DOI: https://doi.org/10.52756/ijerr.2024.v39spl.012 *Int. J. Exp. Res. Rev.*, Vol. 39: 154-169 (2024)

Original Article | Peer Reviewed | Open Access

International Journal of Experimental Research and Review (IJERR)

ISSN: 2455-4855 (Online)
www.iaph.in

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

Article History:

Received: 4th March, 2024
Accepted: 22nd May, 2024
Published: 30th May, 2024

Keywords:

Authentication, AVISPA tool, BAN logic, biometric, elliptic curve cryptosystem, wireless sensor network

How to cite this Article:
Khushboo Jha, Aruna Jain and Sumit Srivastava (2024). A Secure Biometric-Based User Authentication Scheme for Cyber-Physical Systems in Healthcare. *International Journal of Experimental Research and Review*, *39*(spl.) 154-169.
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

*Corresponding Author: kjha.phd@gmail.com

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.

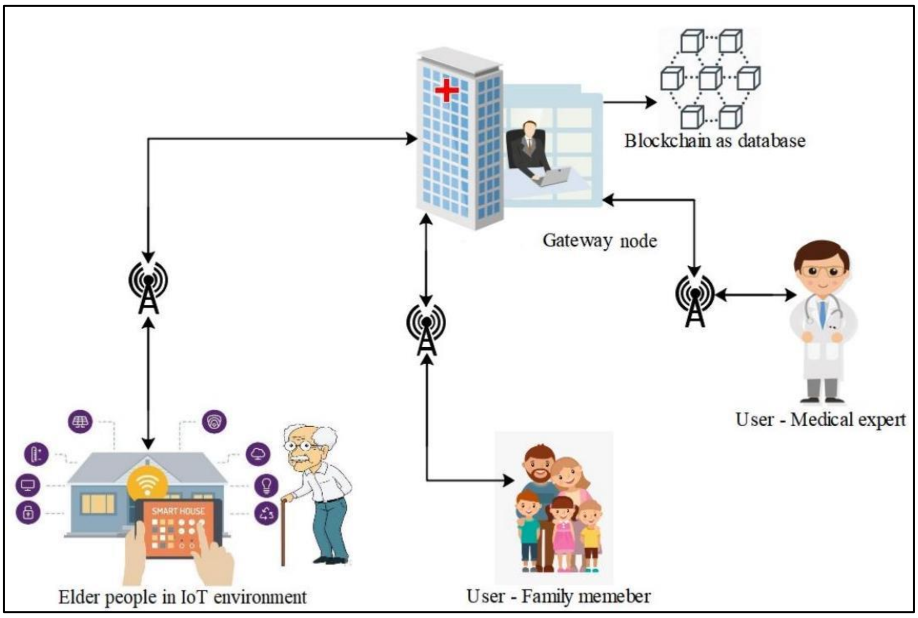

Figure 1. Proposed WSN-based model for the healthcare system.

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.

$h(RPW_i' \| ID_i \| F_i')$ and check $A_i' \stackrel{?}{=} A_i$, 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 $C_i = B_i \oplus h(F_i' \parallel RPW_i') = h(ID_i \parallel K_{GWN}) \oplus h(F_i \parallel RPW_i) \oplus h(RPW_i' \parallel F_i') = h(ID_i \parallel K_{GWN})$. The SC_i selects a nonce r and $U_{SK} \in Z_n^*$ and computes, $M_0 = rP, M_1 = rX = rxP, M_2 = ID_i \oplus M_1 = ID_i \oplus rxP, M_3 = SID_j \oplus h(C_i \parallel M_1), M_4 = h(C_i \| SID_j \| M_1 \parallel T_1)$ and $M_5 = U_{SK} \oplus h(M_1) \oplus C_i$. At the last, the login (request) message $\{M_0, M_2, M_3, M_4, M_5, T_1\}$ 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 $\{M_0, M_2, M_3, M_4, M_5, T_1\}$ at T_2. And checks

Table 1. User registration phase.

U_i		GWN
U_i selects ID_i, PW_i produce a nonce a_i calculates $RPW_i = h(a_i \parallel PW_i)$ stamps the biometric b_i on a specific gadget and gets F_i as $H(b_i)$		
	$\xrightarrow{\{ID_i, F_i, RPW_i\}}$ secure channel	Calculates $A_i = h(ID_i \| F_i \| RPW_i)$, $B_i = h(RPW_i \parallel F_i) \oplus h(ID_i \parallel K_{GWN})$,
Stores a_i as $V_i = a_i \oplus F_i$ SC_i contains $\{A_i, B_i, \mathrm{h}(.), \mathrm{H}(.), \mathrm{X}, \mathrm{P}, V_i\}$	send the SC_i $\longleftarrow$ secure channel	stores $\{A_i, B_i, \mathrm{h}(.), \mathrm{H}(.), \mathrm{X}, \mathrm{P}\}$ in the SC_i

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 $a_i' = V_i \oplus F_i' = a_i \oplus F_i \oplus F_i' = a_i, RPW_i' = h(a_i' \parallel PW_i), A_i' =$

$(T_2 - T_1) \leq \triangle T$ is in the acceptable interval or not. If not then the session is terminated by GWN else evaluates $M_1' = xM_0 = xrP, ID_i' = M_2 \oplus M_1' = ID_i \oplus rxP \oplus rxP$ and $C_i' = h(ID_i' \parallel K_{GWN})$ and retrieve $SID_j' = M_3 \oplus h(C_i' \parallel M_1')$, $M_4' = h(C_i' \| SID_j' \| M_1' \parallel T_1)$ and checks if $M_4' \stackrel{?}{=} M_4$, if not then the session is rejected else U_i is authenticated to GWN. And computes $U_{SK}' = M_5 \oplus h(M_1') \oplus C_i'$, $MID_i = h(h(ID_i') \parallel T_1)$. Then compute the required message for SN_j as $M_6 = MID_i \oplus h(h(SID_j' \parallel K_{GWN}) \parallel T_3)$ and chooses a nonce $G_{SK} \in Z_n^*$ and compute $M_7 = G_{SK} \oplus MID_i, M_8 = G_{SK} \oplus U_{SK}', M_9 = h(G_{SK} \| U_{SK}' \| h(SID_j' \parallel K_{GWN}) \| MID_i \parallel T_3)$. At last, GWN transmits the communication $\{M_6, M_7, M_8, M_9, T_3\}$ 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 $(T_4 - T_3) \leq \triangle T$ is in allowed interval or not. If not then the session is rejected by SN_j else computes $M_6' = M_6 \oplus h(K_{GWN-S} \parallel T_3) = MID_i, G_{SK}' = M_7 \oplus MID_i = G_{SK}, U_{SK}' = M_8 \oplus G_{SK}' = G_{SK} \oplus U_{SK}' \oplus G_{SK}' = U_{SK}, M_9' = h(G_{SK}' \| U_{SK}' \| K_{GWN-S} \| MID_i \| T_3)$ and checks $M_9' \stackrel{?}{=} M_9$, if not session is terminated by SN_j. Otherwise SN_j choose a nonce $S_{SK} \in Z_n^*$ and evaluates the session key as $SK_j = h\left(MID_i \| SID_j \| U_{SK}' \| G_{SK}' \| S_{SK}\right), M_{10} = S_{SK} \oplus h(G_{SK}' \parallel K_{GWN-S})$, $M_{11} = h(G_{SK}' \| S_{SK} \| U_{SK}' \| MID_i \| T_5)$. At the last, SN_j sends response $\{M_{10}, M_{11}, T_5\}$ to GWN via the public channel.

Step 3: Presume that GWN receives the message as $\{M_{10}, M_{11}, T_5\}$ at T_6 and checks if $(T_6 - T_5) \leq \triangle T$ is in an acceptable interval or not. If not then the session is rejected otherwise GWN computes and retrieves $S_{SK}' = M_{10} \oplus h\left(G_{SK} \parallel h\left(SID_j' \parallel K_{GWN}\right)\right) = S_{SK}$, $M_{11}' = h(G_{SK} \| S_{SK}' \| U_{SK}' \| MID_i \| T_5)$ and checks $M_{11}' \stackrel{?}{=} M_{11}$, if not the session is rejected by the GWN. Otherwise, GWN computes the session key as $SK_g = h\left(MID_i \| SID_j' \| U_{SK}' \| G_{SK} \| S_{SK}'\right), M_{12} = G_{SK} \oplus M_1', M_{13} = S_{SK}' \oplus MID_i$, $M_{14} = h(G_{SK} \| S_{SK}' \| U_{SK}' \| MID_i \| T_7)$. 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 $(T_8 - T_7) \leq \triangle T$ is in an acceptable interval or not. If not, session is terminated else U_i computes and retrieves $G_{SK}' = M_{12} \oplus M_1 = G_{SK} \oplus xrP \oplus xrP = G_{SK}, S_{SK}' = M_{13} \oplus MID_i$. Computes session key $SK_i = h\left(MID_i \| SID_j \| U_{SK} \| G_{SK}' \| S_{SK}'\right), M_{14}' = h(G_{SK}' \| S_{SK}' \| U_{SK} \| MID_i \| T_7)$. Checks $M_{14}' \stackrel{?}{=} M_{14}$, if it is 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 $a_i' = V_i \oplus F_i' = a_i, RPW_i' = h(a_i' \| PW_i)$, and $A_i' = h(RPW_i' \| ID_i \| F_i')$. Verifies $A_i' \stackrel{?}{=} A_i$ if the unequal session is rejected otherwise legitimacy of U_i is ensured, thus permission for password update PW_{new} is granted.

Step 2: Now, SC_i computes $RPW_{\text{new}} = h(PW_{\text{new}} \parallel a_i'), A_{\text{new}} = h(ID_i \| RPW_{\text{new}} \| F_i')$ 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:

Step 1: To ensure the security as per BAN logic our proposed approach entails fulfilling some authentication goals such as:

Goal 1: $GWN \mid\equiv U_i \stackrel{\text{SK}}{\leftrightarrow} GWN$

Goal 2: $GWN \mid\equiv U_i \mid\equiv U_i \stackrel{\text{SK}}{\leftrightarrow} GWN$

Goal 3: $SN_j \mid\equiv GWN \stackrel{SK}{\leftrightarrow} SN_j$

Goal 4: $SN_j \mid\equiv GWN \mid\equiv GWN \stackrel{SK}{\leftrightarrow} SN_j$

Goal 5: $GWN \mid\equiv SN_j \stackrel{SK}{\leftrightarrow} GWN$

Goal 6: $GWN \mid\equiv SN_j \mid\equiv SN_j \stackrel{SK}{\leftrightarrow} GWN$

Goal 7: $U_i \mid\equiv GWN \stackrel{SK}{\leftrightarrow} U_i$

Goal 8: $U_i \mid\equiv GWN \mid\equiv GWN \stackrel{SK}{\leftrightarrow} U_i$

Step 2: Conversion of communication messages into Idealized form:

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

$M_0: < r >_P, M_2: < ID_i >_{rX}$,

$M_3: < SID_j > h(h(ID_i \parallel K_{GWN}) \parallel rX)$,

$M_4: < SID_j > h(h(ID_i \parallel K_{GWN}), rX, T_1)$,

$M_5: < U_{SK} >_{h(ID_i \| K_{GWN})}, h(rX)$

$Msg2: GWN \to SN_j: \{M_6, M_7, M_8, M_9, T_3\}$

$M_6: < MID_i >_{h(K_{GWN-S}), T_3}$,

$M_7: < G_{SK} > MID_i$,

$M_8: < U_{SK}' > G_{SK}$,

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

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

$M_{10}: < S_{SK} >_{h(G_{SK}', K_{GWN-S})}$,

$M_{11}: h(G_{SK}', S_{SK}, U_{SK}', MID_i, T_5)$

Table 2: Login and authentication phase.

User (U_i)/Smartcard (SC_i)	Gateway Node (GWN)	Sensor Node (SN_j)
U_i inserts SC_i into specific gadget gives PW_i, ID_i, biometric b_i' on a special device and gets $F_i' = H(b_i)'$ SC evaluates $a_i' = V_i \oplus F_i' = a_i$, $RPW_i' = h(a_i' \Vert PW_i)$, $A_i' = h(RPW_i' \Vert ID_i \Vert F_i')$, check $A_i' \stackrel{?}{=} A_i$, if equal then computes $C_i = B_i \oplus h(RPW_i' \Vert F_i') = h(ID_i \Vert K_{GWN})$ selects a nonce r and $U_{SK} \in Z_n^*$, computes $M_0 = rP$, $M_1 = rX$, $M_2 = ID_i \oplus M_1$, $M_3 = SID_j \oplus h(C_i \Vert M_1)$, $M_4 = h(C_i \Vert SID_j \Vert M_1 \Vert T_1)$, $M_5 = U_{SK} \oplus h(M_1) \oplus C_i$.		
send login request $\xrightarrow[\text{public channel}]{\{M_0, M_2, M_3, M_4, M_5, T_1\}}$	If $(T_2 - T_1) \le \Delta T$ is acceptable then $M_1' = xM_0 = xrP$, $ID_i' = M_2 \oplus M_1'$, $C_i' = h(ID_i' \Vert K_{GWN})$, $SID_j' = M_3 \oplus h(C_i' \Vert M_1')$, $M_4' = h(C_i' \Vert SID_j' \Vert M_1' \Vert T_1)$ and checks $M_4' \stackrel{?}{=} M_4$ if equal then computes $U_{SK}' = M_5 \oplus h(M_1') \oplus C_i'$, $MID_i = h(h(ID_i') \Vert T_1)$, $M_6 = MID_i \oplus h(h(SID_j' \Vert K_{GWN}) \Vert T_3)$, chooses a nonce G_{SK}, $M_7 = G_{SK} \oplus MID_i$, $M_8 = G_{SK} \oplus U_{SK}'$, $M_9 = h(G_{SK} \Vert U_{SK}' \Vert h(SID_j' \Vert K_{GWN}) \Vert MID_i \Vert T_3)$	
	sends the message $\xrightarrow[\text{public channel}]{\{M_6, M_7, M_8, M_9, T_3\}}$	If $(T_4 - T_3) \le \Delta T$ is acceptable then computes $M_6' = M_6 \oplus h(K_{GWN-S} \Vert T_3) = MID_i$, $G_{SK}' = M_7 \oplus MID_i$, $U_{SK}' = M_8 \oplus G_{SK}'$, $M_9' = h(G_{SK}' \Vert U_{SK}' \Vert K_{GWN-S} \Vert MID_i \Vert T_3)$, checks $M_9' \stackrel{?}{=} M_9$ if equal then choose a nonce S_{SK} $SK_j = h(MID_i \Vert SID_j \Vert U_{SK}' \Vert G_{SK}' \Vert S_{SK})$, $M_{10} = S_{SK} \oplus h(G_{SK}' \Vert K_{GWN-S})$, $M_{11} = h(G_{SK}' \Vert S_{SK} \Vert U_{SK}' \Vert MID_i \Vert T_5)$,
	If $(T_6 - T_5) \le \Delta T$ is acceptable then $\xleftarrow[\text{public channel}]{\{M_{10}, M_{11}, T_5\}}$ retrieves $S_{SK}' = M_{10} \oplus h(G_{SK} \Vert h(SID_j' \Vert K_{GWN}))$, $M_{11}' = h(G_{SK} \Vert S_{SK}' \Vert U_{SK}' \Vert MID_i \Vert T_5)$, checks $M_{11}' \stackrel{?}{=} M_{11}$, if equal then computes $SK_g = h(MID_i \Vert SID_j' \Vert U_{SK}' \Vert G_{SK} \Vert S_{SK}')$, $M_{12} = G_{SK} \oplus M_1'$, $M_{13} = S_{SK}' \oplus MID_i$, $M_{14} = h(G_{SK} \Vert S_{SK}' \Vert U_{SK}' \Vert MID_i \Vert T_7)$	sends the response
Checks if $(T_8 - T_7) \le \Delta T$ acceptable then $G_{SK}' = M_{12} \oplus M_1$, $S_{SK}' = M_{13} \oplus MID_i$, $SK_i = h(MID_i \Vert SID_j \Vert U_{SK} \Vert G_{SK}' \Vert S_{SK}')$, $M_{14}' = h(G_{SK}' \Vert S_{SK}' \Vert U_{SK} \Vert MID_i \Vert T_7)$, checks $M_{14}' \stackrel{?}{=} M_{14}$, if true then only mutual authentication holds i.e., $SK_i = SK_g = SK_j$	$\xleftarrow[\text{public channel}]{\{M_{12}, M_{13}, M_{14}, T_7\}}$ sends the message	

$Msg4: GWN \to U_i: \{M_{12}, M_{13}, M_{14}, T_7\}$

$M_{12}: < G_{SK} > rX, M_{13}: < S_{SK}' > MID_i,$

$M_{14}: h(G_{SK}, S_{SK}', U_{SK}', MID_i, T_7),$

Step 3: Further, certain assumptions to validate the reliability of the proposed system include:

$A1: U_i \mid\equiv \sharp\{U_{SK}, r, T_1, T_7\}$

$A2: GWN \mid\equiv \sharp\{U_{SK}, G_{SK}, T_1, T_3, T_5, T_7\}$

$A3: SN_j \mid\equiv \sharp\{U_{SK}, G_{SK}, S_{SK}, T_3, T_5\}$

$A4: U_i \mid\equiv U_i \stackrel{\{X, P, SID_j, h(K_{GWN} \Vert ID_i)\}}{\longrightarrow} GWN$

$A5: GWN \mid\equiv GWN \stackrel{K_{GWN-S}}{\longleftrightarrow} SN_j$

$A6: SN_j \mid\equiv SN_j \stackrel{K_{GWN-S}}{\longleftrightarrow} GWN$

$A7: GWN \mid\equiv GWN \stackrel{\{rX, SID_j, h(K_{GWN} \Vert ID_i)\}}{\longleftrightarrow} U_i$

$A8: GWN \mid\equiv U_i \Rightarrow h(ID_i \Vert K_{GWN})$

$A9: SN_j \mid\equiv GWN \Rightarrow K_{GWN-S}$

$A10: GWN \mid\equiv SN_j \Rightarrow K_{GWN-S}$

$A11: U_i \mid\equiv GWN \Rightarrow h(ID_i \Vert K_{GWN})$

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:

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

$M_0: < r >_P, M_2: < ID_i >_{rX},$

$M_3: < SID_j > h(h(ID_i \Vert K_{GWN}) \Vert rX),$

$M_4: < SID_j >_{h(h(ID_i \Vert K_{GWN}), rX, T_1)},$

$M_5: < U_{SK} >_{h(ID_i \Vert K_{GWN}), h(rX)}$

By seeing Msg1, we get

S1: $GWN \triangleleft < r >_P, < ID_i >_{rX}, < SID_j >_{a^*}, < SID_j >_{b^*},$
$< U_{SK} >_{h(ID_i \Vert K_{GWN}), h(rX)}, T_1$

where $a^* = h(h(ID_i \Vert K_{GWN}) \Vert rX), b^* = h(h(ID_i \Vert K_{GWN}), rX, T_1)$

Based on the principle of message meaning, S1 and A4, we procure

S2: $GWN \mid\equiv U_i \mid\sim U_{SK}$

According to nonce verification rule, freshness conjucatenation, A2 and S2, we procure:

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

According to jurisdiction rule, S3 and A8, we procure

S4: $GWN \mid\equiv U_{SK}$

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

S5: $GWN \mid\equiv U_i \overset{SK}{\leftrightarrow} GWN$

Goal 1 is achieved

As per S5, A2 and nonce verification rule we procure

S6: $GWN| \equiv U_i| \equiv U_i \overset{SK}{\leftrightarrow} GWN$

Goal 2 is achieved

According to the idealized form of Msg2:

Msg2: $GWN \rightarrow SN_j: \{M_6, M_7, M_8, M_9, T_3\}$

where $M_6: \langle MID_i >_{h(K_{GWN-S}), T_3}$,

$M_7: < G_{SK} > MID_i, M_8: < U'_{SK} > G_{SK}$,

$M_9: h(G_{SK}, U'_{SK}, K_{GWN-S}, MID_i, T_3)$

By seeing Msg2, we get

S7: $SN_j \triangleleft < MID_i > h(K_{GWN-S}), T_3, < G_{SK} > MID_i, < U'_{SK} > G_{SK}, h(c^*), T_3$

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 conjucatenation rules, we get

S9: $SN_j| \equiv GWN| \equiv G_{SK}$, here G_{SK} is the required component for the

proposed scheme's session key.

As per S9, A9 and jurisdiction rules, we procure

S10: $SN_j \mid\equiv G_{SK}$

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

S11: $SN_j \mid\equiv GWN \overset{SK}{\leftrightarrow} SN_j$

Goal 3 is achieved

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

S12: $SN_j| \equiv GWN| \equiv GWN \overset{SK}{\leftrightarrow} SN_j$

Goal 4 is achieved

According to the idealized form of Msg3:

Msg3: $SN_j \rightarrow GWN: \left\{M_{10}: < S_{SK} >_{h(G'_{SK}, K_{GWN-S})}, M_{11}: h(e^*), T_5\right\}$

where $e^* = G'_{SK}, S_{SK}, U'_{SK}, MID_i, T_5$

By seeing Msg3, we get

S13: $GWN \triangleleft < S_{SK} >_{h(G'_{SK}, K_{GWN-S})}, h(G'_{SK}, S_{SK}, U'_{SK}, MID_i, T_5), T_5$

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

S14: $GWN| \equiv SN_j| \sim S_{SK}$

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

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

From jurisdiction rule, S15 and A10, we get

S16: $GWN \mid\equiv S_{SK}$

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

S17: $GWN \mid\equiv SN_j \overset{SK}{\longrightarrow} GWN$

Goal 5 is achieved

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

S18: $GWN| \equiv SN_j| \equiv SN_j \overset{SK}{\leftrightarrow} GWN$

Goal 6 is achieved

According to the idealized form of Msg4:

Msg4: $GWN \rightarrow U_i: M_{12}: < G_{SK} > rX, M_{13}: < S'_{SK} > MID_i, M_{14}: h(f^*), T_7$

where $f^* = G_{SK}, S'_{SK}, U'_{SK}, MID_i, T_7$

By seeing Msg4, we get

S19: $U_i \triangleleft < G_{SK} > rX, < S'_{SK} > MID_i, h(G_{SK}, S'_{SK}, U'_{SK}, MID_i, T_7), T_7$

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 conjucatenation rules, we get

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

From S21, A11 and jurisdiction rule, we procure

S22: $U_i \mid\equiv G_{SK}$

As per session key rules, A1 and S21 we procure

S23: $U_i \mid\equiv GWN \overset{SK}{\leftrightarrow} U_i$

Goal 7 is achieved

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

S24: $U_i| \equiv GWN| \equiv GWN \overset{SK}{\leftrightarrow} U_i$

Goal 8 is achieved

Hence, mutual authentication as well as the session key $SK_i = SK_j = SK_g$ 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

$GWN\{M_{10}, M_{11}, T_5\}$. When the above sensor node SN_j gets captured by $\hat{A}$, all the above parameters stored in its memory are disclosed to $\hat{A}$. But this does not hamper the security of the system as the personel data and messages in the proposed scheme are in encrypted form like $MID_i = h(h(ID_i) \parallel T_1)$, session key, M_{11} etc. which is possible due to the involvement of time stamp and nonce. Therefore, $\hat{A}$ is unable to disclose the secret parameters of other legitimate users and protects the system even though the sensor node gets captured.

Session key leak attack

When an attacker $\hat{A}$ successfully retrieve the necessary data required for the computation of the session key then $\hat{A}$ is capable of breaching system security. Now if U_i wish to gain access to another sensor node SN_k so he has to transmit the message $\{M_0, M_2, M_3, M_4, M_5, T_{1\text{ new}}\}$ to GWN via a public channel from where $\hat{A}$ can get these message values. Here, $M_0 = rP, M_2 = ID_i \oplus M_1, M_3 = SID_k \oplus h(C_i \parallel M_1), M_4 = h(C_i \| SID_k \| M_1 \| T_{1\text{ new}})$. GWN sends the message $\{M_6, M_7, M_8, M_9, T_3\}$ to SN_k via public channels. $M_6 = MID_i' \oplus h(h(SID_k \parallel K_{GWN}) \parallel T_3), M_7 = G_{SK} \oplus MID_i', M_8 = G_{SK} \oplus U_{SK}$, $M_9 = h(G_{SK} \| U_{SK} \| h(SID_k \parallel K_{GWN}) \| MID_i' \| T_3)$. From previous data $\hat{A}$ knows $MID_i = h(h(ID_i) \parallel T1)$ and a nonce U_{SK} of legal user U_i (through the captured sensor node's stored data) but due to the involvement of a timestamp $T_3, T_{1\text{ new}}$ in M_4, M_6, M_7, M_9 is infeasible to disclose any parameters to evaluate the session key of the uncaptured sensor node $SN_k . SK_k = h(MID_i' \| SID_k \| U_{SK} \| G_{SK} \| S_{SK})$, thus we deduce that the proposed approach resists session key leak attacks.

Resists sensor node impersonation attack

In the authentication phase, GWN sends $\{M_6, M_7, M_8, M_9, T_3\}$ to SN_k i.e, SID_k through public channels. $\hat{A}$ impersonating as SID_k receives the messages, but since the proposed scheme resists session key leak attacks for SID_k so $\hat{A}$ finds it impossible to retrieve any values to send a response $\{M_{10}, M_{11}, T_5\}$ to GWN.

Where, $M_{10} = S_{SK} \oplus h(G_{SK}' \parallel K_{GWN-S}), M_{11} = h(G_{SK}' \| S_{SK} \| U_{SK}' \| MID_i \| T_5)$. 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_t and GWN, based on some disclosed secret data from previous attacks. In the proposed scheme, as per the sensor node capture attack (Ahlawat and Bathla, 2023), only U_i's and SN_j's data are known to $\hat{A}$ and fails to retrieve other legal users' and sensor node's data. Here to access sensor node $SN_t, \hat{A}$ tries to impersonate as U_a to GWN and SN_t (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 $M_0 = rP$ and $M_1 = rX$. 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 $M_3 = SID_t \oplus h(C_a \parallel M_1)$, $M_4 = h(C_a \| SID_t \| M_1 \parallel T_1)$ and $M_5 = U_{SK} \oplus h(M_1) \oplus C_a$. 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 (Ahlawatand 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 $M_4 = h(C_i \| SID_j \| M_1 \| T_1)$, $M_7 = G_{SK} \oplus MID_i$, $M_9 = h(G_{SK} \| U_{SK}' \| h(SID_j' \parallel K_{GWN}) \| MID_i \parallel T_3)$, $M_{11} = (G_{SK}' \| S_{SK} \| U_{SK}' \| MID_i \| T_5)$ and $M_{14} = h(G_{SK} \| S_{SK}' \| U_{SK}' \| MID_i \| T_7)$ 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 $\{A_i, B_i, \mathrm{h}(.), \mathrm{H}(.), \mathrm{X}, \mathrm{P}, V_i\}$ where, $A_i = h(ID_i \| F_i \| RPW_i), B_i = h(ID_i \parallel K_{GWN}) \oplus h(RPW_i \parallel F_i)$, X = xP is a public key of GWN, P is the generator point on an elliptic curve and $V_i = a_i \oplus F_i$. 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 $M_4 = h(C_i \| SID_j \| M_1 \parallel T_1)$ 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 $V_i \oplus F_i' = a_i \oplus F_i \oplus F_i' = a_i, RPW_i' = h(a_i' \parallel PW_i), A_i' = h(RPW_i' \| ID_i \| F_i')$ and check $A_i' \stackrel{?}{=} A_i$, 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_5} 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 $SK_i = h(MID_i \| SID_j \| U_{SK} \| G_{SK}' \| S_{SK}')$ is evaluated by the user, GWN and the sensor node using the nonce U_{SK}, $G_{SK}$and S_{SK} respectively and unidentified SID_j and ID_i . Suppose an adversary can disclose SID_j. But it's impossible to evaluate the session key without knowing $MID_i = h(h(ID_i) \parallel T_1)$ 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, 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).

```
role user (Ui, SNj, GWN : agent,
SK1 : symmetric_key ,
SK2 : symmetric_key ,
Xor,Mul,H,H1:hash_func,
Snd, Rcv : channel (dy))
played_by Ui
def=
local State:nat,
SIDj, KGWNS, RPWi,B1, Fi,
F1i,Ai,Ci,Bi,X1,Aii,Bii,Cii,X,P,Vi,A1,USK,GSK,SSK,PWi,IDi,R,B21,MIDi,
M19,SKj,UiSK,RPWii,GiSK,RPW1i,B1i,SiSK,SK,Mi14,KGWN,IDiiV,SIDij,
Mi4,Mi1,Mi11,SKGWN,Ti1,Uisk,Mi6,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,user_snode_usk,
snode_gway_ssk,gway_snode_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}_SK1 )
/\secret( {PWi,A1,B1},subs1,Ui)
/\secret ({RPWi,Fi},subs2,{Ui,GWN})
2.State=1/\Rcv({Ai.Bi.X.P}_SK1) =|>
% Receives smart card information from GWN
State':=2/\R':=new()
/\Vi':=Xor(A1,Fi)
/\B21':=Xor(Vi,Fi)
/\RPW1i':=H(PWi.A1 )
/\Aii':=H(IDi.RPW1i.Fi)
/\Ci':=Xor(Bi,H(RPW1i.Fi))
/\T1':=new()
/\USK':=new()
/\M0':=Mul(R,P)
/\M1':=Mul(R,X)
/\M2':=Xor(IDi,M1)
/\M3':=Xor(SIDj,H(Ci.M1))
/\M4':=H(Ci.SIDj.M1.T1)
/\M5':=Xor(USK,H(M1),Ci)
/\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/\GiSK':=Xor(M12,M1)
/\SiSK':=Xor(M13,MIDi)
/\SK':=H(MIDi.SIDj.USK.GiSK.SiSK)
/\Mi14':=H(GiSK.SiSK.USK.MIDi.T7)
/\request(GWN,Ui,gway_user_gsk,GSK)
/\request(SNj,Ui,snode_user_ssk,SSK)
end role
```

Figure 2. HLPSL code for user

```
role gway (Ui,GWN,SNj:agent,
SK1:symmetric_key,
SK2:symmetric_key,
Xor,Mul,H,H1:hash_func,
Snd,Rcv:channel(dy))
played_by GWN
def=
local State:nat,
SIDj,KGWNS,RPWi,B1,Fi,F1i,Ai,Bi,X1,Aii,Ci,Cii,X,P,Vi,A1,USK,GSK,SSK,
PWi,IDi,R,B21,MIDi,M19,SKj,UiSK,RPWii,RPW1i,B1i,SiSK,SK,Mi14,
KGWN,IDiiV,SIDij,Mi4,Mi1,Mi11,SKGWN,Ti1,Uisk,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,user_snode_usk,
snode_gway_ssk,gway_snode_gsk,
subs1,subs2,subs3,subs4,subs5,subs6:protocol_id
init State:=0
transition
1.State=0/\Rcv({IDi.RPWi.Fi}_SK1)=|>
%Receives registration request message from user
State':=1/\Ai':=H(IDi.RPWi.Fi)
/\Bi':=Xor(H(IDi.KGWN),H(RPWi.Fi))
/\Snd({Ai'.Bi'.X'.P'}_SK1)
%Send smart card information securely
/\secret({KGWN},subs4,GWN)
2.State=1/\Rcv(M0.M2.M3.M4.M5.T1)=|>
%Receives login request message from user
State':=2/\GSK':=new()
/\Mi1':=Mul(X1,M0)
/\IDiiV':=Xor(M2,Mi1)
/\Cii':=H(IDiiV.KGWN)
/\SIDij':=Xor(M3,H(Ci.M1))
/\Mi4':=H(Cii.SIDij.Mi1.Ti1)
/\UiSK':=Xor(M5,H(Mi1),Cii)
/\MIDi':=H(H(IDi).T1)
/\T3':=new()
/\M6':=Xor(MIDi,H(H(SIDj.KGWN).T3))
/\M7':=Xor(GSK,MIDi)
/\M8':=Xor(GSK,USK)
/\M9':=H(GSK.USK.T3.H(SIDj.KGWN).MIDi)
/\Snd(M6'.M7'.M8'.M9'.T3')
%Send message to the sensor node
/\secret({GSK},subs5,{GWN,SNj,Ui})
3.State=2/\Rcv(M10.M11.T5)=|>
State':=3/\T7':=new()
/\SiSK':=Xor(M10,H(GSK.H(SIDj.KGWN)))
/\Mi11':=H(GSK.SSK.USK.MIDi.T5)
/\SKGWN':=H(MIDi.SIDj.USK.GSK.SSK)
/\M12':=Xor(GSK,M1)
/\M13':=Xor(SSK,MIDi)
/\M14':=H(GSK.SSK.USK.MIDi.T7')
/\Snd(M12'.M13'.M14'.T7')
% Send message to the user
/\request(Ui,GWN,user_gway_usk,USK)
/\request(SNj,GWN,snode_gway_ssk,SSK)
/\witness(GWN,Ui,gway_user_gsk,GSK)
end role
```

Figure 3. HLPSL code for gateway node

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.

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

```
role sensor(Ui,GWN,SNj:agent,
SK1:symmetric_key ,
SK2:symmetric_key,
Xor,Mul,H,H1:hash_func,
Snd,Rcv:channel(dy))
played_by SNj
def=
local State:nat,
SIDj,KGWNS,RPWi,B1,B2,Ai,Bi,X,X1,P,Vi,F1i,Cii,Fi,Ci,Aii,Bii,Biii,SIDi,A1,
USK,GSK,SSK,PWi,IDi,R,B21,MIDi,M19,SKj,UiSK,RPWii,RPW1i,B1i,SiSK,
SK,Mi14,KGWN,IDiiV,SIDij,Mi4,Mi1,Mi11,SKGWN,Ti1,Uisk,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,user_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.SSK.USK.MIDi.T5)
/\Snd(M10'.M11'.T5')
/\secret({SSK},subs6,{GWN,SNj,Ui})
%/\request(Ui , SNj, user_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.

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL
PROTOCOL
/home/preeti/Downloads/span-1.6-linux64-ubuntu/span//testsuite/results/khushboo2.if
GOAL
As specified
BACKEND
CL-AtSe
STATISTICS
Analysed  : 0 state
Reachable  : 0 state
Translation: 0.21 seconds
Computation: 0.00 seconds
```

Figure 5(a). Simulation output in CL-AtSe back-end.

```
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/preeti/Downloads/span-1.6-linux64-ubuntu/span//testsuite/results/khushboo2.if
GOAL  as specified
BACKEND  OFMC
STATISTICS
TIME 362 ms
parseTime 0 ms
visitedNodes: 29 nodes
depth: 4 plies
```

Figure 5(b). Simulation output in OFMC back-end.

Table 3. Comparison of functional features and security.

Security Properties	Liu et al. (2019)	Vinoth et al. (2020)	Far et al. (2021)	Wu et al. (2021)	Saqib et al. (2022)	Wang et al. (2023)	Proposed Scheme
SP1	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SP2	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SP3	No	No	No	No	Yes	Yes	Yes
SP4	Yes	Yes	Yes	No	Yes	Yes	Yes
SP5	Yes	Yes	Yes	Yes	No	No	Yes
SP6	Yes	No	No	Yes	No	No	Yes
SP7	Yes	No	Yes	Yes	Yes	Yes	Yes
SP8	Yes	Yes	Yes	Yes	Yes	No	Yes
SP9	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SP10	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SP11	Yes	No	Yes	Yes	Yes	Yes	Yes

Table 4. Computational and communication overhead comparison.

Schemes	Computation cost (in second)	Smart card storage (in bits)	Communication Cost (in bits)
Liuetal., 2019	$14T_H+12T_{EC}\approx 0.764$	1248	2880
Vinothetal., 2020	$19T_H+1T_{EC}\approx 0.730$	2048	3040
Faretal., 2021	$24T_H+4T_{EC}\approx 0.264$	2400	2216
Wuetal., 2021	$27T_H+7T_{EC}\approx 0.455$	2048	1824
Saqibetal., 2022	$9T_H+10T_{EC}\approx 0.635$	N/A	2720
Wangetal., 2023	$10T_H+10T_{EC}\approx 0.636$	640	3808
Saini et al., 2024	$36T_H+5T_{EC}\approx 0.395$	1152	2304
Huang, 2024	$48T_H+12T_{EC}\approx 0.781$	1120	3650
Proposed scheme	$27T_H+3T_{EC}\approx 0.202$	1440	2880

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.

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

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

Ahlawat, P., & Bathla, R. (2023). A multi objective optimization modeling in WSN for enhancing the attacking efficiency of node capture attack. *International Journal of System Assurance Engineering and Management*, *14*(6), 2187–2207. https://doi.org/10.1007/s13198-023-02048-2

Alghamdi, A., Shahrani, A. M. A., AlYami, S. S., Khan, I. R., Sri, P. S. G. A., Dutta, P., Rizwan, A., & Venkatareddy, P. (2023). Security and energy efficient cyber-physical systems using predictive modeling approaches in wireless sensor network. *Wireless Networks*. https://doi.org/10.1007/s11276-023-03345-1

Ali, R., Pal, A. K., Kumari, S., Sangaiah, A. K., Li, X., & Wu, F. (2018). An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring. *Journal of Ambient Intelligence & Humanized Computing/Journal of Ambient Intelligence and Humanized Computing*, *15*(1), 1165–1186. https://doi.org/10.1007/s12652-018-1015-9

Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuellar, J., Drielsma, P. H., Heám, P. C., Kouchnarenko, O., Mantovani, J., Mödersheim, S., Von Oheimb, D., Rusinowitch, M., Santiago, J., Turuani, M., Viganò, L., & Vigneron, L. (2005). The AVISPA tool for the automated validation of internet security protocols and applications. In *Lecture notes in Computer Science*, pp. 281–285. https://doi.org/10.1007/11513988_27

Chetry, A., & Sharma, U. (2023). Anonymity in decentralized apps: Study of implications for cybercrime investigations. *International Journal of Experimental Research and Review*, *32*, 195–205. https://doi.org/10.52756/ijerr.2023.v32.017

Cho, Y., Oh, J., Kwon, D., Son, S., Yu, S., Park, Y., & Park, Y. (2022). A secure Three-Factor authentication protocol for E-Governance system based on multiserver environments. *IEEE Access*, *10*, 74351–74365. https://doi.org/10.1109/access.2022.3191419

Das, A. K., Kumari, S., Odelu, V., Li, X., Wu, F., & Huang, X. (2016). Provably secure user authentication and key agreement scheme for wireless sensor networks. *Security and Communication Networks*, *9*(16), 3670–3687. https://doi.org/10.1002/sec.1573

Dawn, N., Ghosh, T., Ghosh, S., Saha, A., Mukherjee, P., Sarkar, S., Guha, S., & Sanyal, T. (2023). Implementation of Artificial Intelligence, Machine Learning, and Internet of Things (IoT) in revolutionizing Agriculture: A review on recent trends and challenges. *Int. J. Exp. Res. Rev.*, *30*, 190-218. https://doi.org/10.52756/ijerr.2023.v30.018

Far, H. a. N., Bayat, M., Das, A. K., Fotouhi, M., Pournaghi, S. M., & Doostari, M. A. (2021). LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-based IIoT. *Wireless Networks*, *27*(2), 1389–1412. https://doi.org/10.1007/s11276-020-02523-9

Hemalatha, T., Bhuvaneswari, A., Poornima, N., Shubha, B., Santhi, K., Lawanyashri, M., & Mara, G. C. (2023). Secure and private data sharing in CPS e-health systems based on CB-SMO techniques. *Measurement. Sensors*, *27*, 100787. https://doi.org/10.1016/j.measen.2023.100787

Huang, W. (2024). ECC-based three-factor authentication and key agreement scheme for wireless sensor networks. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-52134-z

Jain, N., Awasthi, Y., & Jain, R. (2023). An IoT-based soil analysis system using optical sensors and multivariate regression. *Int. J. Exp. Res. Rev.*, 31(Spl Volume), 23-32. https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.003

Jha, K., Jain, A., & Srivastava, S. (2023a). An Efficient Speaker Identification Approach for Biometric Access Control System. *In:2023 5th International Conference on Recent Advances in Information Technology (RAIT), IEEE*, pp. 1-5. https://doi.org/10.1109/RAIT57693.2023.10127101

Jha, K., Jain, A., & Srivastava, S. (2024a). Analysis of Human Voice for Speaker Recognition: Concepts and Advancement. *Journal of Electrical Systems*, 20(1), 582-599. https://doi.org/10.52783/jes.806

Jha, K., Srivastava, S., & Jain, A. (2023b). Integrating Global and Local Features for Efficient Face Identification Using Deep CNN Classifier. *In:2023 International Conference on Device Intelligence, Computing and Communication Technologies, (DICCT), IEEE* pp. 532-536. https://doi.org/10.1109/DICCT56244.2023.10110170

Jha, K., Srivastava, S., & Jain, A. (2024b). Cryptanalysis of a Biometric based Anonymous Authentication Approach for IoT Environment. *International Journal of Microsystems and IoT*, 2(2), 591–597. https://doi.org/10.5281/zenodo.10804461

Jha, R., & Singh, M. K. (2024). Electric Mobility Adoption in India–Policy & Initiatives to Promote E-Mobility in Jharkhand. *International Management Review,* 20(1), 63-74.

Lekha, J., Sandhya, K., Archana, U., Anilkumar, C., Soman, S. J., & Satheesh, S. (2023). Secure medical sensor monitoring framework using novel optimal encryption algorithm driven by Internet of Things. *Measurement. Sensors*, *30*, 100929. https://doi.org/10.1016/j.measen.2023.100929

Liu, W., Wang, X., Peng, W., & Xing, Q. (2019). Center-Less single Sign-On with Privacy-Preserving remote Biometric-Based ID-MAKA scheme for mobile cloud computing services. *IEEE Access*, *7*, 137770–137783. https://doi.org/10.1109/access.2019.2942987

Mirsaraei, A. G., Barati, A., & Barati, H. (2022). A secure three-factor authentication scheme for IoT environments. *Journal of Parallel and Distributed Computing*, *169*, 87–105. https://doi.org/10.1016/j.jpdc.2022.06.011

Mondal, S., Nag, A., Barman, A. K., & Karmakar, M. (2023). Machine Learning-based maternal health risk prediction model for IoMT framework. *International Journal of Experimental Research and Review*, *32*, 145–159. https://doi.org/10.52756/ijerr.2023.v32.012

Nyangaresi, V. O. (2022). Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. *Journal of Systems Architecture*, *133*, 102763. https://doi.org/10.1016/j.sysarc.2022.102763

Pal, D., Funilkul, S., Charoenkitkarn, N., & Kanthamanon, P. (2018). Internet-of-Things and Smart Homes for Elderly Healthcare: An end user perspective. *IEEE Access*, *6*, 10483–10496. https://doi.org/10.1109/access.2018.2808472

Rai, A., Kundu, K., Dev, R., Keshari, J., & Gupta, D. (2023). Design and development Virtual Doctor Robot for contactless monitoring of patients during COVID-19. *Int. J. Exp. Res. Rev.*, 31(Spl Volume), 42-50. https://doi.org/10.52756/10.52756/ijerr.2023.v31spl.005

Saini, K. K., Kaur, D., Kumar, D., & Kumar, B. (2024). An efficient three-factor authentication protocol for wireless healthcare sensor networks. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-024-18114-1

Saqib, M., Jasra, B., & Moon, A. H. (2022). A lightweight three factor authentication framework for IoT based critical applications. *Journal of King Saud University. Computer and Information Sciences/Mağalaẗ Ğam'aẗ Al-malīk Saud: Ùlm Al-ḥasib Wa Al-ma'lumat*, *34*(9), 6925–6937. https://doi.org/10.1016/j.jksuci.2021.07.023

Sarkar, A., & Singh, B. (2019). A cancelable biometric based secure session key agreement protocol employing elliptic curve cryptography. *International Journal of System Assurance Engineering and Management*, *10*(5), 1023–1042. https://doi.org/10.1007/s13198-019-00832-7

Soni, P., Pal, A. K., & Khushboo, K. (2019a). A User Convenient Secure Authentication Scheme for Accessing e-Governance Services. *In: 2019 10th International Conference on Computing, Communication and Networking Technologies*

(ICCCNT), *IEEE*, pp.1-7. https://doi.org/10.1109/ICCCNT45670.2019.8944393

Soni, P., Pal, A. K., & Islam, S. H. (2019b). An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. *Computer methods and programs in biomedicine*, *182*, 105054. https://doi.org/10.1016/j.cmpb.2019.105054

Soni, P., Pal, A. K., Islam, S. H., Singh, A., & Kumar, P. (2021). Provably secure and biometric-based secure access of E-Governance services using mobile devices. *Journal of Information Security and Applications*, *63*, 103016. https://doi.org/10.1016/j.jisa.2021.103016

Vinoth, R., Deborah, L. J., Vijayakumar, P., & Kumar, N. (2021). Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT. *IEEE Internet of Things Journal*, *8*(5), 3801–3811. https://doi.org/10.1109/jiot.2020.3024703

Wang, Z., Deng, D., Hou, S., Guo, Y., & Li, S. (2023). Design of three-factor secure and efficient authentication and key-sharing protocol for IoT devices. *Computer Communications*, *203*, 1–14. https://doi.org/10.1016/j.comcom.2023.02.015

Wu, T., Yang, L., Lee, Z., Chen, C., Pan, J., & Islam, S. H. (2021). Improved ECC-Based Three-Factor Multiserver Authentication scheme. *Security and Communication Networks*, *2021*, 1–14. https://doi.org/10.1155/2021/6627956

How to cite this Article:

Khushboo Jha, Aruna Jain and Sumit Srivastava (2024). A Secure Biometric-Based User Authentication Scheme for Cyber-Physical Systems in Healthcare. *International Journal of Experimental Research and Review*, *39*(spl.) 154-169.

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