Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 3 (2024)

User Authentication and Communication Security in IOT Enabled Wireless Sensor Networks Using Biometric Verification

[1]N.V.S.S. Prabhakar, [2]Talari Surendra, [3]R. Hari kishore, [4]M. Manjusha, [5]Subrahmanya .S.Meduri, [6]Suryaprakash Nalluri,

[1]*Research Scholar, Department of Mathematics, GSS, GITAM Deemed to be University, Visakhapatnam - 45, Andhra Pradesh, India*

[2]*Department of Mathematics, GSS, GITAM Deemed to be University, Visakhapatnam - 45, Andhra Pradesh, India*

[3]*Department of Mathematics, Vasavi College of Engineering, Ibrahimbagh, Hyderabad, Telagana – 31, India*

[4]*Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India*

[5]*Technical Architect, Wipro Technologies, USA.*

[6] *Department - Information Security, Affiliation-University of Cumberland,Williamsburg, USA.*

Abstract:- In this study, we extend wireless sensor networks (WSNs) with biometric authentication to propose a novel self-verification authentication mechanism for securing Internet of Things (IoT) services. With regard to real-world applications in WSNs, communication security is a top priority. This system prevents user credentials from being lost, stolen, or used improperly, ensuring secure access to IoT sensor nodes. The proposed scheme employs biometric authentication for user verification, which improves communication security and provides users with a number of benefits. Along with user-friendly password/biometric change mechanisms, the scheme also supports dynamic node addition. Formal security techniques like ROR and analysis tools like AVISPA are used to examine the proposed mechanism’s security, showing that the scheme is secure even with a finite number of sessions. Additionally, the performance evaluation’s analytical findings show that the proposed scheme effectively implements authentication, information exchange, and other crucial security features.

Keywords: Authentication, Internet of Things, Random oracle model, AVISPA, Security and privacy

1. Introduction

Internet of Things (IoT) is a smart-devices-based technology. Parallel to the WSNs ran the development of the notion of IoT. In a framework that seems “internet-like”, Kevin Ashton developed the phrase “Internet of Things” which indicates the unique items and their virtual activity [1]. This includes home equipment, smart phones, sensing and other networking devices that can transform the scope of the sector. Wireless communication technologies will be of great importance even if IoT does not imply special communication technologies and WSNs will in particular multiply applications and sectors. The IoT will cost reasonably with a compact, robust, cheap and low-power WSN node even for the tiniest items put in any sort of environment. Integrating these objects into the IoT is an important WSN development. In the era of getting things done with less computing resources, the connected devices need to utilize the limited bandwidth and provide 24/7 connectivity to the applications which ranges from supply-chain across all industries to space. According to IDC (International Data Corporation) forecast, comparing to previous years records, in year 2019, the studies reveal that nearly 15.4% $745 billion were spent worldwide in the connectivity domain. By the end of 2020-2022, it is expected that $1 trillion mark of global spending will be crossed. This advantage helps IoT to be deployed in many application domains which includes smart cities[2], smart homes (lighting control, security, and AC control)[3, 4], healthcare, and smart manufacturing (controlling manufacturing systems and monitoring and operating the industrial things)[5, 6]. As IoT spans and can be utilized in such a wide variety of application domains, its deployment requires heterogeneous network connectivity [7]. The communicators can foresee attentive data authorisation in IoT-based fundamental applications. For access to such information the outsider(user) must be informed that the data is accessed directly from the net work IoT sensors. If both users and IoT sensors regularly check, an established sessionkey has to be set up. They can interact securely with each other using the Session Key [8]. In the last few years, among many studies one of the research topics attracted much more fanfare is the user authentication and key agreement schemes to ensure legitimacy of participants and security of WSNs. Basically, from the previous studies, we observed that the user authentication models are categorized into five different models [11] where the users can authenticate in the WSN, which provides a very good insight on the design guide for the proposal of a new user authentication and key agreement protocol. The authentication protocols can restrict the attackers in framing any network attacks, which includes replay attacks, Man-in-the-middle attack, impersonation attack, eavesdropping attack, and most important dictionary and password guessing attacks etc. The authentication protocols are necessary as they ensure mutual authentication and session key agreement while also restricting any attacker to gain advantage over the network say in the WSNs tailored for IoT.

2. Literature Review

Crucial research has been carried out in WSN-IoTs on user authentication and the agreement protocol to ensure that user may safely access information. In 2014, Turkanovic et al.[12] proposal is considered as the first IoT notion based research proposal in WSN, which discusses about IoT notion that can also be applicable in authentication and communication model in WSN. Turkanovic et al. [12] scheme adopts the 5 th model in WSN as per the discussion in [11]. The first IoT notion based development in relate to user authentication and key agreement scheme for IoT and WSN environment was proposed here by Turkanovic et al. [12]. However, the vulnerabilities of Turkanovic et al. [12] were brought out by Farash et al. [13] in 2016 which says, Turkanovic et al.'s scheme fails to resist offline password guessing and fails to achieve user anonymity. To address the issue, Farash et al. [13] proposed an improved authentication scheme which was tailored for IoT environment. As per their proposition the sensor nodes are capable members to propel the validation messages to the GWN, which isn't the preparation in WSN as the sensor nodes have restricted battery utilization power. Hence, the authors in [14, 15, 16] still accepts the gateway in WSN and IoT should play the main role in conveying and displaying the authentication and key agreement protocol. In addition to this a few schemes were presented in Table 1. The recent advancements and developments suggest using various authentication factors such as biometric factors in the designing the authentication schemes. As the physiological biometrics features such as fingerprints, facial, and iris information are specifically unique to each user, it is an added advantage which favors the user by implementing user authentication successfully. However, they usually require additional; often costly equipment. In this paper, we have considered smartphone instead of smartcard. The smartphones can be easily used by the user due to the enhanced features and advantages over smartcard. Our paper proposes authentication and key agreement scheme rather than designing an improved version to any existing schemes in IoT and WSN.

Table 1. Summary Of Cryptographic Techniques Applied And Limitations Of Previous Existing User Authentication Mechanisms

Scheme	Year	Cryptographic Techniques	Advantages	Drawbacks/Limitations
Wazid et al. [38]	2018	* Based on "three-factor (smart card, user password & biometrics)" Uses "one-way cryptographic hash function" * Based on "fuzzy extractor for biometric	* Fits for generic IoT networking environment	* Fails to preserve "revocability" * No "formal security" analysis.

		verification		
Li et al. [61]	2018	*Based on “three-factor (user mobile device, user password and personal biometrics” * Applies “ECC cryptographic technique” * Uses “fuzzy extractor for biometric verification	* Applicable in industrial IoT environment	* Does not support “revocability, and password/biometric update” * Vulnerable to “known session key attack”
Srinivas et al. [21]	2018	* Based on “two-factor (smart card and user password) * Based on Chinese Remainder Theorem (CRT)-based public key concept * Uses “one-way hash function”	* Applicable for “wearable healthcare monitoring system”	*Need more computation cost.
Kumar et al. [62]	2019	*Based on One-way Hash functions, XOR	* Applicable in coal mines for safety monitoring	* Does not support “revocability, and Vulnerable to Known session key attack”
Wang et al. [63]	2019	* Based on “three-factor authentication using Chebyshev chaotic map	* Applicable for Wireless Sensor Networks	*Vulnerable to “known session specific temporary information, user impersonation attacks”
Yu et al. [64]	2019	*Based on pairing-based cryptography *Designed for home-based multisensor Internet of Things	*Applicable for Multisensor IoT and Smart city	*Does not preserve “user anonymity”
Luo et al.[65]	2020	* Fuzzy Extractor *lightweight 3FA scheme which only used hash function	* Applicable for IoT applications	* Though secure against various attacks, no “formal security” analysis
Shuai et al. [66]	2020	*Rabin Cryptosystem	*Forward secrecy between industrial management gateway and industrial sensor nodes is provided	*Vulnerable to “known session specific temporary information, and needs high computation cost
Nashwan[67]	2020	*Hash functions, XOR	* Applicable for Big Data environment.	*Fails to provide “user anonymity” * No “formal security” analysis.
Chaudhry et al.[68]	2020	*Uses Elliptic Curve Cryptosystem	* Applicable for IoT based sensor cloud systems	* Needs more computation cost.
Chaudhry et	2020	*Uses Elliptic Curve	* Applicable for	*Though secure against

al.[69]		Cryptosystem	Industrial IoT environment	various attacks, its computation cost is high

3. Definitions and Mathematical Preliminaries

3.1. Biohashing

To maintain uniqueness and distinguish the users, biometric is widely considered due to its several advantages in comparison to the traditional authentication methods (i.e. password and smart card) which can also be helpful in verifying the legitimacy of the user. Differentiated and cryptographic keys and passwords, biometric keys have various inclinations. A couple of great conditions are portrayed as follows [15, 27, 28]:

- The biometric keys cannot be lost, stolen or captured;
- Copying or sharing the biometric keys is extremely difficult;
- Create/scatter the biometrics is hard;
- Guessing of biometric keys is hard;
- Breaking the biometric keys is extremely hard.

3.2. Network Model

In Figure. 1, the smart-sensing IoT tailored to WSNs monitoring system is illustrated. In this network model, a legitimate user can establish a secure connection with the IoT integrated sensor nodes via the GWN. The users send request to GWN for extracting the on-demand information from the sensing devices (IoT sensors). On successful authentication, users can benefit from accessing the demanded information. In this network model, the monitoring system is built to sense the data from the smart sensors which are deployed in the hostile network. These sensing devices are deployed in such a manner that the surveillance can happen time-to-time such that the scanning/monitoring of things can be done in real-time. Ensuring security of the on-demand real-time communication would be challenging due to the limited resources available in IoT sensing devices, and vulnerabilities include the physical capturing of the deployed devices. In such scenarios, a secure and efficient user authentication scheme comes handy, where the user's authenticity is validated so that the real-time data access from the smart sensing devices can be ensured only if the legitimacy is validated.

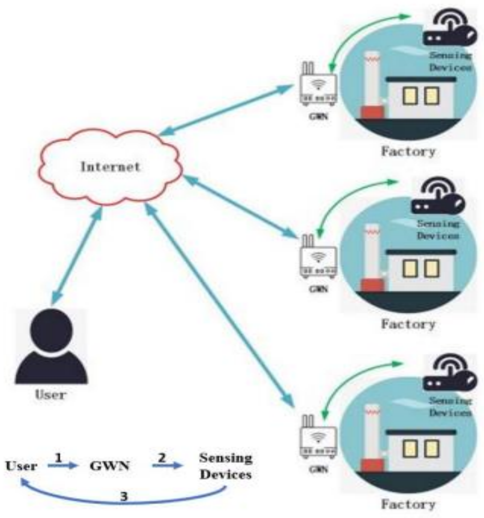

Figure 1: Network Model (Adopted from [39])

3.3. Threat Model

We explore a more realistic model of threat recently described in [26] for IoT security. The threatening Dolev-Yao (DY) model [33], fully understood by an adversary of $\mathcal{A}$, has complete monitoring of the correspondence channel in our authentication system. Thus, throughout communication, $\mathcal{A}$ can eavesdrop, alter, detruce and insert impersonation messages. In addition, end-point entities (IoT nodes and applicators) cannot generally be trusted. $\mathcal{A}$ is expected to get certain IoT smart devices (S D j). All the sensitive information in their memory is then eliminated. In addition, by use of power analysis assaults, the $\mathcal{A}$ can insulate delicate credentials from a user's lost cell phone [36].We also assume that the locking method will really assure the gateway nodes (GWN). This makes the physical capture of the GWN a lot problematic as compared to the fact that clever gadgets are genuinely captured [35].

At last, it is additionally a regular suspicion that the GWN is trusted node, and it won't be undermined by the adversary [38]. The GWN can therefore in the IoT environment, depending on applications, be set in an actual securing framework (e.g., smart home, healthcare and Industrial IoT). In the IoT context, GWN are regarded as trusted entities.

The following assumptions are also considered under this threat model so that what the attacker $\mathcal{A}$ can possibly sense the confidential information from the communicating parties or from the communicating network [36, 40]:

• $\mathcal{A}$ can extract the confidential user specific information from the user's smartphone by examining the power consumption or using the leaked information.

• The participants communicate over the insecure public channel which gives an advantage to $\mathcal{A}$ to eavesdrop the communication and learn to collect the communicated information.

• All the transmitted messages can be resent, redirect, modify or delete by $\mathcal{A}$ due to the publicly communication.

• $\mathcal{A}$ can be an insider or outsider in the system.

• Due to the low entropy nature of the password/identity, $\mathcal{A}$ can guess them. Moreover, it is observed that guessing of two secret parameters such as identity, password or biometric in polynomial time are computationally infeasible.

3.4. ROR-Model

The ROR model [42, 43] became famous while assessing the safety of several current literature authentication techniques [21, 37, 6]. Under this model, adversaries say that a has access to a set of executing entity queries including CorruptMDi(MD$_i$), Test($\mathcal{P}^t$), Test($\mathcal{P}^t$), Execute(MD$_i$,IoS_{sn_j}) and Reveal($\mathcal{P}^t$) required to simulate the real attack. The query descriptions of such queries are tabulated in a Table 2. The ROR model components are the following:

• **Participants.** The associated participants with the proposed scheme are the mobile device MD$_i$, gateway node GWN or a IoT sensor node IoS_{sn_j} . The instances t$_1$ and t$_s$ of MD$_i$ and $IoS_{sn_j}$are marked as $Ƥ^{t_1}_{MD_i}$ and $Ƥ^{t_2}_{IoS_{sn_j}}$ which are known as oracles.

• **Accepted state**. If the peer points achieve an accepted status when the final communication has been authenticated, the instance " $\mathcal{P}^t$ " comes under "accepted State'.' The For the ongoing session, sid is a $\mathcal{P}^t$ session ID created in a sequence by $\mathcal{P}$Pt after the sent and received messages were rearranged.

• **Partnering**. The following things must be accomplished to be partnered between $Ƥ^{t_1}$and $Ƥ^{t_2}$:

– They are in "accepted states".

– They possess the same sid. Further also "authenticate mutually with each other".

– They are also "mutual partners of each other".

• **Freshness**. as $\mathcal{P}^{t_1}_{MD_i}$ or $\mathcal{P}^{t_2}_{IoS_{sn_j}}$ is fresh when the constructed session key between MD_i and IoS_{sn_j} is not leaked to $\mathcal{A}$ using the Reveal(P t) query listed in Table 2.

The proposed scheme undergoes "semantic security" as defined in Definition 1.

Definition 1. Let $Adv_{\mathcal{A}}^{DAM-IoS_{sn_j}}$ (t_p) represent the ability of an adversary $\mathcal{A}$ to breach the semantic security of DAM − IoS_{sn_j} and extract the session key (SK_{ij}) between a mobile device MD_i and an IoT sensor node IoS_{sn_j} The adversary runs in polynomial time t_p. The advantage is calculated as $Adv_{\mathcal{A}}^{DAM-IoS_{sn_j}}$ (t_p) = |2Pr[c' = c] − 1|, where c represents the correct bits and c' represents the guessed bits.

Table 2. Various queries with their descriptions

Query	Significance
CorruptMD(MD_i)	$\mathcal{A}$ can extract the stored credentials by compromised mobile device MD_i's memory
Execute(MD_i , IoS_{sn_j})	This supports $\mathcal{A}$ in intercepting communications between MD_i and IoS_{sn_j}
Reveal($\mathcal{P}^t$)	This allows $\mathcal{A}$ to obtain the S K_{ij}(= S K_{ji}) session key from $\mathcal{P}^t$ and its partner
Test($\mathcal{P}^t$)	It allows $\mathcal{A}$ to request P t for the session key S K_{ij}(= S K_{ji}) and is probably a consequence of a flickered "unbiased coin c" $\mathcal{P}^t$ output

Furthermore, Definition 2 defines a "collision-resistant one-way hash function" h: 0,1 → $0,1^{l_b}$ that produces a fixed-length output string h(m) ∈ 0, 1^{l_b} on an arbitrary length input string m ∈ 0, 1. This definition is important for the security of DAM – IoS_{sn_j}. Definition 3 defines the "Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP)" which is relevant for the security of DAM − IoS_{sn_j}.

Definition 2. A function h : 0, 1 ∗ → 0, 1^{l_b} is considered to be a one-way collision-resistant hash function if it maps an input string m ∈ 0, 1^* of arbitrary length to a fixed-length output string of l_b bits, known as the hash value or message digest. An adversary $\mathcal{A}$ attempting to find a hash collision is said to have an advantage $Adv^{Hash}\mathcal{A}$ (t_h), which is given by Pr[(m_1, m_2) $\leftarrow_r$ $\mathcal{A}$: $m_1 \neq m_2$, , , h(m_1) = h(m_2)]. Here, Pr(X) represents the probability of the occurrence of a random event X, and (m_1, m_2) $\leftarrow_r$ $\mathcal{A}$ denotes that the pair (m_1, m_2) is chosen randomly by the adversary $\mathcal{A}$. The resstance of h(·) to collision attacks by an (η, t)-adversary $\mathcal{A}$ implies that the maximum runtime t_h satisfies Adv $\mathcal{A}^{Hash}(t_h) \leq \eta$.

Definition 3. Consider an elliptic curve E_q(u, v) and a point P, the ECDDHP is "for a quadruple <P, uv_1.P, uv_2.P, uv_3.P>, decide whether $uv_3 = uv_1 \cdot uv_2$ or it is a uniform value", where uv_1, uv_2, $uv_3 \in Z^*_q$(= {1, 2, . . . , q − 1}).

To make ECDDHP intractable, the chosen prime q needs to be at least 160-bit number. In Theorem 1, we prove the semantic security of DAM – $IoS_{snj.}$

3.5. Research contributions

The contributions made in this article are listed below.

- We have discussed the recent works happening in the relative works section.
- We have proposed a new WSNs tailored for IoT scheme with respect to the architecture which ensures a better security by withstanding many security features
- By the help of formal method, ROR Models and informal security analysis, we have shown how the proposed scheme ensures the security.
- With the help of computation and communication cost we have presented the performance analysis.
- Lastly, we make a number of proposals crucial to the future

Table 3. Notations along with their descriptions

Symbol	Description
GWN	Gateway in the network
U_i,IoS_{sn_j}	User and IoT sensor nodes, respectively
SC_i/MD_i	Smart card/Mobile Device of U_i
ID_i,ID_{sn_j}	Unique identities of U_i and IoS_{sn_j} , respectively
PW_i	Password of U_i
X_{pri}	Long-term secret key of the GWN
IS_{key_j}	Secret key between GWN and IoS_{sn_j}
‖, ⊕	Operations of bitwise Concatenation and bitwise XOR
$S\ K_{ij}$/$S\ K_{ji}$	Session key established between Ui and IoT sensor nodes
h(.)	Cryptographic collision-resistant one way hash function
n_1,a_i,b_i,n_2	Random numbers/nonces
T_1,T_2,T_3	Timestamps used
ΔT	Maximum threshold transmission delay allowed
RTS_i	Registration timestamp of U_i
$i \stackrel{?}{=} j$	Validation check, if expression i matches j or not
$\mathcal{A}$	An adversary

3.6. Paper outline

The rest of this article is organised as following. Section 4 provides a novel system to assure a secure key agreement for a session and to ensure security characteristics, while the informal security analysis is described in Section 6. The performance analysis system is provided in section VII and compared against different schemes proposed by various researchers. Finally, in Section 9, the article is concluded.

4. Our Proposed Scheme

Considering the architecture as shown in Fig.1, the participants in the scheme such as user(U_i), gateway node (GWN), and IoT sensor node(IoS_{snj}) are involved in the complete communication mechanism. Initially, the user registers to the GWN to login into the system. Once the user receives the login credentials from GWN, as and when required and desires to get the information from the targeted S_{sn_j} , user makes a login request to GWN to avail the services from S_{sn_j} . Once the login request is successful, the request is transmitted to the targeted IoS_{sn_j} to establish a session key. Here IoS_{sn_j}validates the legitimacy of U_i and GWN before preparing a valid session key. On successful verification, IoS_{sn_j}responds with the possible session key to U_i . The user checks the authenticity of the received message, on successful establishment of session key between U_i and S_{sn_j} . Therefore, the fundamental concept is that three categories of WSN participants typically exist. Sensors are first distributed in a region on or in specific items. Secondly, a gateway is a particular node with relatively high WSN computational capacity. Thirdly, following mutual authentication, those who want information from specific items may access the sensors. When the user is authorised, a session key is created and used for encryption of further communications as required [72]. The entire process of the design is divided into f phases: a "user registration phase", "login and authentication phase", "password change/update phase", "node addition phase" (as briefed in Tables 2, 3, and 4).

In that system, we used the Honey_list list that is honey words. Honey words are kind of a honey encryption scheme, meaning flawed passwords and phrases. The complexities of [46] are referenced in the honeyword generating algorithm. This article uses the accompanying method among many tactics utilised during the login stage [46] for preventing passwords guessing attack by using the honey list. Naturally, we allow the login to proceed, but the framework monitors the login source. In addition, the framework ends when the honey list exceeds the threshold of ending the session [22].

Furthermore, in this process, we have adopted current timestamps of the system to restrict the replay attack. The clock synchronization needs to be done by all the participants at their end. This assumption is found reasonable, as the synchronization process is applied by many other recent proposals [6, 47, 16]. In Table 3, a list of notations with their description is given which we use in our proposed scheme. The description of the five phases are as follows:

4.1. Sensor node Registration Phase

GWN checks the availability of IoT sensor node identity ID_{sn_j}IDsnj from the list. If ID_{sn_j} is available, computes IS_{key_j}= h(ID_{sn_j}||X_{pri}) and stores before deploying it in the target field.

4.2. User registration phase

The user must register with the GWN in order to use the services of IoT-enabled sensor nodes. The description is as follows:

R1: The user U_i is free to select his ID_i , PW_i and chooses two random numbers a_i and b_i . Computes $UID_i = h(ID_i||b_i)$ and $UPW_i=h(b_i||ID_i||PW_i)$ further submits < UID_i , $UPW_i \oplus a_i$ > to the GWN through secure channel.

R2: On receiving the request, GWN checks the availability of UID_i . If UID_i is available, for each user, the gateway node computes $XU_i = h(UID_i||X_{pri}||RTS_i)$, $D_i=XU_i \oplus (UPW_i \oplus a_i)$. GWN stores ($TID_i$,$UID_i$) corresponding to the register user U_i where, RTS_i is the registration time stamp, TID_i is the temporary identity of the user.

R3: Finally, for each user, the GWN issues the credentials {D_i , XU_i , h(·), H(·)} else, send the "non availability" message.

R4: After receiving the credentials, U_i imprints the biometrics Bio_i in the Bio-hash function to computes

---

$L_i = H(Bio_i)$, $XU_i = D_i \oplus UPW_i \oplus a_i$, $A_i = XU_i \oplus h(UPW_i||L_i)$, $B_i = h(ID_i||L_i||PW_i)$, $LA_i = b_i \oplus h(PW_i||L_i)$,$LB_i = h(ID_i||XU_i||L_i||PW_i)$, and $TID'_i = TID_i \oplus h(L_i||b_i||UPW_i)$ stores the credentials in the mobile device MD_i as $\{LA_i$, LB_i , A_i , B_i , TID'_i , $h(\cdot)$, $H(\cdot)\}$ and completes the registration process.

4.3. **Login and Authentication Phases**

Here in this phase, the user produces his/her login credentials to the mobile device. The credentials issued during the registration phase are validated and allowed to transmit the message to the participants to get access to the desired services only once the user and IoT sensor node establishes a valid session key. This communication happens over the public channel. The details are as follows:

L1 : The user Ui uses his/her mobile device to input the login credentials such as identity ID_i, password PW_i and biometric Bio_i . MD_i computes $L_i = H(Bio_i)$, $b_i = LA_i \oplus h(PW_i||L_i)$,$UID_i = h(ID_i||b_i)$, $UPW_i=h(b_i||ID_i||PW_i)$, $XU_i=A_i \oplus h(UPW_i||L_i)$, and verifies $LB_i \stackrel{?}{=} h(ID_i||XU_i||L_i||PW_i)$ to validate the user's login credentials.

L2 : If this verification does not hold, user terminates the process. Otherwise, the user U_i submit the identity ID_{sn_j} of IoT sensor node from which the user wishes to get the services. This process is done under public channel.

L3 : MD_i generates a random number $n_1 \in Z_p^*$ within time T_1 and computes $TID_i = TID'_i \oplus h(L_i||b_i||UPW_i)$, ID'_i $h(UID_i||TID_i||UPW_i||L_i||T_1)$, $X_{u1} = n1 \cdot P$, $X_{u2} = n1 \cdot N_{pub}$, $X_{u3} = X_{u2} + X_{u1}$, $LID_i = ID'_i \oplus h(X_{u3} \oplus T_1)$, $M_2 = h(ID'_i||X_{u2}||LID_i)$, and LS $N_{j\text{–}ID} = ID_{snj} \oplus UID_i$.

L3 : Further, transmit the message $MSG_1 = \{LID_i , TID_i , M_2, X_{u1}, LSN_{j\text{–}ID}, T_1\}$ to GWN over a public channel.

A1 : Upon receiving the message MSG_1 from U_i , checks the freshness of the message $|T2 - T1| < \Delta T$ and retrieve UID_i using TID_i and computes $X'_{u2} = X_{u1} \cdot X_{pri}$, $X'_{u3} = X'_{u2} + X_{u1}$, $ID'_i = LID'_i \oplus h(X'_{u3} \oplus T_1)$, and verify $M_2 \stackrel{?}{=} h(ID'_i||X'_{u2}||LID'_i)$.

A1 : Upon receiving the message MSG_1 from U_i , checks the freshness of the message $|T2 - T1| < \Delta T$ and retrieve UID_i using TID_i and computes $X'_{u2} = X_{u1} \cdot X_{pri}$, $X'_{u3} = X'_{u2} + X_{u1}$, $ID'_i = LID'_i \oplus h(X'_{u3} \oplus T_1)$, and verify $M_2 \stackrel{?}{=} h(ID'_i||X'_{u2}||LID'_i)$.

A2 : GWN rejects the user's legitimacy by denying the request message, if the verification doesn't hold. Otherwise, GWN computes and $ID_{sn_j} = LSN_{j\text{–}ID} \oplus UID_i$, $B_j = h(ID_{sn_j} ||X_{pri})$, $\alpha_{GWN} = h(ID'_i||X_{u1}) \oplus B_j$, $\beta_{GWN} = h(\alpha_{GWN}|| ID_{sn_j}||B_j||X_{u1}||T_2)$ and transmit the message $MSG_2 =\{X_{u1}, \beta_{GWN}, \alpha_{GWN}, T_2\}$ to the IoT sensor node IoS_{sn_j} . **A3 :** On receiving the message MS G2, IoS_(sn_j) checks the freshness of the message $|T_3 - T_2| < \Delta T$. If the verification hold, using its shared secret IS_{keyj} computes $PID_i = \alpha_{GWN} \oplus IS_{keyj}$ and verifies $\beta_{GWN} \stackrel{?}{=} h(\alpha_{GWN}||ID_{sn_j} ||IS_{key_j}||X_{u1}||T_2)$. If the verification doesn't holds, IoS_{sn_j} reject the messages. Otherwise, generates a random number $n_2 \in Z_p^*$ within time T_3.

A4: IoS_{sn_j} computes $Y_{u1} = n_2 \cdot P$, $Y_{u2} = n_2 \cdot X_{u1}$, S $K_{ji} = h(PID_i||Y_{u1}||Y_{u2}||X_{u1}||T_3||ID_{sn_j})$, and $M_3 = h(PID_i||S K_{ji}||ID_{sn_j} ||T_3)$. Furthermore, sends the message $MSG_3 = \{Y_{u1}, M_3, T_3\}$ to U_i .

A5 : U_i receives the message MSG_3 and checks the freshness of the message as $|T4 - T3| < \Delta T$. If the verification holds, computes $X_{u4} = n_1 \cdot Y_{u1}$, $PID'_i = h(ID'_i ||X_{u1})$, the session key $SK_{ij} = h(PID'_i||Y_{u1}||X_{u4}||X_{u1}||T_3||ID_{sn_j})$ to verify $M_3 \stackrel{?}{=} h(PID'_i||SK^*_{ij}||ID_{sn_j}||T_3)$ if the verification holds, U_i authenticates IoS_{sn_j} and GWN. Otherwise, terminates the process.

4.4. User's Password/Biometric change/update phase

A registered user U_i can update his/her current password/biometrics and follows the steps without contacting the registered GWN:

PB1: U_i enters his/her login credentials ID_i , PW_i , and also imprints the current biometric Bio_i into MD_i . MD_i then computes $L_i = H(Bio_i)$, $b_i = LA_i \oplus h(PW_i||L_i)$, $UID_i = h(ID_i||b_i)$, $UPW_i = h(b_i||ID_i||PW_i)$, $XU_i = A_i \oplus h(UPW_i||L_i)$, and verifies $LB_i \stackrel{?}{=} h(ID_i||XU_i||L_i||PW_i)$ and validates the condition. Upon unsuccessful verification, this process is terminated by MD_i . Otherwise, MD_i asks U_i to supply new password and imprint new biometrics, if needed.

PB2: U_i picks PW_i^{new} and imprints Bio_i^{new} according to the user need. It is worth noticing that if U_i may not wish to update Bio_i , it will then taken as new biometrics, that is, Bio_i^{new} will be in this case as Bio_i . MD_i computes $UID_i = h(ID_i||b_i)$ and $UPW_i^{new} = h(b_i||ID_i||PW_i^{new})$. U_i imprints the new biometrics Bio_i^{new} in the Bio-hash function to computes $L_i^{new} = H(Bio_i^{new})$, $XU_i = D_i \oplus UPW_i^{new} \oplus a_i$, $A_i = XU_i^{new} \oplus h(UPW_i^{new}||L_i^{new})$, $B_i^{new} = h(ID_i||L_i^{new}||PW_i^{new})$, $LA_i = b_i \oplus h(PW_i^{new} || L_i^{new})$, $LB_i = h(ID_i||XU_i||L_i^{new}||PW_i^{new})$, and $TID'_i = TID_i \oplus h(L_i^{new}||b_i||UPW_i^{new})$ stores the credentials in the mobile device MD_i as$\{LA_i^{new}, LB_i^{new}, A_i^{new}, B_i^{new}, TID'_i$,h(·), H(·)} and completes the process.

4.5. Dynamic sensor node addition phase

As discussed in the Section 1, IoT sensor nodes are powered with limited battery consumption and memory requirements, they may get expired or been captured physically by an attacker. To ensure and maintain the dynamic nature of deploying the IoT sensor nodes in the unattended IoT environment, there should be a mechanism to support the deployment of new IoT sensor node $IoS_{sn_j}^{new}$ in the existing network. The details of this mechanism is presented in the following steps:

DA1: To initiate this process, the GWN is flexible enough to choose a unique identity IDnew snj for the new IoT sensor node $IoS_{sn_j}^{new}$.

DA2: GWN checks the availability of new IoT sensor node's identity, $IoS_{sn_j}^{new}$ from the list. If $IoS_{sn_j}^{new}$ is available, computes $IS_{key_j}^{new} = h(ID_{sn_j}^{new} || X_{pri})$ and stores before deploying it in the target field.

5. Formal Security Analysis

Formal security examination strategies are usually used to inspect and evaluate diverse check plans. According to literature [15, 27, 48, 49, 45, 44], various security assessment systems can be used to evaluate authentication methods. These methodologies can be ordered into three groups [50]; BAN Logic[41], and GNY[51] is applied for modal logic; AVISPA[56] and ProVerif [23] are employed for model checking. In this paper, we used ROR security theories.

5.1. ROR-Model based proof

Theorem 1. Assuming that our scheme $DAM - IoS_{sn_j}$ runs in polynomial time t_p and the adversary A aims to gain advantage over $DAM - IoS_{sn_j}$,we can analyze the security of the scheme under certain conditions. Let $query_h$ denote the cardinality of hash queries, |Hash| denote the size of the one-way hash function h(·), and $Adv^{ECDDHP}\mathcal{A}(tp)$ denote the adversary's advantage in breaching ECDDHP in time t_p (as per Definition 3). We assume that chosen passwords follow the Zipf 's law [52] and the bit-lengths of the biometric secret key σ_u and the user identity $IDMD_i$ are l_1 and l_2, respectively. Further, let $\beta' and\ s\beta'$ be the Zipf 's parameters [52, 21], and $\mathcal{A}$'s advantage in compromising the semantic security of the proposed scheme $DAM - IoS_{sn_j}$ be denoted by $Adv_{\mathcal{A}}^{DAM-IoS_{sn_j}}(t_p)$. Under these assumptions, we can derive an upper bound on the adversary's advantage as follows:

$$Adv_{\mathcal{A}}^{DAM-IoS_{sn_j}}(t_p) \leq 2Adv_{\mathcal{A}}^{ECDDHP}(t_p) + \frac{query_h^2}{|Hash|} + 2max\{\frac{query_s}{2^{l1}}, \frac{query_s}{2^{l2}}, \beta' \cdot query_s^{s\beta'}$$

Here, the upper bound consists of three terms: the first term represents the adversary's advantage in breaching ECDDHP, the second term represents the effect of hash queries on the scheme's security, and the third term represents the effect of biometric secret key and user identity lengths, as well as the Zipf 's parameters, on the scheme's security.

This proof is presented in the similar way as presented by authentication protocols [35, 6]. Here four games are played, such as $Game_k$, (k = 0, 1, 2, 3) related with the evidence where $Game_0$ is the starting and $Game_3$ is the finishing games. We define $Succ_{\mathcal{A}}^{Game_k}$ as "an event wherein $\mathcal{A}$ can guess the random bit c in the game Gamek correctly" and also the "advantage of $\mathcal{A}$ in winning the game $Game_k$ as $Adv_{\mathcal{A}Game_k}^{DAM-IoS_{sn_j}} = Pr[Succ_{\mathcal{A}}^{Game_k}]$". The detailed study of these games is as follows:

$Game_0$:Game0 is the same as the real ROR model protocol. Therefore, the semantic security of DAM $- IoS_{sn_j}$ is defined in Definition 1.

$$Adv_{\mathcal{A}}^{DAM-\mathrm{IoS}_{\mathrm{sn_j}}}(t_p) = |2 \cdot Adv_{\mathcal{A},Game_0}^{DAM-\mathrm{IoS}_{\mathrm{sn_j}}} - 1| \quad (1)$$

$Game_1$: Consider the proposed scheme DAM $- IoS_{sn_j}$ for authentication and key agreement between MD_i and S_{sn_j} , with polynomial time t_p. Let $\mathcal{A}$ be an adversary that can intercept all messages exchanged during the authentication and key agreement phase, including $MSG_1 = LID_i$, T ID_i , M_2, X_{u1}, LS N_{j-ID}, T_1, $MSG_2 = X_{u1}$, β_{GWN}, α_{GWN}, T_2, and $MSG_3 = Y_{u1}$, M_3, T_3, and can execute the Execute, Reveal, and Test queries as described in Table 2. Let SK_{ij} be the session key established between MD_i and IoS_{sn_j} using the proposed scheme.

If the chosen passwords follow the Zipf's law and the bit-lengths of the biometric secret key σu and the user identity ID_{MDi} are l_1 and l_2, respectively, with Zipf's parameters β' and $s\beta'$, then the advantage of $\mathcal{A}$ in compromising the semantic security of the proposed scheme is negligible, i.e.,

$$Adv_{\mathcal{A}}^{DAM-\mathrm{IoS}_{\mathrm{sn_j}}}(t_p) = \in \quad (2)$$

where ∈ is a negligible function of the security parameter n.

$$Adv_{\mathcal{A},Game_1}^{DAM-\mathrm{IoS}_{\mathrm{sn_j}}} = Adv_{\mathcal{A},Game_0}^{DAM-\mathrm{IoS}_{\mathrm{sn_j}}} \quad (3)$$

$Game_2$: In this game, the hash searches are simulated. Both X_{u1} and T_1 are altered in the MSG_1 message. Similarly, MSG_2 and MSG_3 are also equally unexpected, as they include random timestamps and random numbers, such as Y_{u1}, Y_{u2}, T_2, PID_i , X_{u4}, and T_3 are equally unforeseeable. So no collision occurs when $\mathcal{A}$ does hash queries. Since both $Game_1$ and $Game_2$ are "indistinguishable" except for the inclusion of the $Game_2$ simulations, we obtain birthday paradox outcomes, we have

$$|Adv_{\mathcal{A},Game_2}^{DAM-\mathrm{IoS}_{\mathrm{sn_j}}} - Adv_{\mathcal{A},Game_1}^{DAM-\mathrm{IoS}_{\mathrm{sn_j}}}| \leq \frac{query_h^2}{2|Hash|} \quad (4)$$

$Game_3$: To summarize, in the final game, $\mathcal{A}$ can use the CorruptMD(MDi) query to extract the credentials from a compromised mobile device MD_i . The probability that $\mathcal{A}$ can guess the biometric secret key σ_u of l_1 bit-length and user identity ID_{MDi} of l_2 bit-length is $\frac{query_s}{2l_1}$ and $\frac{query_s}{2l_2}$, respectively. If $\mathcal{A}$ can use targeted attacks exploiting the user's personal data, then $query_s \leq 10^6$ gives them an advantage over 0.5. However, if passwords follow the Zipf's law and $\mathcal{A}$ uses attacks via trawling, then $query_s = 10^7$ or 10^8 is needed for $\mathcal{A}$ to have an advantage greater than 0.5.

Furthermore, $\mathcal{A}$ will have all the intercepted messages MSG_1, MSG_2 and MSG_3. To derive the session key $SK_{ij} = h(PID'_i||Y_{u1}||X_{u4}||X_{u1}||T_3||ID_{sn_j}) = SK_{ji}$ shared between MD_i and IoS_{sn_j} , $\mathcal{A}$ needs to calculate $X_{u4}(= Y_{u2})$, X_{pri}, and $X_{u3} = (X'_{u2})$.This is the derivation of both the $h(ID'_i||X_{u1})$ and the $h(ID_{snj} \mid X_{pri})$, which in a polynomially restricted time t_p is computationally costly owing to the intractability of ECDDHP. Since the $Game_2$ and $Game_3$ games are "indistinguishable", the following is excerpted to include the question and ECDDHP of $CorruptMD(MD_i)$ such as

$$\left|Adv_{\mathcal{A},Game_3}^{DAM-IoS_{sn_j}} - Adv_{\mathcal{A},Game_2}^{DAM-IoS_{sn_j}}\right| \leq Adv_{\mathcal{A}}^{ECDDHP}(t_p) + max\{\frac{query_s}{2^{l_1}}, \frac{query_s}{2^{l_2}}, \beta' \cdot query_s^{s\beta'}\} \quad (5)$$

Now, all the relevant queries related to the above games are executed, and then the Reveal query is executed along with Test query to guess the random bit c. Thus, we get

$$Adv_{\mathcal{A},Game_3}^{DAM-IoS_{sn_j}} = \frac{1}{2} \quad (6)$$

The following equations (1), (3) and (6) derives:

$$\frac{1}{2}.Adv_{\mathcal{A}}^{DAM-IoS_{sn_j}}(t_p) = \left|Adv_{\mathcal{A},Game_0}^{DAM-IoS_{sn_j}} - \frac{1}{2}\right|$$
$$= |Adv_{\mathcal{A},Game_1}^{DAM-IoS_{sn_j}} - Adv_{\mathcal{A},Game_3}^{DAM-IoS_{sn_j}}|$$
$$\leq \left|Adv_{\mathcal{A},Game_1}^{DAM-IoS_{sn_j}} - Adv_{\mathcal{A},Game_2}^{DAM-IoS_{sn_j}}\right|$$
$$+|Adv_{\mathcal{A},Game_2}^{DAM-IoS_{sn_j}} - Adv_{\mathcal{A},Game_3}^{DAM-IoS_{sn_j}}| \quad (7)$$

Next, Equations (4), (5) and (7) provide to the following result:

$$\frac{1}{2}.Adv_{\mathcal{A}}^{DAM-IoS_{sn_j}}(t_p) \leq \frac{query_h^2}{2|Hash|} + Adv_{\mathcal{A}}^{ECDDHP}(t_p) + max\{\frac{query_s}{2^{l_1}}, \frac{query_s}{2^{l_2}}, \beta' \cdot query_s^{s\beta'}\} \quad (8)$$

Finally, the equation (8) is multiplied by 2 on both sides, we have the desired result:

$$Adv_{\mathcal{A}}^{DAM-IoS_{sn_j}}(t_p) \leq 2Adv_{\mathcal{A}}^{ECDDHP}(t_p) + \frac{query_h^2}{|Hash|} + 2max\{\frac{query_s}{2^{l_1}}, \frac{query_s}{2^{l_2}}, \beta' \cdot query_s^{s\beta'}\}$$

6. Security Evaluation

In this section, the following known attacks are analyzed under the informal security analysis.

Proposition 1. Achieving user anonymity and IoT sensor node anonymity

This attack is seen in this way, let us suppose that the login message {LID_i , TID_i , M_2, X_{u1}, LS N_{j-ID}, T_1} of the user is eavesdropped by $\mathcal{A}$. Due to the randomness in the session random values a_i , b_i , n_1, $\mathcal{A}$ cannot obtain the identities of the participants from the computations $LID_i = ID'_i \oplus h(X_{u3} \oplus T_1)$, $LSN_{j-ID} = ID_{sn_j} \oplus UID_i$ and $M_2 = h(ID'_i||X_{u2}||LID_i)$ due to the advantage of using one-way hash function. Furthermore, it is computationally hard to guess the two values at a time. Thus, $\mathcal{A}$ fails in guessing the identities of the participants from the computed parameters. Additionally, $\mathcal{A}$ needs to posses the private key of gateway node i.e., X_{pri} in order to frame the attack. Let us suppose, $\mathcal{A}$ possesses the credentials {LA_i , LB_i , A_i , B_i , TID'_i } of MDi . Again, in this case too, the attacker still fails to guess or extract the identities of the participants from $LB_i = h(ID_i ||XU_i|| L_i||PW_i)$ because of the one-way characteristic nature of the hash function. In addition to this, the bindingness of biometric and password of user completes the possibility of guessing. Therefore, our proposed scheme successfully withstand user and IoT sensor node anonymity.

Proposition 2. Mobile device loss attack resistance

In this attack, we assume that U_i's mobile device is lost. Then the credentials issued by the gateway node are exposed to $\mathcal{A}$. As discussed in proposition 1, $\mathcal{A}$ fails to guess the password correctly from $LB_i = h(ID_i ||XU_i|| L_i||PW_i)$, and with the inclusion of Bioi rules out guessing chances. Even if, $\mathcal{A}$ wants to use LA_i , A_i , B_i , TID'_i to frame the attack, due to the inclusion of gateway node's private key X_{pri} it becomes computationally hard for the $\mathcal{A}$ to obtain any valuable information. Thus, $\mathcal{A}$ fails to compute a valid login request without having IDi , L_i and PW_i .

Proposition 3. Offline password/biometric guessing attack resilience

Here, in the scheme, the password of the user is embedded within the parameters such as LB_i , LA_i , A_i , B_i and not involved in direct communication either with the login messages nor with the other credentials issued by GWN. Furthermore, as and when we compute M_2, β_{GWN}, α_{GWN}, M_3, to perform login and authentication values, these values are performed as a output of hash function and other one is a bio-hash value $L_i = H(Bio_i)$. Thus, security of the password and biometric is strictly relying on one-way hash functions and Bio-hash characteristics. Therefore, to break the relying functions and guess the password and biometric is computationally hard.

Proposition 4. Replay attack resilience

$\mathcal{A}$ may capture the transmitted messages and tries to replay the messages to frame the attack. Let us suppose, A captures the login message {LID_i , TID_i , M_2, X_{u1}, LSN_{j-ID}, T_1} and replays to GWN. However, as discussed in proposition 1, we understood that $\mathcal{A}$ cannot compute the session key as computed by S_{sn_j} . Thus fails to validate the legitimacy of the message and couldn't differentiate the arbitrary messages captured. This happens due to the non-control on the {ID_i , ID_{snj} , n_1, X_{pri}}. Therefore, replaying any other random message can be easily detectable due to the session specific key and the random values {n_1, n_2} chosen by the participants.

Proposition 5. User, GWN node and IoT sensor node impersonation attack resilience

This attack is similar to the above proposition 4. To impersonate the participants, attacker may capture the login messages and modify the transmitted messages, but $\mathcal{A}$ must have {LID_i , ID_i}. From the earlier discussions propositions 2 and 3 it is clear that $\mathcal{A}$ fails to guess the user login credentials. Now, to impose this attack, $\mathcal{A}$ has to extract X_{pri} to successfully impersonate GWN and $\{IS_{key_j}, ID_{sn_j}\}$ to impersonate S_{sn_j} . As secret credentials of GWN and IoS_{sn_j} are not transmitted in plaintext, it is a challenging task for $\mathcal{A}$ to obtain them in real-time and compromise the communication by imposing impersonation attack. Therefore, impersonation attacks are not applicable on the scheme.

Proposition 6. Achieving mutual authentication

The following three instances are used for mutual authentication between Ui , GWN and IoS_{sn_j}

- GWN authenticates Ui by verifying first RIDi and then RIDi by checking $M_2 \overset{?}{=} h(ID'_i||X'_{u2}||LID'_i)$.
- The validity of GWN may be verified using IoS_{sn_j} by verifying whether $\beta_{GWN} c\ h(\alpha_{GWN}||\ ID_{sn_j}||IS_{key_j}||X_{u1}||T_2)$.
- U_i validates the legitimacy of GWN $and\ IoS_{sn_j}$ by verifying $M_3 \overset{?}{=} h(PID'_i\,||S\,K^*_{ij}||\,ID_{sn_j}||T_3)$.

Proposition 7. Ephemeral secret leakage attack

After mutual authentication, in the proposed system (Proposition 10), both U_i and IoS_{sn_j} during the login & authentication process, $SK_{ji} = h(PID_i||Y_{u1}||Y_{u2}||X_{u1}||T_3||ID_{sn_j}) = SK = h(PID'_i||Y_{u1}||Y_{u2}||X_{u1}||T_3||ID_{sn_j}) = SK_{ij}$ agree on a common session key. In the two situations, the key security of the session of the technique presented relates to secret credentials:

Case 1: Suppose that n_1 and n_2 are known to $\mathcal{A}$ for short-term secret credentials. In order to build the session key without knowing of long-term secreties, it would be computationally impossible for the $\mathcal{A}$, as they are not revealed to $\mathcal{A}$.

Case 2: If some or all the long-term secrets PW_i , X_{pri}, UID_i , b_i , X_{u3}, X_{u4}, PID_i are leaked to $\mathcal{A}$, and the ephemeral secret credentials n_1 and n_2 are not leaked to $\mathcal{A}$, $\mathcal{A}$'s task to generate session key becomes again be computationally infeasible. From the preceding examples, it is obvious that only if both ephemeral & secret credentials are exposed, $\mathcal{A}$ can deduce a session key. In addition, it should be noted that the safety of past and future sessions to $\mathcal{A}$ is not affected, even if the current session key is compromised [6]. The suggested approach thereby safeguards both forward and backward secrecy along with crucial safety session. In addition, the suggested system does not influence the safety of other previous and forthcoming sessions by leaking a session key with the assistance of a session hijacking attack in a given session. The scheme proposed is secure against the ESL attack in summarizing all these cases.

7. Observations and Analysis

7.1. Comparison with the current state-of-the-art

In this subsection, we compare our work with the recently proposed schemes in terms of the evaluation on security features and their functionalities.

7.2. Computation Cost Comparison

Table 4 shows the execution time needed for different cryptographic primitives, where the computation time in executing "Hash and Bio-Hashing function" say T_h, T_{BioH} takes 0.00032 approximately. Similarly, "Symmetric encryption/decryption" ($T_{s_{E/D}}$) takes 0.0056, "ECC point multiplication" (T_{ECCM}) takes 0.0171, "ECC point addition " ($T_{ECCA} \approx 5T_{mul}$) takes 0.0044 seconds. "Biometric-Fuzzy extractor" ($T_{fe} \approx T_{ECCM}$) and "Chaotic Map Chebysev" ($T_{cm} \approx T_{ECCM}$) takes 0.0171, and "Message Authentication Code " ($T_{MAC} \approx T_h$) takes 0.00032 seconds which are based on the existing experimental results [6, 21].

Table 4. Approximate time required for various operations [6, 21].

Notation	Description (Time to compute)	Approximate computation time (in seconds)
T_h,T_{BioH}	Hash and Bio-Hashing functions	0.00032
$T_{s_{E/D}}$	Symmetric encryption/decryption	0.0056
T_{ECCM}	ECC point multiplication	0.0171
$T_{ECCA} \approx 5T_{mul}$	ECC point addition	0.0044
$T_{fe} \approx T_{ECCM}$	Biometric-Fuzzy extractor	0.0171
$T_{cm} \approx T_{ECCM}$	Chaotic Map Chebysev	0.0171
$T_{MAC} \approx T_h$	Message Authentication Code	0.00032

Table 5. Comparison of communic ation costs

Scheme	No.of messages	Messages Transmission	Cost (in bits)
Srinivas et at.[6]	3	$U_i \overset{992}{\longrightarrow} GWN \overset{672}{\longrightarrow} IoS_{sn_j} \overset{512}{\longrightarrow} U_i$	2176
Choi et al. [19]	4	$U_i \overset{992}{\longrightarrow} GWN \overset{1504}{\longrightarrow} SN_j \overset{352}{\longrightarrow} GWN \overset{704}{\longrightarrow} U_i$	3552
Challa et al. [20]	3	$U_i \overset{992}{\longrightarrow} GWN \overset{1024}{\longrightarrow} SN_j \overset{512}{\longrightarrow} U_i$	2528
Choi et al. [20]	3	$U_i \overset{992}{\longrightarrow} GWN \overset{672}{\longrightarrow} IoS_{sn_j} \overset{672}{\longrightarrow} U_i$	2336
Li et al. [49]	4	$U_i \overset{1120}{\longrightarrow} GWN \overset{640}{\longrightarrow} SN_j \overset{320}{\longrightarrow} GWN \overset{480}{\longrightarrow} U_i$	2560
Wazid et al. [38]	4	$U_i \overset{736}{\longrightarrow} GWN \overset{576}{\longrightarrow} SN_j \overset{512}{\longrightarrow} GWN \overset{768}{\longrightarrow} U_i$	2592

Li et al. [61]	4	$U_i \overset{800}{\longrightarrow} GWN \overset{640}{\longrightarrow} SN_j \overset{640}{\longrightarrow} GWN \overset{640}{\longrightarrow} U_i$	2720
Wu et al. [59]	4	$U_i \overset{800}{\longrightarrow} GWN \overset{480}{\longrightarrow} SN_j \overset{640}{\longrightarrow} GWN \overset{960}{\longrightarrow} U_i$	2880
Our scheme	3	$U_i \overset{992}{\longrightarrow} GWN \overset{672}{\longrightarrow} IoS_{sn_j} \overset{512}{\longrightarrow} U_i$	2176

Table 6. Computation cost comparison

Parties →	Gateway node	Sensor node	User	Total	Time (ms)
Schemes ↓	(GWN)	(S_j/ISD_j/IoD_{sn_j})	(SC_i/MD_i)		
Srinivas et at.[6]	$10T_h$	$6T_h + 2T_{cm}$	$15T_h + 2T_{cm} + T_{fe}$	$31T_h + 4T_{cm} + T_{fe}$	≈ 0.09542
Choi et al. [19]	$5T_h + T_{ECCM}$	$6T_h + 2T_{ECCM}$	$8T_h + 3T_{ECCM}$	$19T_h + 6\ T_{ECCM}$	≈ 0.14036
Challa et al. [20]	$4T_h + 5T_{ECCM}$	$3T_h + 4T_{ECCM}$	$5T_h + 5T_{ECCM} + T_{fe}$	$12T_h + 14T_{ECCM} + T_{fe}$	≈ 0.26034
Choi et al. [20]	$10T_h + 2T_{E/D}$	$6T_h + T_{E/D} + 2T_{ECCM}$	$10T_h + T_{E/D} + 2T_{ECCM}$	$26T_h + 4T_{E/D} + 4T_{ECCM}$	≈ 0.09912
Li et al. [49]	$9T_h + T_{ECCM}$	$4T_h$	$9T_h + 2T_{ECCM} + T_{fe}$	$22T_h + 3T_{ECCM} + T_{fe}$	≈ 0.07544
Wazid et al. [38]	$5T_h + 4T_{E/D}$	$4T_h + 2T_{E/D}$	$13T_h + 2T_{E/D} + T_{fe}$	$2T_h + 8T_{E/D} + T_{fe}$	≈ 0.06894
Li et al. [61]	$7T_h + T_{ECCM}$	$4T_h + 2T_{ECCM}$	$8T_h + 3T_{ECCM} + T_{fe}$	$19T_h + 6T_{ECCM} + T_{fe}$	≈ 0.12578
Wu et al. [59]	$11T_h + 2T_{E/D}$	$4T_h + T_{E/D} + 2T_{ECCM}$	$11T_h + T_{E/D} + 2T_{ECCM}$	$26T_h + 4T_{E/D} + 4T_{ECCM}$	≈ 0.09912
Our scheme	$5T_h + T_{ECCM} + T_{ECCA}$	$3T_h + 2\ T_{ECCM}$	$12T_h + T_{BioH} + 3T_{ECCM} + T_{ECCA}$	$20T_h + T_{BioH} + 6T_{ECCM} + 2T_{ECCA}$	≈ 0.11812

In this study, we consider the computational results of the experiments as shown in Table 5 to understand the behavior of login and authentication phases of our scheme and other examined schemes such as [19, 6, 57, 13, 58, 59, 49, 61, 20, 38]. The detailed analysis is tabulated in Table 6. The estimated cost computations required for Srinivas et al. [6]≈ 0.09542, Choi et al. [19] ≈ 0.14036, Choi et al.[57] ≈ 0.09912, Li et al. [49] ≈ 0.07544, Challa et al. [20] ≈ 0.26034, Wazid et al. [38] ≈ 0.06894, Li et al. [61] ≈ 0.12578, Wu et al.[59] ≈ 0.09912 ms, respectively. Our scheme performs better than [19], [20], and [61]. Although our scheme performs the computations slightly higher than rest of the compared schemes, due to the potentiality in preserving and ensuring the security features, our scheme has much advantage over the other schemes. Thus, from the Table 5, and Table 6 it is clear that the proposed scheme performs well as compared to other existing schemes.

7.3. Communication Cost Comparison

To compare the communication cost with the other schemes, we have considered the following assumptions. The communication cost required for random nonce, identity, timestamp, hash output (if we apply SHA-1 as h(·) [70]), message authentication code and certificate (signature using elliptic curve digital signature algorithm

(ECDSA) [71]) are 160, 160, 32, 160, 160, 320 bits respectively. Furthermore, modular exponentiation and inversion operations consume 1024-bits is considered for this comparative study such that the level of security is ensured.

Table 5 provides a summary of the comparative study on overhead comparisons of communication during the login/authentication phase. The proposed scheme consumes the communication cost while transmitting the messages from the user to GWN as $Message_1$=(160+160+160+320+160+32)=992 bits, $Message_2$ =(320+160+160+32)=672 bits from GWN to IoS_{sn_j}, and from IoS_{sn_j} to U_i as $Message_3$=(320+160+32)= 512 bits respectively. Therefore, the total communication cost consumed is 2176 bits which is equal to that of Srinivas et al. [6]. It is observed from the Table 6, our scheme consumes less number of bits in comparison to the schemes such as Choi et al. [19] consumes 3552 bits, Challa et al. [20] consumes 2528, Choi et al.[57] takes 2336 bits, Li et al. [49] takes 2560 bits, Wazid et al.[38] consumes 2592 bits, Li et al. [61] uses 2720 bits and Wu et al.[59] consumes 2880 bits. This shows, from Tables 5 and Table 6 we can observe that our proposed scheme proves its efficiency in terms of ensuring security attributes, computational cost and communication bits.

8. Concluding Remarks

This study proposes a self-verifiable user authentication and key agreement method for safe communication with the biometric characteristics of users in WSNs adapted to IoT. Our bio-hashing system extracts the user’s biometrics and uses our proposed three-factor characteristics to collect data via a smartphone device, providing practical advantages for the safe building and transmission of essential elements. The proposed approach allows dynamic node addition and user-friendly password/biometric updates effectively. Our informal security analysis shows that the proposed approach effectively avoids all well-known authentication protocol security threats. Our suggested scheme’s performance is comparable to related schemes while offering greater safeguards than other relevant protocols. In the future, we plan to extend our work to industrial environments to enhance its performance and safety. This will allow us to make further changes and validations to the proposed method. Additionally, we aim to continue our work on decentralizing ways to connect our method to IoT and blockchain. This study shows the potential of our proposed approach to enhance the security of WSNs adapted to IoT and provide practical advantages for safe communication.

9. Acknowledgements

The author[1] extends his sincere gratitude to Raghu Engineering College, Visakhapatnam for its support. The author[2] extends his sincere gratitude to GITAM Deemed to be University, Visakhapatnam for its support. The author[3] extends his sincere gratitude to Vasavi College of Engineering, Hyderabad. for its support.

Refrences

[1] Ashton, K. That ‘internet of things’ thing. RFID journal, 22(7) 2009, pp.97-114.
[2] J. Li, W. Zhang, V. Dabra, K.-K. R. Choo, S. Kumari, D. Hogrefe, Aep-ppa: An anonymous, efficient and provably-secure privacy-preserving authentication protocol for mobile services in smart cities, Journal of Network and Computer Applications 134 (2019) 52–61.
[3] M. Wazid, A. K. Das, V. Odelu, N. Kumar, W. Susilo, Secure remote user authenticated key establishment protocol for smart home environment, IEEE Transactions on Dependable and Secure Computing.
[4] S. Pandya, H. Ghayvat, K. Kotecha, M. Awais, S. Akbarzadeh, P. Gope, S. C. Mukhopadhyay, W. Chen, Smart home anti-theft system: A novel approach for near real-time monitoring and smart home security for wellness protocol, Applied System Innovation 1 (4) (2018) 42.
[5] L. D. Xu, W. He, S. Li, Internet of things in industries: A survey, IEEE Transactions on Industrial Informatics 10 (4) (2014) 2233–2243.
[6] J. Srinivas, A. K. Das, M. Wazid, N. Kumar, Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things, IEEE Transactions on Dependable and Secure Computing.
[7] S. K. Lee, M. Bae, H. Kim, Future of iot networks: A survey, Applied Sciences 7 (10) (2017) 1072.

[8] M. Wazid, A. K. Das, R. Hussain, G. Succi, J. J. Rodrigues, Authentication in cloud-driven iot-based big data environment: Survey and outlook, Journal of Systems Architecture 97 (2019) 185–196.
[9] P. K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for iot services, Journal of Information Security and Applications 34 (2017) 255–270.
[10] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of things (iot): A vision, architectural elements, and future directions, Future Generation Computer Systems 29 (7) (2013) 1645 – 1660.
[11] K. Xue, C. Ma, P. Hong, R. Ding, A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks, Journal of Network and Computer Applications 36 (1) (2013) 316–323.
[12] M. Turkanovic, B. Brumen, M. H ´ olbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor ¨ networks, based on the internet of things notion, Ad Hoc Networks 20 (2014) 96–112.
[13] M. S. Farash, M. Turkanovic, S. Kumari, M. H ´ olbl, An efficient user authentication and key agreement scheme for heterogeneous wireless ¨ sensor network tailored for the internet of things environment, Ad Hoc Networks 36 (2016) 152–176.
[14] R. Amin, G. Biswas, A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks, Ad Hoc Networks 36 (2016) 58–80.
[15] J. Srinivas, S. Mukhopadhyay, D. Mishra, Secure and efficient user authentication scheme for multi-gateway wireless sensor networks, Ad Hoc Networks 54 (2017) 147–169.
[16] F. Wu, L. Xu, S. Kumari, X. Li, J. Shen, K.-K. R. Choo, M. Wazid, A. K. Das, An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment, Journal of Network and Computer Applications 89 (2017) 72–85.
[17] H.-Y. Chien, New efficient user authentication scheme with user anonymity facilitating e-commerce applications, in: The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007), IEEE, 2007, pp. 461–464.
[18] S. Arunkumar, M. Srivatsa, M. Rajarajan, A review paper on preserving privacy in mobile environments, Journal of Network and Computer Applications 53 (2015) 74–90.
[19] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, D. Won, Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography, Sensors 14 (6) (2014) 10081–10106.
[20] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, K.-Y. Yoo, Secure signature-based authenticated key establishment scheme for future iot applications, IEEE Access 5 (2017) 3028–3043.
[21] J. Srinivas, A. K. Das, N. Kumar, J. Rodrigues, Cloud centric authentication for wearable healthcare monitoring system, IEEE Transactions on Dependable and Secure Computing. 18 Author / xx (2023) 1–2019
[22] J. Lee, S. Yu, M. Kim, Y. Park, A. K. Das, On the design of secure and efficient three-factor authentication protocol using honey list for wireless sensor networks, IEEE Access 8 (2020) 107046–107062.
[23] L. Xu, F. Wu, A lightweight authentication scheme for multi-gateway wireless sensor networks under iot conception, Arabian Journal for Science and Engineering 44 (4) (2019) 3977–3993.
[24] W. Zhang, Z. Wang, S. K. Das, M. Hassan, Security issues in wireless mesh networks, in: Wireless Mesh Networks, Springer, 2008, pp. 309–330.
[25] M. El-Hajj, M. Chamoun, A. Fadlallah, A. Serhrouchni, Analysis of authentication techniques in internet of things (iot), in: 2017 1st Cyber Security in Networking Conference (CSNet), IEEE, 2017, pp. 1–3.
[26] A. K. Das, S. Zeadally, D. He, Taxonomy and analysis of security protocols for internet of things, Future Generation Computer Systems 89 (2018) 110–125.
[27] D. He, D. Wang, Robust biometrics-based authentication scheme for multiserver environment, IEEE Systems Journal 9 (3) (2015) 816–823. doi:10.1109/JSYST.2014.2301517.
[28] J. Lee, S. Yu, K. Park, Y. Park, Y. Park, Secure three-factor authentication protocol for multi-gateway iot environments, Sensors 19 (10) (2019) 2358.

[29] Q. Jiang, S. Zeadally, J. Ma, D. He, Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks, IEEE Access 5 (2017) 3376–3392.

[30] C. Wang, G. Xu, J. Sun, An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks, Sensors 17 (12) (2017) 2946.

[31] J. Srinivas, D. Mishra, S. Mukhopadhyay, S. Kumari, Provably secure biometric based authentication and key agreement protocol for wireless sensor networks, Journal of Ambient Intelligence and Humanized Computing 9 (4) (2018) 875–895.

[32] A. T. B. Jin, D. N. C. Ling, A. Goh, Biohashing: two factor authentication featuring fingerprint data and tokenised random number, Pattern recognition 37 (11) (2004) 2245–2255.

[33] D. Dolev, A. Yao, On the security of public key protocols, IEEE Transactions on information theory 29 (2) (1983) 198–208.

[34] R. Canetti, H. Krawczyk, Universally composable notions of key exchange and secure channels, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2002, pp. 337–351.

[35] J. Srinivas, A. K. Das, N. Kumar, J. J. Rodrigues, Tcalas: Temporal credential-based anonymous lightweight authentication scheme for internet of drones environment, IEEE Transactions on Vehicular Technology 68 (7) (2019) 6903–6916.

[36] T. S. Messerges, E. A. Dabbish, R. H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE transactions on computers 51 (5) (2002) 541–552.

[37] T. A. Alghamdi, Parametric analysis on optimized energy-efficient protocol in wireless sensor network, Soft Computing (2020) 113.

[38] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, “Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks,” IEEE Internet of Things Journal, vol. 5, no. 1, pp. 269-282, Feb 2018.

[39] Vinoth, R., Deborah, L. J., Vijayakumar, P., Kumar, N., Secure Multi-factor Authenticated Key Agreement Scheme for Industrial IoT, IEEE Internet of Things Journal 2020.

[40] S. Mrdovic, B. Perunicic, Kerckhoffs’ principle for intrusion detection, in: Networks 2008-The 13th International Telecommunications Network Strategy and Planning Symposium, IEEE, 2008, pp. 1–8.

[41] M. Burrows, M. Abadi, R. Needham, A logic of authentication, ACM Transactions on Computer Systems 8 (1) (1990) 18–36.

[42] R. Canetti, H. Krawczyk, Analysis of key-exchange protocols and their use for building secure channels, in: International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT’01), Springer, Innsbruck (Tyrol), Austria, 2001, pp. 453–474.

[43] R. Canetti, H. Krawczyk, Universally Composable Notions of Key Exchange and Secure Channels, in: International Conference on the Theory and Applications of Cryptographic Techniques– Advances in Cryptology (EUROCRYPT’02), Amsterdam, The Netherlands, 2002, pp. 337–351.

[44] Kumar, V., Ahmad, M., Mishra, D., Kumari, S., Khan, M. K. (2020). RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. Vehicular Communications, 22, 100213.

[45] Safkhani, M., Camara, C., Peris-Lopez, P., Bagheri, N. (2021). RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing. Vehicular Communications, 28, 100311.

[46] A. Juels, R. L. Rivest, Honeywords: Making password-cracking detectable, in: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, 2013, pp. 145–160.

[47] S.-K. Yang, Y.-M. Shiue, Z.-Y. Su, I.-H. Liu, C.-G. Liu, An authentication information exchange scheme in wsn for iot applications, IEEE Access 8 (2020) 9728–9738.

[48] P. R. Yogesh, et al., Formal verification of secure evidence collection protocol using ban logic and avispa, Procedia Computer Science 167 (2020) 1334–1344.

[49] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, K.-K. R. Choo, A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments, Journal of Network and Computer Applications 103 (2018) 194 – 204.

[50] M. Alizadeh, M. Zamani, S. Baharun, A. Abdul Manaf, K. Sakurai, H. Anada, H. Keshavarz, S. Ashraf Chaudhry, M. Khurram Khan, Cryptanalysis and improvement of" a secure password authentication mechanism for seamless handover in proxy mobile ipv6 networks", PloS one 10 (11) (2015) e0142716.
[51] A. Mathuria, R. Safavi-Naini, P. Nickolas, On the automation of gny logic, Australian Computer Science Communications 17 (1995) 370– 379.
[52] D. Wang, H. Cheng, P. Wang, X. Huang, G. Jian, Zipfs law in passwords, IEEE Transactions on Information Forensics and Security 12 (11) (2017) 2776–2791.
[53] D. von Oheimb, The high-level protocol specification language hlpsl developed in the eu project avispa, in: Proceedings of 3rd APPSEM II (Applied Semantics II) Workshop (APPSEM'05), Frauenchiemsee, Germany, 2005, pp. 1–17.
[54] AVISPA, Automated Validation of Internet Security Protocols and Applications, http://www.avispa-project.org/. Accessed on March 2019 19 Author / xx (2023) 1–20 20 (2019).
[55] J. Srinivas, A. K. Das, A. V. Vasilakos, Designing secure lightweight blockchain-enabled rfid-based authentication protocol for supply chains in 5g mobile edge computing environment, IEEE Transactions on Industrial Informatics.
[56] AVISPA, SPAN, the Security Protocol ANimator for AVISPA, http://www.avispa-project.org/. Accessed on March 2019 (2019).
[57] Y. Choi, Y. Lee, D. Won, Security improvement on biometric based authentication scheme for wireless sensor networks using fuzzy extraction, International Journal of Distributed Sensor Networks 12 (1) (2016) 8572410.
[58] Q. Jiang, N. Kumar, J. Ma, J. Shen, D. He, N. Chilamkurti, A privacy-aware two-factor authentication protocol based on elliptic curve cryptography for wireless sensor networks, International Journal of Network Management 27 (3) (2017) e1937.
[59] F. Wu, L. Xu, S. Kumari, X. Li, A new and secure authentication scheme for wireless sensor networks with formal proof, Peer-to-Peer Networking and Applications 10 (1) (2017) 16–30.
[60] T. Liaqat, M. Akbar, N. Javaid, U. Qasim, Z. A. Khan, Q. Javaid, T. A. Alghamdi, I. A. Niaz, "On reliable and efficient data gathering based routing in underwater wireless sensor networks, Sensors 16 (9) (2016) 1391.
[61] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A Robust ECC-Based Provable Secure Authentication Protocol With Privacy Preserving for Industrial Internet of Things," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3599-3609, 2018.
[62] Kumar, D., Chand, S. and Kumar, B., 2019. Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines. Journal of Ambient Intelligence and Humanized Computing, 10(2), pp.641-660.
[63] Wang, F., Xu, G. and Xu, G., 2019. A provably secure anonymous biometrics-based authentication scheme for wireless sensor networks using chaotic map. IEEE Access, 7, pp.101596-101608.
[64] Yu, B. and Li, H., 2019. Anonymous authentication key agreement scheme with pairing-based cryptography for home-based multi-sensor Internet of Things. International Journal of Distributed Sensor Networks, 15(9), p.1550147719879379.
[65] Luo, H., Wen, G. & Su, J. Lightweight three factor scheme for real-time data access in wireless sensor networks. Wireless Networks 26, 955-970 (2020).
[66] Shuai, M., Xiong, L., Wang, C. and Yu, N., 2020. A secure authentication scheme with forward secrecy for industrial internet of things using Rabin cryptosystem. Computer Communications, 160, pp.215-227.
[67] Nashwan, S., 2020. AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment. Egyptian Informatics Journal.
[68] Chaudhry, S.A., Yahya, K., Al-Turjman, F. and Yang, M.H., 2020. A secure and reliable device access control scheme for IoT based sensor cloud systems. IEEE Access, 8, pp.139244-139254.
[69] Chaudhry, S.A., Farash, M.S., Kumar, N. and Alsharif, M.H., 2020. PFLUA-DIoT: A Pairing Free Lightweight and Unlinkable User Access Control Scheme for Distributed IoT Environments. IEEE Systems Journal.

[70] Secure Hash Standard, FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. Accessed on April 2017.

[71] D. Johnson, A. Menezes, The Elliptic Curve Digital Signature Algorithm (ECDSA), Technical Report CORR 99-34, Dept. of C & O, University of Waterloo, Canada, August 23, 1999.

[72] Wu, Fan, Lili Xu, Saru Kumari, Xiong Li, Jian Shen, Kim-Kwang Raymond Choo, Mohammad Wazid, and Ashok Kumar Das. "An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment." Journal of Network and Computer Applications 89 (2017): 72-85.