T_{Ii} + 7T_{EC} \approx 0.455$</td>
<td>2048</td>
<td>1824</td>
</tr>
<tr>
<td>Saqib et al., 2022</td>
<td>$9T_{Ii} + 10T_{EC} \approx 0.635$</td>
<td>N/A</td>
<td>2720</td>
</tr>
<tr>
<td>Wang et al., 2023</td>
<td>$10T_{Ii} + 10T_{EC} \approx 0.636$</td>
<td>640</td>
<td>3808</td>
</tr>
<tr>
<td>Saini et al., 2024</td>
<td>$36T_{Ii} + 5T_{EC} \approx 0.395$</td>
<td>1152</td>
<td>2304</td>
</tr>
<tr>
<td>Huang, 2024</td>
<td>$48T_{Ii} + 12T_{EC} \approx 0.781$</td>
<td>1120</td>
<td>3650</td>
</tr>
<tr>
<td>Proposed scheme</td>
<td>$27T_{Ii} + 3T_{EC} \approx 0.202$</td>
<td>1440</td>
<td>2880</td>
</tr>
</tbody>
</table>

Note: SP1: Session key agreement; SP2: Mutual authentication; SP3: User anonymity; SP4: Easily password change; SP5: Unauthorized login detection; SP6: Apt for IoT environment; SP7: Resist replay attack; SP8: Resist stolen smartcard attack; SP9: Resist the user impersonation attack; SP10: Resist the gateway node impersonation attack; SP11: Resist the sensor node impersonation attack.
Conclusion

A proposal has been put forward to enhance the security of CPS in healthcare by implementing an ECC-based resilient three-factor authentication and key agreement scheme. Moreover, it effectively addresses the limitations observed in prior password or two-factor-based authentication schemes. This scheme utilizes the lightweight and robust ECC. The effectiveness of the proposed approach in establishing mutual authentication is validated using BAN logic. Furthermore, the simulation outcome, conducted using the AVISPA tool, validates the effectiveness of the proposed scheme in mitigating both passive and active threats. The informal security perusal additionally guarantees that the suggested scheme successfully attains every specified security characteristic (even though the sensor node gets captured), which is essential for the development of secure session key agreements and mutual authentication between different parties. Hence, the aforementioned strategy has been demonstrated to be a more advantageous option in terms of both security and efficiency. It can be considered as the state-of-the-art for key agreements and mutual authentication for CPS applications in remote healthcare monitoring for smart cities.

Conflict of Interest

The authors declare no conflict of interest.

References


DOI: https://doi.org/10.52756/ijerr.2024.v39spl.012


