Design of a Multifactor Unidentified Remote End User Authentication Mechanism for IoT Network

Neha Sharma*, Pankaj Dhiman
Department of Computer Science and Engineering, Jaypee University of Information Technology Waknaghat, Solan, H. P., India
E-mail: nehasharma.bu@gmail.com, pankajdhiman12508@gmail.com
*Corresponding author

Keywords: authentication, key agreement, internet of things, wireless sensor networks (WSN)

Received: December 5, 2023

The rapid proliferation of Internet of Things (IoT) devices, coupled with the rollout of advanced 5G networks, has generated significant concerns regarding security breaches. These concerns stem from the expanded attack surfaces that come with improved connectivity, making IoT systems more vulnerable to malicious threats. A crucial strategy to counter these security challenges is the implementation of robust user authentication methods. Despite numerous proposals for multi-factor authentication mechanisms, many of these systems exhibit weaknesses, particularly in their susceptibility to user impersonation attacks and the risks posed by stolen mobile devices. Furthermore, several schemes fail to incorporate essential features such as session key agreements or backup solutions for instances of lost or stolen devices and compromised private keys. To address urgent security challenges in IoT environments, we developed a three-factor user authentication system tailored for low-cost IoT devices. This system tackles critical vulnerabilities while maintaining low computing and communication costs, enhancing security without compromising usability and efficiency.

Povzetek: Raziskava uvaja večfaktorski sistem za avtentikacijo uporabnikov v IoT, ki izboljša varnost, zmanjšuje ranljivosti in zagotavlja nizke računske stroške, hkrati pa omogoča odpornost proti več vrstam napadov

1 Introduction

The Internet of Things (IoT) is a network of nodes with limited resources that are densely distributed throughout environments. IoT requires that related items or objects be intelligent enough to make deft decisions without human intervention. Considering that different architectures and platforms have been used to develop IoT devices, they have unique environments and characteristics that have increased the difficulties this technology presents. This is especially true of intelligent home-based systems Wang et al. [1]. In addition, they are susceptible to security risks. These nodes provide continuous service, regardless of location or time, and are employed in a variety of applications, including healthcare, smart homes, manufacturing, and cities. The launch of the 5G cellular network has increased expectations for a highly interconnected network that facilitates information sharing between portable devices and everyday objects. The misuse of IoT technologies in smart homes can endanger the environment and people's lives. Therefore, it is crucial to focus on security and privacy Park et al [2]. One way to ensure security and privacy is to use authentication protocols to verify the legitimacy of both users and servers before transmitting data. home networks are vulnerable to security flaws due to the use of various wired and wireless mediums and protocols, as well as the difficulty in keeping up with evolving cyber threats. However, ensuring the security of IoT networks is vital in protecting user privacy from potential threats. Robust security measures must be implemented to achieve this, including virtual network security, data security, service availability, and data integrity. User authentication techniques must also adhere to strict security and functional standards to enhance IoT network security. Our proposed scheme is perfect for IoT devices because it offers cost-effective computing and communication capabilities. Additionally, our scheme is highly efficient in enhancing IoT network security, a crucial factor in today's digital landscape, where cyber threats are widespread Ahmed et al [3]. By utilizing our system, users can have peace of mind knowing that their IoT devices are thoroughly safeguarded against possible risks.

(1) User anonymity: The authentication mechanism should maintain user anonymity to safeguard user privacy. In other words, an attacker should be unable to determine the user's identity.

(2) Unlinkability: The system must prevent

attackers from tracking the user's activities, thus ensuring unlinkability and improving user privacy.

(3) Session key agreement: The key used for encrypting and decrypting messages in the authentication system must be fresh while guaranteeing forward secrecy.

(4) Resistance to several attacks: The authentication mechanism must satisfy all essential security objectives and resist known attacks Perrig et al [4].

(5) A secure user authentication method must have countermeasures to prevent attackers from taking control of the IoT network, even if physical memory keys are exposed through side-channel attacks Mishra and Srinivas et al. [5][6]. Revoking is a straightforward and efficient way to prevent it from being used or accessed. If a user loses their private key or it gets stolen, the revocation mechanism can be implemented to issue the user a new key. Recently, several authentication systems have been developed to improve security. Dhillon and Kalra [7] proposed a computationally efficient three factor remote authentication technique suitable for IoT environments. In our analysis, we discovered security flaws in their plan. This paper proposes a new authentication scheme AUSS (Authenticated Unidentified Security Scheme) for IoT networks that addresses these vulnerabilities through cryptanalysis. It adeptly handles the intricate processes of calculating and communicating costs, ensuring seamless interactions across the network while maintaining robust protection against potential vulnerabilities.

1.1 Main contributions of the proposed scheme

1. The user authentication scheme introduced by Dhillon and Kalra was innovative but had security vulnerabilities.
2. The authors addressed these issues by proposing an enhanced scheme that fixes the vulnerabilities and improves security.
3. To ensure the robustness of their proposed scheme, they conducted a comprehensive set of informal and formal security analyses using the random oracle model, BAN logic, and the AVISPA tool.
4. The analysis shows that the proposed scheme resists various known attacks and satisfies all essential security requirements.
5. Additionally, the authors performed a comparative performance analysis, considering the hardware specifications of mobile and sensor devices in a real IoT environment.
6. The proposed scheme is compatible with highly low- cost IoT devices, making it practical for user authentication in IoT scenarios.

Table 1: List of symbols and their descriptions

Symbol	Description
Sn_i	Sensor Node
Mn_i	Mobile Node
Id_i	Mobile device identity
Pw_i	Mobile node's password
Id_i , NS_{ni}	Identities of Sn_i and Id_i
Bio_i	Mn_i biometric
T_x	Timestamp
n_x , r_x	Random numbers
SK	Session key between Mn_i and Sn_i
EK(.) , DK(.)	Symmetric key encryption and decryption
$H(.)$	Hash function
||	Concatenation
$\oplus$	Xor operation
K_{gu}	Private key of Mn_i
K_{gn}	Secret key shared between Sn_i and GW

2 Literature review

Various studies have been conducted on two-step verification methods to improve security and efficiency across network settings [9-11]. The authors of [12] refused IoT's goal to bridge the gap between physical and computer-based systems, to maximize economic welfare and efficiency with minimal human intervention. WSNs and IoT authentication issues are similar. IoT architecture can leverage knowledge from anonymous authentication schemes for WSNs, improving accuracy and efficiency, while reducing the need for human intervention. Lamport et al. [8] Proposed the first password-based authentication scheme, and research into cryptographic technologies, such as symmetric and asymmetric key cryptography and hash functions, was sparked to ensure secure user authentication in WSNs. In this the author Wong et al. [9] introduced the first password-based authentication system for WSNs. However, Das et al. [10] identified security vulnerabilities in that technique as it could not withstand attacks involving multiple users with the same login ID or stolen-verifier attacks.

To improve the security, Das et al. implemented a two-factor authentication strategy for users using the gateway [14][18]. However, later vulnerabilities were discovered in Das' method, and organizations faced several types of security threats, such as attacks against privileged insiders, impersonation, gateway node bypassing, etc. Additionally, Das et al. scheme fails to ensure mutual verification between the gateway and sensor nodes. In response to security concerns with user authentication, Khan and Alghathbar [19] developed an improved two-factor authentication strategy. However, Vaidya et al. [20] discovered that their system was vulnerable to theft and attacks. In 2011, Yeh et al. [21] presented a novel

user authentication method for WSNs that used smart cards. They improved the scheme's security by using elliptic curve cryptography (ECC). However, Xue et al. [22] found that the ECC-based technique required more processing and storage resources. However, Li et al. identified weaknesses in attacks such as offline password guessing, smart card loss, insider, and multiple logged-in users with the same login ID.

Turkanovic et al. [25] proposed an enhanced mutual authentication technique to address security issues, ensuring crucial aspects such as mutual authentication, key agreement, password security, and cost-effectiveness through hash and exclusive-OR (XOR) operations. However, Farash et al. [26] discovered security flaws in Turkanovic et al.'s approach, stating that it does not ensure the sensor node's untraceability or anonymity.

As a solution, Farash et al. [26] suggested a user authentication mechanism for WSNs optimized for IoT to address these security vulnerabilities. Subsequently, Kumari et al. [27] found that the approach described by Farash et al. [26] violates user and sensor-node anonymity and is vulnerable to multiple attacks.

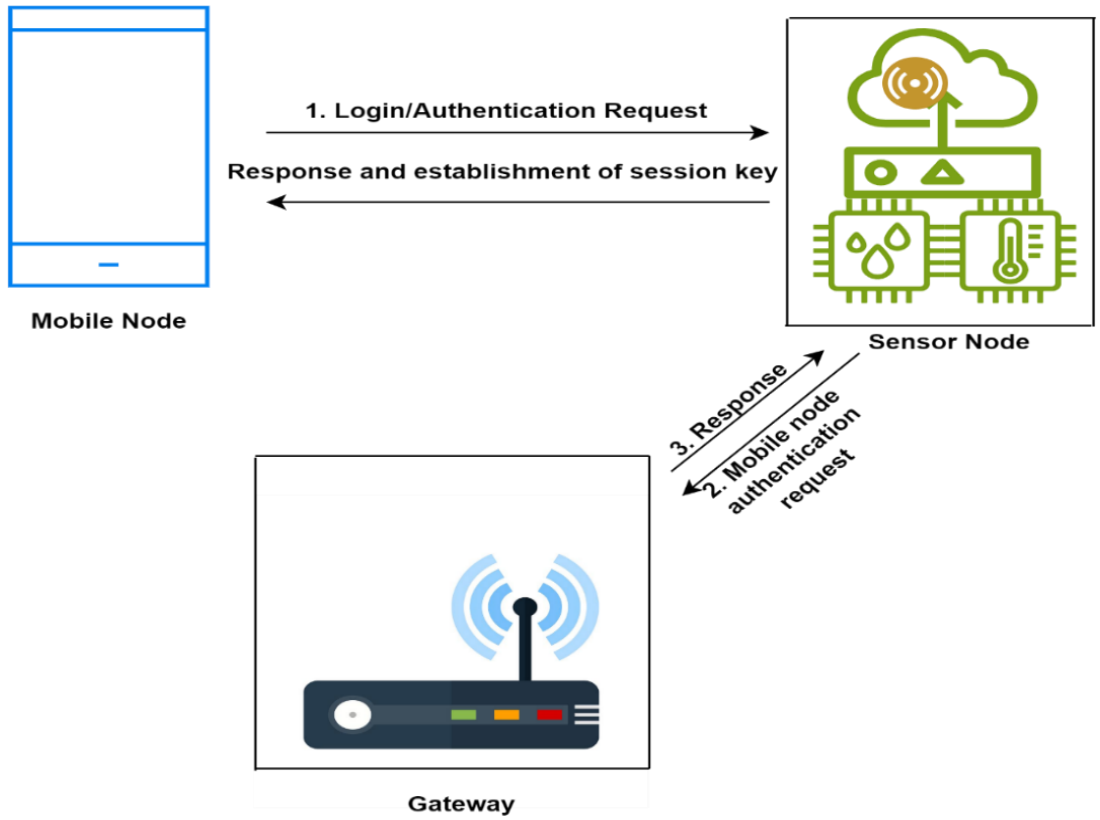

Figure 1: The proposed technique offers a user authentication model for IoT

Dhillon and Kalra's study [7] demonstrate that traditional two-factor authentication methods are not safe in real- world scenarios, such as in the event of a password leak or the loss of a smart device. In response to the IoT network architecture used in the discussed schemes [25-27]. They claimed that their system can withstand offline password guessing, password changes, denial of service attacks, stolen mobile devices, and impersonation assaults. However, it was found that their method is still susceptible to user impersonation attacks using a stolen mobile device and it lacks a session key agreement and revocation plan. Based on the IoT network architecture, they developed a lightweight multi- factor authentication system that utilizes passwords, biometrics, and mobile devices. Their technique can resist password guessing, denial of service attacks, mobile phishing spoofing, etc. Nevertheless, their method lacks a session key agreement and a method for revocation, making it vulnerable to user impersonation attacks and exploitation of stolen mobile devices. In this paper, we assess the security system weaknesses in Dhillon and Kalra's approach [7] and introduce an improved lightweight authentication method suitable for IoT contexts that only utilizes cryptography with symmetric hashing and XOR methods.

3 Preface

3.1 Networking model and authentication mechanism

Various IoT architecture approaches are employed to accomplish security, scalability, and low computing costs. Xue et al. [23] proposed five resource-limited communication techniques. In our scheme, the mobile node Mn_i sends login and authentication requests to Sn_i and N_j to exchange session keys. This two-way authentication is carried out via the gateway GW. The user authentication procedure is explained in Figure 1.

(1) To access the IoT network Mn_i, send a request to Sn_i for login and authentication.
(2) Upon receiving the request message Sn_i, forwards it to GW for Mn_i authentication.
(3) GW is analyzing the message received from Sn_i, verifies Mn_i, and responds to Sn_i.
(4) After Mn_i responds to Sn_i, authentication establishes a session key.

3.2 Bio-Hash functions

Biometric identification is an effective and unique way to address security issues related to individual user credentials, such as passwords and tokens, which can be forgotten or stolen. However, dry or cracked skin can cause slight variations in biometric properties with each input or dust on the impression sensors, leading to high false rejection rates.

Jin et al. [24] developed a two-factor authentication (2FA) system in 2004 that utilises fingerprint traits unique to each user and inner products of tokenised pseudo-random integers. They created a biohash code, a unique and compact code set for every user. A user-specific token of pseudo-random digits was employed to convert the random binary string into a biometric characteristic. Biohash technology has been proposed in papers [30, 31] due to its suitability for low-capacity devices, making it a practical choice for biometrics-based multi-factor authentication schemes [32]. An anonymous user authentication scheme for IoT environments featuring three factors and four phases has been developed.

4 Proposed scheme

We propose a three-factor anonymous user authentication technique for IoT contexts. The proposed scheme consists of four parts (1) registration, (2) login and authentication, (3) password change phase (4) revocation phase. Table 1 lists all the symbols used in this paper.

Table 2: The phase of user registration for the proposed method

Mobile Node Mn_i	Gateway (GW)
Select Id_i, Pw_i, Bio_i $PwB_i = h(Pw_i \parallel H(Bio_i))$ $Mid_i = h(Id_i \parallel h(Bio_i))$ $\langle Id_i, PwB_i, Mid_i \rangle$ →	Generate random numbers r_{gu} and r_d $Rid_i = E_{K_G}(Id_i)$ $Pid_i = E_{K_a}(Id_i \parallel r_d)$ $X_i = h(Id_i \parallel PwB_i)$ $Y_i = h(Id_i \parallel PwB_i \parallel r_{gu}) \oplus h(K_{gu} \parallel Id_i)$ $\langle PID_i, X_i, Y_i, r_{gu} \rangle$ Store into the mobile device ←

.

4.1 Registration of user

The registration phase for Mn_i is illustrated in table 1 and 2 and includes the following steps:

(a) Mn_i selects Id_i, Pw_i, and Bio_i and calculates $PwB_i = h(Pw_i \parallel H(Bio_i))$and $Mid_i = h(Id_i \parallel h(Bio_i))$.

(b) Mn_i sends $< , PwB_i, Mid_i >$ to GW via the secure channel.

(c) GW randomly selects numbers r_{GU} and , and computes $Rid_i = E_{kg}(Id_i), Pid_i = E_{kg}(Id_i \parallel r_{gu}), x_i = h(Id_i \parallel PwB_i)$, and $y_i = h(Id_i \parallel PwB_i \parallel r_{gj}) \oplus h(K_{gu} \parallel Id_i)$. A pair is stored by GW (Rid_i) in the database.

(d) GW sends $< Pidi, x_i, , r_{gu} >$ to Mn_i.

(e) In the final step, Mn_i saves the parameters received $< Pid_i \ , >$, in the mobile device.

4.2 Registration of IoT node

Figure 3 depicts the registration step of the proposed strategy for the sensor node Nj, which includes the following procedures.

(a) Sn_i randomly selects numbers r_j and computes $Mp_j = h(K_{gn} \| r_j \| Nid_j)$ and $Mi_j = r_j \oplus h(Nid_j \parallel K_{gn})$.

(b) Sn_i Sends $< Nid_j, Mp_j, Mi_j >$ to GW via the public channel.

(c) GW Computes $r_j^* = Mi_j \oplus h(Nid_j \parallel K_{gn})$ and $MP_j^* = h(K_{gn} \| r_j^* \| Nid_j)$ and checks whether Mp_j^* and Mp_j are the same. If they are, GW computes $x_j = h(Nid_j || K_{gn})$ and $y_j = x_j \oplus Mp_j^*$.

(d) GW sends $< y_j >$ to Sn_i.

(e) Sn_i Stores $< y_j >$ i memory space.

Table 3: Phase of registration for the proposed method's IoT node

Sensor Node Sn_i	**Gateway (GW)**
Generate a random number, r_j $Mp_j = h(K_{gn} \| r_j \| Nid_j)$ $Mi_j = r_j \oplus h(Nid_j \| \| K_{gn})$ $< Nid_j, Mp_j, Mi_j >$ ⟶	$r_j^* = Mi_j \oplus h(Nid_j \parallel K_{gn})$ $Mp_j^* = h(K_{gn} \| r_j^* \| Nid_j)$ $Mp_j{}^*? = Mp_j$ $x_j = h(Nid_j \parallel K_{gn})$ $y_j = x_j \oplus Mp_j^*$ $< y_j >$ ⟵

Table 4: Login and authentication phase

Mobile Node MN_i	**Sensor Node N_j**	**Gateway Node**
Input Id_i, Bio_i, Pw_i $PwB_i = h(Pw_i \parallel H(Bio_i))$ $x_i^* = h(ID_i \parallel PwB_i)$ $x_i^* \stackrel{?}{=} x_i$ Generate n_i $A_i = y_i \oplus h(Id_i \| PwB_i \| r_{gu})$ $UN_i = h(A_i \| Pid_i \| n_i)$ $UZ_i = n_i \oplus A_i$ $M_1 = \langle Pid_i, Un_i, Uz_i, T_1 >$	Check $T_{\text{fresh}} - T_1 \leq \Delta T$ Generate n_j $x_j = y_j \oplus h(K_{gn} \| r_j \| Nid_j)$ $A_j = h(x_j) \oplus n_j$ $B_j = h(x_j \parallel n_j)$ $M_2 = < M_i, Nid_j, A_j, B_j >$ $F_j^* = G_j \oplus x_j$ $n_i^* = R_{ij} \oplus n_j$ $H_j^* = h(x_j \| \| n_j \| n_i^* \| F_j^*)$ $H_j^* \stackrel{?}{=} H_j$ Choose m_j $L_j = h(Nid_j \parallel n_i^*) \oplus m_j$ $SK_{ji} = h(F_j^* \| n_i^* \| m_j)$ $SV_j = h(Sk_{ji} \| T_1 \| T_2)$ $M_4 = < Pid_i^{\text{new}}, L_j, Sv_j, T_2 >$	$x_j^* = h(Nid_j \parallel K_{gn})$ $n_j^* = h(x_j^*) \oplus A_j$ $B_j^* = h(x_j^* \parallel n_j^*)$ $B_j^* \stackrel{?}{=} B_j$ $< Id_i, r_d >= D_{K_G}(Pid_i)$ $A_i^* = h(ID_i \parallel K_{gu})$ $n_i^* = Uz_i \oplus A_i^*$ $UN_i^* = h(A_i^* \| Pid_i \| n_i^*)$ $UN_i^* \stackrel{?}{=} UN_i$ Generate r_D^{new} $F_j = h(Id_i \parallel n_i^*)$ $G_j = F_j \oplus x_j^*$ $R_{ij} = n_j^* \oplus n_i^*$ $H_j = h(x_j^* \| n_j^* \| n_i^* \parallel F_j)$ $PID_i^{\text{new}} = E_{K_G}(Id_i, r_d^{\text{new}})$ $M_3 =< Pid_i^{\text{new}}, G_j, R_{ij}, H_i >$
Check $T_{\text{fresh}} - T_2 \leq \Delta T$ Gateway GW		

$m_j^* = L_j \oplus h(Nid_j \parallel n_i)$ $Sk_{ij} = h(h(Id_i \parallel n_i)\|n_i\|$ $Sv_i = h(Sk_{ij}\|T_1\|T_2)$ $Sv_i \stackrel{?}{=} Sv_j$		

4.3 Login and authentication phase

MN_i and Sn_i mutually authenticate with the help of GW to create a session key. As shown in table 4 the login and authentication phases:

(a) Mn_i enters Id_i, Pw_i, and Bio_i, computes $PwB_i = h(Pw_i \parallel h(Bio_i))$ and $x_i^* = h(Id_i \parallel PwB_i)$, and checks whether x_i^* and x_i are the same. If they are not, Mn_i terminates this phase; otherwise, Mn_i random number produced and computes $A_i = y_i \oplus h(Id_i\|PwB_i\|r_{gu}), Un_i = h(A_i\|Pid_i\|n_i)$, and $Uz_i = n_i \oplus A_i$.

(b) Mn_i Sends the request,$M_1 =< Pid_i, Un_i, Uz_i, T_1 >$ to Sn_i.

(c) Sn_i computes checks T_1's freshness, generates n_j and computes T_1 freshness and calculates $x_j = y_j \oplus h(K_{gn} \parallel r_j||Nid_j)$, $A_j = h(x_j) \oplus n_j$and $B_j = h(x_j \parallel n_j)$.

(d) Sn_i Sends the message, $M_2 =< M_1, Nid_j, A_j, B_j >$ to GW.

(e) Upon reception of the message from Sn_i, GW calculates $x_j^* = h(Nid_j \parallel K_{gn}), n_j^* = h(x_j^*) \oplus A_j$, and $B_j^* = h(x_j^* \parallel n_j^*)$ and examine whether B_j^* and B_j are similar. If they are no identical, GW ends this phase; else, GW gets MN_i 's $< Id_i, r_d >$ by applying a key K_G to decode Pid_i and calculating $A_i^* = h(Id_i \parallel K_{gj}), n_i^* = Uz_i \oplus A_i^*$, and $UN_i^* = h(a_i^*\|Pid_i\|n_i^*)$ and checks whether UN_i^* and UN_i are similar. GW ends this phase if they aren't.; otherwise, GW generates r_D^{new} and computes $F_j = h(Id_i \parallel n_i^*), G_j = F_j \oplus x_j^*, R_{ij} = n_j^* \oplus n_i^*, H_j = h(x_j^*\|n_j^*\|n_i^* \parallel F_j)$, and$PID_i^{\text{new}} = E_{kg}(Id_i, r_d^{\text{new}})$.

(f) GW sends $M_3 =< Pid_i^{\text{new}}, G_j, R_{ij}, H_j >$ to Mn_i.

(g) Sn_i Computes $F_j^* = G_j \oplus X_j$, $n_i^* = R_{ij} \oplus n_j$ and $H_j^* = h(x_j\|n_j\|n_i^* \parallel F_j^*)$ and checks whether $H_j^* = H_j$. If N_j fails to do so, the phase terminates. Otherwise, N_j selects a random value m_j and calculates, $L_j = h(Nid_j \parallel n_i^*) \oplus m_j, Sk_{ji} = h(F_j^*\|n_i^*\|m_j)$ and $Sv_j = h(Sk_{ji}\|T_1\|T_2)$.

(h) N_j Sends $M_4 =< Pid_i^{\text{new}}, L_j, Sv_j, T_2 >$ to Mn_i.

(i) Mn_i Checks whether $T_{\text{fresh}} - T_2 \leq \Delta T$ and computes $m_j^* = L_j \oplus h(Nid_j \parallel n_i)$, $Sk_{ij} = h(h(I_i \parallel n_i)\|n_i\|m_j^*)$, and $Sv_i = h(Sk_{ij}\|T_1\|T_2)$. If Sv_i and Sv_j are the same, Mn_i and Sn_i produce the same session key successfully.

4.4 Password change phase

Mn_i updates their password on their mobile device during this phase. The details are as follows:

(a) Mn_i inputs $Id, Pw_i^{\text{dd}}, Pw_i^{\text{new}}$, and Bio_i, and computes $PWB_i^{\text{old}} = h(Pw_i||h(Bio_i))$ and $x_i^* = h(Id_i \parallel PwB_i^{\text{old}})$.

(b) Mn_i Checks whether x_i^* and x_i are the same. If they are not, Mn_i terminates this phase. Otherwise, Mn_i computes $A_i = y_i \oplus h(ID_i||PwB_i^{dd}||r_{gj}), PwB_i^{\text{new}} = h(PW_i^{\text{new}} \parallel H(Bio_i))$, $x_i^{\text{new}} = h(Id_i \parallel PwB_i^{\text{new}})$, and $y_i^{\text{new } i} = h(ID_i\|Pw^iB_i^{\text{new}} \|r_{gu}) \oplus A_i \oplus y_i$.

(c) Finally, Mn_i replaces the old x_i^{old} and y_i^{old} with x_i^{new} and y_i^{new}, respectively.

4.5 Revocation phase

Mn_i Incorporates a revocation technique that allows the secret parameters to be recovered by the mobile device.

(a) When a user wants to update or renew their secret parameter, they will input their previous identity Id_i^{old}, new identity Id_i^{new} new password Pw_i^{new} and Bio_i into their mobile device. Mn_i then computes $PwB_i^{\text{new}} = h(Pw_i^{\text{new}} \parallel H(Bio_i))$, $Mid_i^{\text{old}} = h(Id_i^{\text{old}} \parallel$

$H(Bio_i)\big)$, and $Mid_i^{\text{new}} = h\big(Id_i^{\text{new}} \parallel H(Bio_i)\big)$.

(b) Mn_i sends the revocation request message, $< Id_i^{\text{old}}, Id_i^{\text{new}}, Mid_i^{\text{old}}, Mid_i^{\text{new}}, PwB_i^{\text{new}} >$, to GW through a reliable channel.
(c) GW calculates $RID_i^{\text{old}} = E_{K_G}\big(Id_i^{\text{old}}\big)$ The system first verifies the identity of $Mn_i$and then searches for a pair. $(Rid_i^{\text{old}}, Mid_i^{\text{old}})$ to locate a registered user in the database. If the pairs (Rid_i, Mid_i) and $\big(RID_i^{\text{old}}, MID_i^{\text{old}}\big)$ are equal, GW produces new random numbers r_d^{new} and r_{gu}^{new}, computes $Pid_i^{\text{new}} =$

$E_{K_G}(Id_i, r_d^{\text{new}}), Rid_i^{\text{new}} = E_{kg}(Id_i^{\text{new}}),\ x_i^{\text{new}} = h(Id_i \parallel PwB_i^{\text{new}})$, and $y_i^{\text{new}} = h\big(Id_i||PwB_i^{\text{new}}||r_{gj}^{\text{new}}\big) \oplus h\big(K_{gu}||Id_i^{\text{new}}\big)$, and stores the new pair $(Rid_i^{\text{new}}, Mid_i^{\text{new}})$ in the database.

(d) GW sends $< Pid_i^{\text{new}}, x_i^{\text{new}}, y_i^{\text{new}}, r_{GJ}^{\text{new}} >$ to Mn_i.
(e) Mn_i the parameters obtained are saved in the mobile device.

5 BAN logic authentication proof

In this section, we utilized Burrows-Abadi-Needham (BAN) logic [51] to demonstrate that Mn_i and Sn_imutually authenticate each other correctly and that their distributed session key is up-to-date. BAN logic is a formal system that verifies the trustworthiness of every entity involved in an authentication protocol based on the source of communications, freshness, and reliability. Researchers also used extensively for evaluating the security of algorithms used in cryptography [51–52]. The following are the fundamental notations of BAN logic:
(1) $U \bowtie C$: U sees condition C.

(2) $U \mid\equiv C$: Condition C is U trust
(3) $\sharp(C)$: It creates an entirely fresh C.
(4) $U \mid\sim C$: U describes the circumstance C.
(5) $\overset{K}{\leftrightarrow} S$: U and S share a secret key K.
(6) $U \Rightarrow C$: Condition C is handled by U.
(7) $(C_K$: C is encryption with key K.

(1) We use the five BAN logic principles stated below to show the mutual authentication of the proposed method. That U notices the C connected to K, that S shares the key K with S, and that U trusts S after bringing up C.

(2) Rule 2: The rule of once-verification: $\frac{U]=\#(C), U|=S\sim C}{U(\equiv)=C}$: If U believes in C's freshness and S believes in C, then U believes S believes in C.

(3) Rule 3: Trust rule: $\frac{U=C, U|=M}{A|=(C,M)}$: If User believes C and M, then (C, M) is also believed by U.

(4) Rule 4: Freshness-concatenation rule: $\frac{U_{\parallel}=\sharp(C)}{A_{\parallel}=+(C,M)}$: If U has faith in C's freshness, then U has jurisdiction over C's freshness as well. Likewise, if U has faith in S's confidence in condition C, then U also has faith in C. Through mutual authentication, we aim to establish a session key between Mn_i and n_j. To do this, we must complete the four tasks listed below.
(1) Goal 1: $MN_i \mid\equiv \left(Mn_i \overset{SK}{\leftrightarrow} Sn_i\right)$
(2) Goal 2: $Sn_i \mid\equiv \left(Mn_i \overset{SK}{\leftrightarrow} Sn_i\right)$
(3) Goal 3: $Mn_i|\equiv Sn_i| \equiv \left(Mn_i \overset{SK}{\hookrightarrow} Sn_i\right)$
(4) Goal 4: $Sn_i|\equiv Mn_i| \equiv \left(MN_i \overset{SK}{\leftrightarrow} Sn_i\right)$
The proposed scheme's four messages can be transformed into ideal forms.

(1) Using $M_1 =< Pid_i, Un_i, Uz_i, T_1 \gg,\ Mn_i \rightarrow Sn_i: Un_i = h(A_i \| Pid_i \| n_i), Uz_i = n_i \oplus A_i$. This has been lowered as $G_1 : (PID_i, A_i, T_1)_{n_i}$
(2) Using $M_2 =< M_1, Nid_j, A_j, B_j >, N_j \rightarrow GW: A_j = h(x_j) \oplus$

Sn_i, $B_j = h(x_j \parallel Sn_i)$. This is reduced as $M_{SG}: (M_1, Nid_j, Sn_i)x_j$
(3) Using $M_3 =< PID_i^{\text{new}}, G_j, R_{ij}, H_j >, GW_i \rightarrow Sn_i: G_j = F_j \oplus x_j^*,\ R_{ij} = n_j^* \oplus n_i^*,\ H_j = h(x_j^*||n_j^*\|n_i^*\|F_j)$. This is reduced as MSG $_3: (F_j, n_j, n_i, K_{gn})x_j$
(4) Using $M_4 =< Pid_i^{new}, L_j, Sv_j, T_2 >, Sn_i \rightarrow Mn_i:\ L_j = h(Nid_j \parallel n_i^*) \oplus m_jt, Sv_j = h(SK_{ji}\|T_1\|T_2)$. This decreases as: $\text{MSG}_4: (\text{Pid}_i, \text{m}_j, \text{T}_1, T_2)_{m_i}$

We define the following assumptions to derive the proposed scheme's goals.

(1) $A_1: Mn_i \mid\equiv \sharp(T_1)$
(2) $A_2: Sn_i \mid\equiv \sharp(Sn_i)$
(3) $A_3: GW \mid\equiv \sharp(K_{CN})$
(4) $A_4: Sn_i \mid\equiv \pm(T_2)$
(5) $A_5: Sn_i \mid\equiv \left(Sn_i \overset{n_i}{\leftrightarrow} Mn_i\right)$
(6) $A_6: CW \mid\equiv \left(CW \overset{x_j}{\rightleftarrows} Sn_i\right)$
(7) $A_7: Sn_i \mid\equiv \left(Sn_i \overset{x_j}{\longrightarrow} CW\right)$
(8) $A_{\text{B}}: Mn_i \mid\equiv \left(Mn_i \overset{\pi_i}{\leftrightarrow} Sn_i\right)$
(9) $A_g: Mn_i \mid\equiv Sn_i \Rightarrow \left(Mn_i \overset{\mathcal{K}}{\leftrightarrow} Sn_i\right)$
(10) $A_{10}: Sn_i \mid\equiv Mn_i \Rightarrow \left(Mn_i \overset{\leftrightarrow}{\leftrightarrow} Sn_i\right)$

The following describes the primary proof that the proposed method is based on BAN logic rules, messages, and premises.

(1) Through MSG_1, we get $V_1: Sn_i \triangleleft (Pid_i, A_i, T_1)n_i$

(2) Through A_5 and Rule 1 , we get V_2: $Sn_i|\equiv Mn_i| \sim (Pid_i, A_i, T_1)_{m_i}$
(3) Through A_1 and Rule 4 , we get V_3: $Sn_i \equiv \sharp(Pid_i, A_i, T_1)_{n_j}$
(4) Through V_1, V_2 and Rule 2, we get V_4: $Sn_i|\equiv Mn_i| \equiv (Pid_i, A_i, T_1)n_i$
(5) Through MSG_2, we get V_5 : CW $\triangleleft$ $(M_1, Nid_j, Sn_i)x_j$
(6) Using A_6 and Rule 1 , we get V_6: $GW|\equiv Sn_i| \sim (M_1, Nid_j, Sn_i)x_j$
(7) ThroughA_2 and Rule 4 , we get V_7: $GW \equiv \sharp(M_1, Nid_j, sn_i)x$.
(8) Through V_5, V_6 and Rule 2, we get V_8: $GW|\equiv Sn_i| \equiv (M_1, Nid_j, Sn_i)x_j$

(9) Through MSG_3. we get V_g: $Sn_i \triangleleft (F_j, n_j, n_i, K_{cn})x_j$
(10) Through A_7 and Rule 1, we get V_{10}: $Sn_i| \equiv GW| \sim (F_j, Sn_i, n_i, K_{cn})x_1$.
(11) From A_3 and 4 , we get V_{11}: $Sn_i \equiv \pm(F_j, Sn_i, n_i, K_{cn})x_j$
(12) From V_9, V_{10} and Rule 2, we get V_{12}: $Sn_i| \equiv dW| \equiv (F_j, Sn_i, n_i, K_{gn})x_j$
(13) Through MSG_4. We obtain V_{13}: $Mn_i \triangleleft (Pid_i, m_j, T_1, T_2)_{m_i}$ (14) Through A_8 and Rule 1 , we get V_{14}: $Mn_i|\equiv Sn_i| \sim (Pid_i, m_j, T_1, T_2)_{n_i}$
(15) Through A_4 and Rule 4 , We obtain V_{15}: $Mn_i \equiv \sharp(Pid_i, m_j, T_1, T_2)_{m_i}$

(16) From $V_{13}.V_{14}$ and Rule 2 , we get V_{16}: $Mn_i \equiv Sn_{i_j}| \equiv (Pid_i, m_j, T_1, T_2)_{n_i}$
(17) From V_{12}, V_{16}, and $SK = h(F_j \| n_i \| m_j)$. we get V_{17}: $Mn_i \equiv (Mn_i \overset{SK}{\leftrightarrow} N_j)$ (Goal1)
(18) From V_4, V_8, and $SK = h(h(Id_i \| \| n_i) \| n_i \| m_j)$, we get V_{18}: $Sn_i \equiv (Mn_i \overset{\leftrightarrows}{\leftrightarrow} Sn_i)$ (Goal2)
(19) From A_9, V_{17} and Rule 5, we get V_{19}: $Mn_i| \equiv Sn_i| \equiv (Mn_i \overset{SK}{\leftrightarrow} Sn_i)$(Goal3)
(20) From A_{10}, V_{18} and Rule 5 , we get V_{20}: $Sn_i| \equiv Mn_i| \equiv$

$(Mn_i \overset{sK}{\leftrightarrow} Sn_i)$(Goal4)

We accomplished goals 1, 2, 3, and 4 are listed above. We see that Mn_i and Sn_i create a session key by means of safe mutual authentication.

```
Role alice (Ui, GWN. SNj: agent,
H: hash func.
SKuigwn: symmetric_key,
Snd, Rcv: channel(dy))
played by Ui
def= local State : nat,
IDi, IDsnj, K, PWi, Bi, T1, T2, T3: text,
Xs, EKi. Ki, Request, R, RPWi : text,
Gen, Rep: hash, func
const alice server_t1, server_bob_t2,
bob_ alice_t3, sub1, sub2, sub3, sub4 : protocol_id
init State := 0
transition
1. Stale = 0 /\ Rcv(start) =|>
% Registration phase
State' = 1 A K'= new()
/\ secret({PWi,Bi,K'),sub1 Ui)
/\ secret(EKi,sub2,{Ui,GWN})
/\ RPWi'= H(IDi.PWi.K')
% Ui sends login message to GWN securely
/\ Snd({IDi.RPWi'.EKi}.SKuigwn)
% Ui receives the smart card from GWN securely
2. State = 1 /\ Rcv ((H.Gen. Rep.H(xor(IDi.H(Xs)))_SKuigwn) =|>
% Login phase
State' := 2 /\ secret(Xs,sub3,GWN)
% Ui sends the login message to the GWN
/\ Snd(IDi.Request)
% Authentication and key agreement phase
% Ui reccives the message <R> from GWN
3. State = 2 /\ Rcv(R') =|>
State' = 3 /\ T1' := new()
% Ui sends the message <E_eki(R,T1,IDsnj)> to GWN
/\ Snd(R'.T1'.IDsnj}_ EKi)
% Ui has freshly generated the value T1 for GWN
/\ witness(Ui, GWN ,alice_server_ti, TI')
% Ui receives the message from sensor node SNj
2. State = 3 /\ Rcv (H {H(H (IDsnj.H (xor (IDi,H(Xs)))).
IDi.IDsnj.T1'.T3').T3')) =|>
% UI's acceptance of the value T3 generated for Ui by SNj
State':= 4 /\ request(SNj, Ui, bob_alice_t3, T3')
end role
role bob (Ui, GWN, SNj: agent,
H: hash_func,
SKuigwn: symmetric_key,
Snd, Rcv: channel(dy))
played_by SNj
def=
local State: nat,
IDi, IDsnj, K, PWi, Bi, TI, T2, T3: text,
Xs, EKi, Kj, Request, R, RPWi: text,
Gen, Rep: hash_func
const alice_server_t1, server_bob t2
```

```
bob_alice_t3, sub1, sub2, sub3, sub4: protocol_id
init State := 0
transition
% Authentication and key agreement phase
% Receive the message from the GWN
1. State = 0 /\ Rcv(IDi. (IDi.IDsnj.TI'.
T2'.H(IDsnj.H(xor(IDi,H(Xs))))] _ Kj)=|>
State': = 1 /\ T3' := new()
/\ secret((PWi,Bi,K),sub,Ui)
/\ secret(EKi,sub2,{Ui, GWN})
/\ secret(Xs,sub3,GWN)
/\ secret(Kj,sub4, {GWN,SNI})
% Send the message to Ui
/\ Snd(H(H(H (IDsnj.H(xor(IDi,H (Xs))))).
IDi.IDsnj,TI'.T3').T3'))
% SNj has freshly generated the value T3 for SNj
/\ witness(SNj.Ui,bob_alice_t3.T3')
% SNi's acceptance of the value T2 generated for SNj by
GWN
/\ request(GWN, SNj, server_bob_t2, T2')
end role
role server (Ui, GWN, SNj: agent,
H: hash_func,
SKuigwn: symmetric_key,
Snd, Rcv: channel(dy))
played_by GWN
def=
local State: nat,
IDi, IDsnj, K, PWi, Bi, T1, 12, T3: text,
Xs, EKi, KJ, Request, R, RAWi: text,
Gen, Rep: hash_func
const alice_server_t1, server_bob_t2,
bob_alice_t3, sub1, sub2, sub3, sub4 : protocol_id
init State := 0
transition
end role
% Registration phase
% GWN receives login message from UI securely
1. State = 0 /\ Rcv((IDi.H(IDi.PWi.K').EKi)_SKuigwn)=|>
State' := 1 /\ secret (PWi,Bi,K'},sub,Ui)
% GWN sends the smart card to Ui securely
/\ Snd({H.Gen.Rep.H(xor(IDi,H(Xs)))]_SKuigwn)
% Login phase: receive the login request message from Ui
2. State = 1 /\ Rcv(IDi.Request)=|>
State': = 2 /\ R' = new()
/\ secret(EKi,sub2, {Ui, GWN})
/\ secret(Xs,sub3,GWN)
/\ secret(Kj,sub4, {GWN,SNj})
% Authentication and key agreement phase
% GWN sends the message to Ui
/\ Snd(R')
end role
```

Figure 2: Role for user and gateway node

6 AVISPA tool simulation for formal security verification

This section presents the formal security verification of the AUSS scheme using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. AVISPA has four back ends, but only the methods for OFMC back-end analysis are considered in this paper. An HLPSL is carried out to evaluate the security resistance to common attacks [39]. The CAS+ specifications are converted into HLPSL in AVISPA using the SPAN animator tool. In SPAN, the intruding mode creates a message sequence chart (MSC). Researchers and academics often use AVISPA or SPAN tools to confirm the security analysis of the design protocol [40].

7 Performance evaluation

In our evaluation we regarded the mobile node and gateway as computing environments in order to minimize the execution time of cryptographic procedures. For each cryptographic execution time, we referred to the results of experiments conducted on the sensor node by Abbasinezhad-Mood and Nikooghadam [50].

Our measurements, along with Abbasinezhad-Mood and Nikooghadam's [50] experiments, reveal the cryptographic times for the mobile node, sensor node, and gateway. We examined the 128-bit Advanced Encryption Standard (AES) algorithm (Ts), the 160-bit hash function (Th), and the 320-bit Elliptic Curve Cryptography (ECC) (Te). The XOR operation was not considered in our analysis due to its negligible impact. We measured the cryptographic execution times on two computing environments: a mobile node and a gateway, using data from Abbasinezhad-Mood and Nikooghadam [50]. The specifications are as follows:

1. Mobile Node: Galaxy Note 9 with an octa-core processor (2.7GHz + 1.7GHz), 8 GB of memory, running Android 9.0.
2. Sensor Node: LPC1768 device with an ARM Cortex-M3 processor (up to 100 MHz), 512 kB flash memory, and 64 kB SRAM.
3. Gateway: Intel(R) Pentium(R) processor G4600 (3.60 GHz), 8 GB of memory, running Windows 10.

The cryptographic times are as follows:

(1) Mobile node: $T_e \approx 29.48\mu s$, $T_s \approx 76.2\mu s$, and $T_h \approx 106.38\mu s$
(2) Sensor node: $T_e \approx 1263\mu s$ and $T_h \approx 15.5\mu s$
(3) Gateway: $T_e \approx 2226\mu s$, $T_s \approx 5.4097\mu s$, and $T_h \approx 4.9465\mu s$

The results show that the Turkanovic et al. scheme [25] has lower computational complexity but it is vulnerable to attacks, as noted by Farash et al. [26]. Our method has lower computational costs compared to those of Das et al. [42], Chang et al. [43], Yang et al. [44], and Wu et al. [46]. The system by Banerjee et al. [45] ranks second but lacks a revocation step. We also compared communication costs during the login and authentication phases. Our proposed scheme has a communication cost of 2112 bits, which is higher than Chang et al.'s approach but still more secure. Using hardware models relevant to real IoT environments, we found that our scheme's computation and transmission costs are slightly higher than some alternatives. Its reliance on XOR and hash operations makes it suitable for low-cost IoT devices while fulfilling all security requirements, thus making it applicable in various IoT scenarios. Figure 2 represents the role of user and gateway note. Figure 3 represents role of session and environment and figure 4 shows OMFC results. Table 5 represents the functionality and security comparison of our scheme with the existing scheme. Table 6 and figure 5 shows the comparison of communication cost of our scheme with the existing scheme. Table 7 and figure 6 represents the comparison of computation cost of our scheme with another scheme. Utilising the approach explained in [53,54], we assessed the communication expenses associated with the login and authentication phases. We presume that the lengths of the identity, timestamp, and random number values are 128, 32, and 64 bits, respectively. The symmetric key encryption, elliptic multiplication operation, and hash function generate 256, 360, and 160 bits, respectively.

```
role session(Ui, GWN,SNj: agent,
% H is hash function
H: hash_func,
SKuigwn: symmetric_key)
def=
local US, UR, SS, SR, VS, VR: channel (dy)
composition
alice(Ui, GWN, SNj, H, SKuigwn, US, UR)
/\ server(Ui, GWN, SNj, H, SKuigwn, SS, SR)
/\ bob(Ui, GWN, SNj, H, SKuigwn, VS, VR)
end role
role environment)
def=
const ui, gwn, snj: agent,
h, gen, rep: hash_func,
skuigwn: symmetric_key,
idi, idsnj, t1, t2, t3 : text,
alice_server_tl, server_bob_t2,
bob_alice_13, sub1, sub2,
sub3, sub4 : protocol_id
intruder_knowledge = (idi,h,gen,rep,t3 )
composition
session (ui, gwn, snj, h, skuigwn)
session(ui, gwn, snj, h, skuigwn)
/\ session(ui, gwn, snj, h, skuigwn)
end role
```

Figure 3: Role for session and environment

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/span/span/testsuite/results/AUSS.if
GOAL
as specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.14s
visitedNodes: 16 nodes
depth: 4 plies
```

Figure 4: OFMC output

Table 5: Comparison functionality and security attribute

ATTACKS	UAA	UUA	SMDA	MA	SKAA	UIA	RA	UVA	SVA	PIA	PCA	FSA	SNIA	RPA
[7]	✓	×	×	✓	✓	×	×	✓	✓	✓	✓	✓	✓	×
[25]	✓	×	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
[42]	✓	×	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	×
[43]	✓	×	×	✓	×	✓	✓	×	✓	✓	✓	×	✓	×
[44]	×	×	×	✓	-	✓	✓	×	×	✓	✓	✓	✓	×
[45]	✓	×	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	×
[46]	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×
AUSS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×

Table 6: Comparison of the communication cost

Scheme	[7]	[25]	[42]	[43]	[44]	[45]	[46]	AUSS
MN(User)	832	672	672	512	864	800	864	480
SN	1760	1440	1184	1024	1728	2080	1408	1472
GW	576	576	512	512	1024	320	320	640
Messages	4	4	4	4	4	4	4	4
Total(bits)	2880	2688	2368	2048	3712	3200	2592	2112

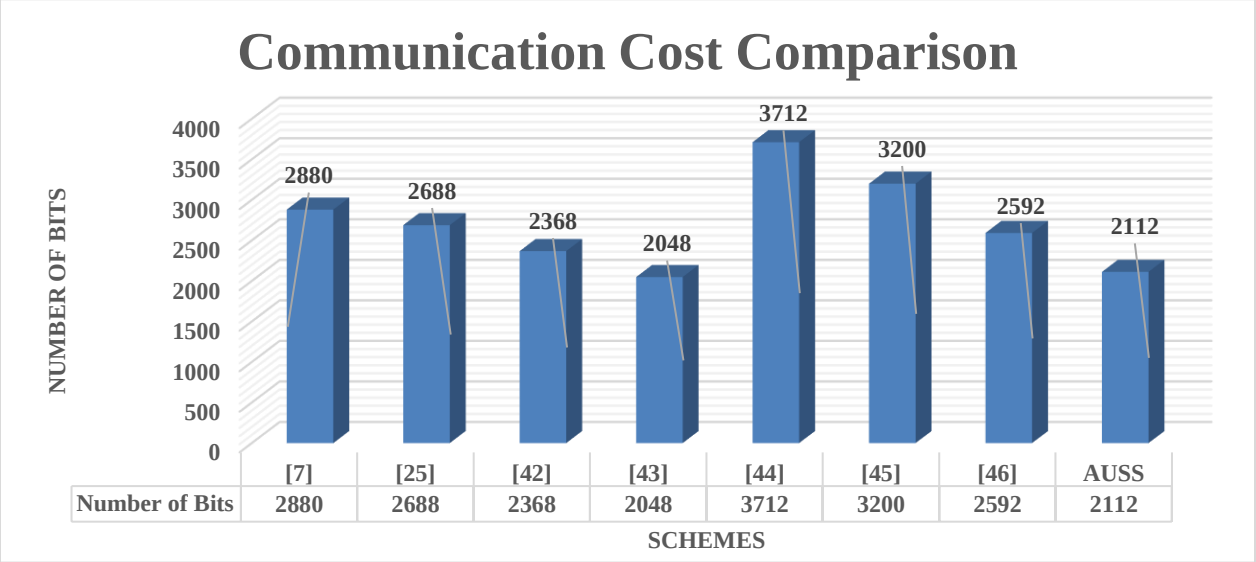

Figure 5: Comparison of Communication cost

Table 7: Comparison of computation

Scheme	[7]	[25]	[42]	[43]	[44]	[45]	[46]	AUSS
MN(User)	$9T_h$	$7T_h$	$8T_h + 2T_e$	$7T_h + 2T_e$	$16T_h$	$9T_h$	$11T_h$	$9T_h$
SN	$6T_h$	$5T_h$	$9T_h + 1T_e$	$5T_h + 2T_e$	$16T_h$	$6T_h$	$5T_h$	$7T_h$
GW	$7T_h$	$7T_h$	$10T_h$	$9T_h$	$20T_h$	$6T_h$	$15T_h$	$8T_h + 2T_s$
Time	$\approx 1085\mu s$	$\approx 856\mu s$	$\approx 1323\mu s$	$\approx 2585\mu s$	$\approx 2049\mu s$	$\approx 1080\mu s$	$\approx 1321\mu s$	$\approx 1115\mu s$

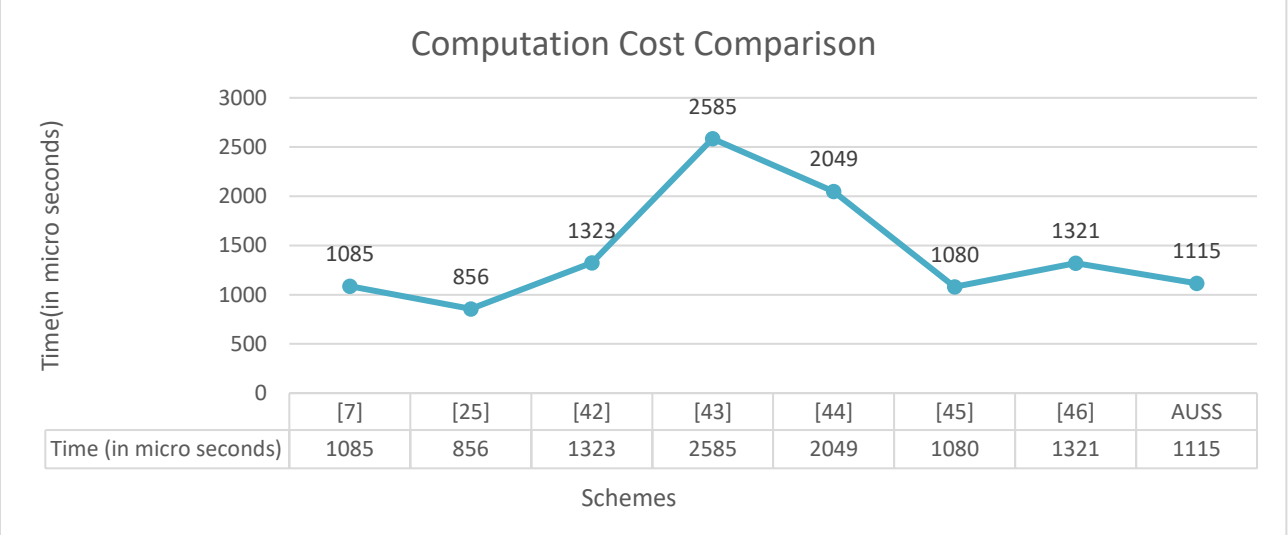

Figure 6: Comparison of computation cost

8 Conclusion

Our research paper presents a significant breakthrough in user authentication techniques. We identified several security flaws in the user authentication method developed by Dhillon and Kalra. In response to these issues, we propose an improved approach that enhances security considerably. To evaluate the effectiveness of our proposed scheme, we utilized BAN logic and conducted both formal and informal security assessments. Our analysis indicates that the proposed scheme meets all security standards and is resistant to

various known threats. Additionally, we performed a comparative performance analysis against other relevant schemes, considering the hardware specifications of mobile and sensor devices in real Internet of Things (IoT) environments. The findings reveal that our proposed method is compatible with low-cost IoT devices. In summary, the proposed user authentication method offers a practical and secure solution for IoT applications.

Conflict of interest

The author has declared no conflicts of interest.

Financial disclosure

The study received no funding, according to the author.

References

[1] C. Wang, G. Xu, and W. Li, ‘‘A secure and anonymous two-factor authentication protocol in multiserver environment,’’ *Secur. Commun. Netw.*, vol. 2018, pp. 1–15, Apr. 2018. DOI: 10.1155/2018/4012820.

[2] Y. Park, ‘‘A secure user authentication scheme with biometrics for IoT medical environments,’’ *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 11, pp. 607–615, 2018. DOI: 10.14569/IJACSA.2018.091173.

[3] Ahmad I, Shahabuddin S, Kumar T, Okwuibe J, Gurtov A, Ylianttila M. Security for 5g and beyond. IEEE Communications Surveys & Tutorials 2019, DOI: 10.1109/COMST.2019.2916180.

[4] Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks. Commun ACM 2004;47(6):53–7. DOI: 10.1145/990680.990707.

[5] Mishra D. Efficient and secure two-factor dynamic ID-based password authentication scheme with provable security. Cryptologia 2018;42 (2):146–75. DOI: 10.1080/01611194.2017.1313385.

[6] Srinivas J, Mukhopadhyay S, Mishra D. A self-verifiable password-based authentication scheme for multi-server architecture using smart card. Wireless Personal Communications 2017;96(4):6273–97.DOI: 10.1007/s11277-017-4406-7.

[7] Dhillon PK, Kalra S. Secure multi-factor remote user authentication scheme for internet of things environments. Int J Commun Syst 2017;30(16): e3323., DOI: 10.1002/dac.3323.

[8] Lamport L. Password authentication with insecure communication. Commun ACM 1981;24(11):770–2. DOI: 10.1145/358790.358797.

[9] Li L-H, Lin L-C, Hwang MS. A remote password authentication scheme for multiserver architecture using neural networks. IEEE Trans Neural Networks 2001;12(6):1498–504. DOI: 10.1109/72.963769.

[10] Das ML. Two-factor user authentication in wireless sensor networks. IEEE Trans Wireless Commun 2009;8(3):1086–90.DOI: 10.1109/TWC.2009.071016.

[11] Xu J, Zhu W-T, Feng DG. An improved smart card-based password authentication scheme with provable security. Computer Standards & Interfaces 2009;31(4):723–8. DOI: 10.1016/j.csi.2008.10.005.

[12] Banerjee S, Mukhopadhyay D. Symmetric key-based authenticated querying in wireless sensor networks. In: Proceedings of the first international conference on Integrated internet ad hoc and sensor networks. ACM; 2006. p. 22. DOI: 10.1145/1189355.1189378.

[13] Du W, Wang R, Ning P. An efficient scheme for authenticating public keys in sensor networks. In: Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing. ACM; 2005. p. 58–67. DOI: 10.1145/1062689.1062698.

[14] Chatterjee S, Das AK. An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. Security and Communication Networks 2015;8(9):1752–71.DOI: 10.1002/sec.1164.

[15] Chung Y, Choi S, Won D. Anonymous authentication scheme for intercommunication in the internet of things environments. Int J Distrib Sens Netw 2015;11(11):305785. DOI: 10.1155/2015/305785

[16] Park Y, Park Y. Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. Sensors 2016;16(12):2123. DOI: 10.3390/s16122123.

[17] Wong KH, Zheng Y, Cao J, Wang S. A dynamic user authentication scheme for wireless sensor networks. In: Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing-Vol 1 (SUTC’06)-Volume 01. IEEE Computer Society; 2006. p. 244–51. DOI: 10.1109/SUTC.2006.1636165.

[18] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos and J. J. P. C. Rodrigues, "Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment," in *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572-3584, April 2019, doi: 10.1109/JIOT.2018.2888821.

[19] Khan MK, Alghathbar K. Cryptanalysis and security improvements of ‘two-factor user authentication in wireless sensor networks Sensors 2010;10 (3): 2450–9.DOI: 10.3390/s100302450

[20] Vaidya B, Makrakis D, Mouftah HT. Improved two-factor user authentication in wireless sensor networks. In: 2010 IEEE 6th International Conference on Wireless and Mobile Computing,

Networking and Communications. IEEE; 2010. p. 600–6. DOI: 10.1109/WIMOB.2010.5644982.

[21] Yeh H-L, Chen T-H, Liu P-C, Kim T-H, Wei HW. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors 2011;11(5):4767–79. DOI: 10.3390/s110504767.

[22] He D, Gao Y, Chan S, Chen C, Bu J. An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc & Sensor Wireless Networks 2010;10(4):361–71.

[23] Xue K, Ma C, Hong P, Ding R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network and Computer Applications 2013;36(1):316–23.DOI: 10.1016/j.jnca.2012.05.013.

[24] Jin ATB, Ling DNC, Goh A. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern Recognition*. 2004;37(11):2245–2255.DOI: 10.1016/j.patcog.2004.03.012.

[25] Turkanović M, Brumen B, Hölbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. Ad Hoc Netw 2014; 20:96–112. DOI: 10.1016/j.adhoc.2014.03.009.

[26] Farash, M. S., Turkanović, M., Kumari, S., & Hölbl, M. (2016). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Networks, 36*, 152–176. DOI: 10.1016/j.adhoc.2015.05.014.

[27] I.-P. Chang, T.-F. Lee, T.-H. Lin, and C.-M. Liu, ‘‘Enhanced two-factor authentication and key agreement using dynamic identities in wireless sensor networks,’’ *Sensors*, vol. 15, no. 12, pp. 29841–29854, Nov. 2015. DOI: 10.3390/s151229782

[28] Y. Park and Y. Park, ‘‘Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks,’’ *Sensors*, vol. 16, no. 12, p. 2123, Dec. 2016. DOI: 10.3390/s16122123.

[29] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, ‘‘A robust and anonymous patient monitoring system using wireless medical sensor networks,’’ *Future Gener. Comput. Syst.*, vol. 80, pp. 483–495, Mar. 2018. DOI: 10.1016/j.future.2016.06.027.

[30] X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, and C. Chen, ‘‘A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems,’’ *IEEE Syst. J.*, vol. 14, no. 1, pp. 39–50, Mar. 2020. DOI: 10.1109/JSYST.2019.2892451.

[31] A. Juels and T. Ristenpart, ‘‘Honey encryption: Encryption beyond the brute-force barrier,’’ *IEEE Security Privacy*, vol. 12, no. 4, pp. 59–62, Jul. 2014. DOI: 10.1109/MSP.2014.72.

[32] A. Juels and T. Ristenpart, ‘‘Honey encryption: Security beyond the brute-force bound,’’ in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2014, pp. 293–310. DOI: 10.1007/978-3-642-55220-5_17.

[33] A. Juels and R. L. Rivest, ‘‘Honeywords: Making password-cracking detectable,’’ in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 145–160. DOI: 10.1145/2508859.2516671.

[34] D. Wang and P. Wang, ‘‘Two birds with one stone: Two-factor authentication with security beyond conventional bound,’’ *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 4, pp. 708–722, Aug. 2018. DOI: 10.1109/TDSC.2016.2631662

[35] D. Wang, W. Li, and P. Wang, ‘‘Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks,’’ *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4081–4092, Sep. 2018. DOI: 10.1109/TII.2018.2803213.

[36] Y. Dodis, L. Reyzin, and A. Smith, ‘‘Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,’’ in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Interlaken, Switzerland, 2004, pp. 523–540. DOI: 10.1007/978-3-540-24676-3_31.

[37] D. Dolev and A. Yao, ‘‘On the security of public key protocols,’’ *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983. DOI: 10.1109/TIT.1983.1056650.

[38] M. Burrows, M. Abadi, and R. Needham, ‘‘A logic of authentication,’’ *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, 1990. DOI: 10.1145/77648.77649

[39] AVISPA. (2020). Automated Validation of Internet Security Protocols and Applications. Accessed: Mar. 2020. [Online]. Available: http://www.avispa-project.org/.

[40] AVISPA. SPAN, A Security Protocol Animator for AVISPA. Accessed: Mar. 2020. [Online]. Available: http://www.avispa-project.org/.

[41] D. Von Oheimb, ‘‘The high-level protocol specification language HLPSL developed in the EU project AVISPA,’’ in *Proc. 3rd APPSEM II Workshop Appl. Semantics (APPSEM)*, Frauenchiemsee, Germany, 2005, pp. 1–17. [Online]. Available: http://www.avispa-project.org/.

[42] Das AK, Kumari S, Odelu V, Li X, Wu F, Huang X. Provably secure user authentication and key agreement scheme for wireless sensor networks. Security and Communication Networks 2016;9(16):3670–87. https://doi.org/10.1002/sec.1575.

[43] Chang C-C, Le HD. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. IEEE Trans Wireless Commun 2015;15(1):357–66. https://doi.org/10.1109/TWC.2015.2473165.

[44] Yang Z, Lai J, Sun Y, Zhou J. A novel authenticated key agreement protocol with dynamic credential for WSNs. ACM Transactions on Sensor Networks (TOSN) 2019;15(2):22. https://doi.org/10.1145/3303704.

[45] Banerjee S, Chunka C, Sen S, Goswami RS. An enhanced and secure biometric based user authentication scheme in wireless sensor networks using smart cards. Wireless Personal Communications 2019:1–28. https://doi.org/10.1007/s11277-019-06252-x.

[46] Wu F, Li X, Sangaiah AK, Xu L, Kumari S, Wu L, Shen J. A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks. Future Generation Computer Systems 2018; 82:727–37. https://doi.org/10.1016/j.future.2017.08.042.

[47] W. Iqbal, H. Abbas, B. Rauf, Y. Abbas, F. Amjad, and A. Hemani, "PCSS: Privacy-preserving communication scheme for SDN enabled smart homes," IEEE Sensors J., to be published, doi: 10.1109/JSEN.2021.3087779.

[48] D. Basin, S. Mödersheim, and L. Vigano, ''OFMC: A symbolic model checker for security protocols,'' *Int. J. Inf. Secur.*, vol. 4, no. 3, pp. 181–208, Jun. 2005. DOI: 10.1007/s10207-005-0061-4.

[49] Wu F, Xu L, Kumari S, Li X, Khan MK, Das AK. An enhanced mutual authentication and key agreement scheme for mobile user roaming service in global mobility networks. Ann Telecommun2017;72(3–4):131–44. https://doi.org/10.1007/s12243-016-0547-2.

[50] Abbasinezhad-Mood D, Nikooghadam M. Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications. Future Generation Computer Systems 2018; 84:47–57. DOI: 10.1016/j.future.2018.01.051.

[51] Burrows M, Abadi M, Needham RM. A logic of authentication. *Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences*. 1989;426(1871):233–271. DOI: 10.1098/rspa.1989.0125.

[52] Chatterjee S, Roy S, Das AK, Chattopadhyay S, Kumar N, Vasilakos AV. Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment. *IEEE Transactions on Dependable and Secure Computing*. 2018;15(5):824–839. DOI: 10.1109/TDSC.2016.2616876.

[53] Reddy AG, Das AK, Odelu V, Yoo KY. An enhanced biometric-based authentication with key-agreement protocol for multi-server architecture based on elliptic curve cryptography. *PLoS ONE*. 2016;11(5): e0154308. DOI: 10.1371/journal.pone.0154308.

[54] Kumari S, Khan MK, Atiquzzaman M**.** User authentication schemes for wireless sensor networks: a review. *Ad Hoc Networks*. 2015; 27:159–94.DOI: 10.1016/j.adhoc.2015.05.004.