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

Neha Sharma[1] , Pankaj Dhiman[2]

[1]Department of Computer Engineering, Jaypee University of Information Technology Waknaghat Solan, HP, India

[2]Department of Computer Engineering, Jaypee University of Information Technology Waknaghat Solan, HP, India

ABSTRACT

The proliferation of IoT devices and the implementation of 5G networks have raised concerns about the potential for increased security breaches due to the expanded attack surfaces resulting from improved connectivity. One of the primary approaches for addressing these security issues in IoT systems is establishing reliable user authentication methods. Many other authors still need to propose a multi-factor user authentication mechanism for the IoT, but their scheme was prone to several security attacks. It was susceptible, for example, to user impersonation attacks and stolen mobile devices. The scheme had no session key agreement or backup plan for lost/stolen devices or compromised private keys. In addition, we demonstrate that the proposed system is suitable for IoT contexts and has low computing and communication costs for low-cost IoT devices. In response to security concerns, we designed a multi-factor user authentication mechanism.

Keywords: Authentication, Key agreement, Internet of Things, Wireless Sensor Networks

I. INTRODUCTION

The Internet of Things (IoT) is a network of nodes with limited resources that are densely distributed throughout environments. 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. 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. 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) Mutual authentication: The scheme should enable participants to confirm one another's authority through mutual authentication.

(4) Session key agreement: The key used for encrypting and decrypting messages in the authentication system must be fresh while guaranteeing forward secrecy [1].

(5) Resistance to several attacks: The authentication mechanism must satisfy all essential security objectives and resist known attacks [2].

When secret keys are revealed, it becomes possible for anyone to decode all network communication. 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. Revoking something is a straightforward and efficient way to prevent it from being used or accessed [3]. 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 [4][5]. In today's world, ensuring security is crucial, particularly in the IoT environment where resources are limited. The author [6] proposed a computationally efficient three-factor remote authentication technique suitable for IoT environments. In our analysis, we discovered security flaws in their plan. In our paper we proposes a new authentication scheme that addresses these vulnerabilities through cryptanalysis. Our analysis verifies that the proposed multifactor authentication scheme satisfies all security requirements and is efficient for IoT contexts in calculating and communicating costs.

A. 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. The author [13] 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 author [14] introduced the first password-based authentication system for WSNs. However, the author [15] 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 of Wong et al.'s scheme, Das et al. implemented a two-factor authentication strategy for users using the gateway (GW) [16]. However, later vulnerabilities were discovered in Das' method, and organizations faced several types of security threats, such as attacks against privileged insiders, impersonation, GW-node bypassing, etc.

Additionally, Das' scheme fails to ensure mutual verification between the gateway and sensor nodes. In response to security concerns with user authentication, [17] developed an improved two-factor authentication strategy.

However, author [20] discovered that their system was vulnerable to theft and attacks. method for WSNs that used smart cards. They improved the scheme's security by using elliptic curve cryptography (ECC). However, the author [22] found that the ECC-based technique required more processing and storage resources.

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

Table 1. List of symbols and their description

In 2011, Yeh et al. [21] presented a novel user authentication A new, more secure approach was then introduced by Xue et al. [22]. 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.

Security concerns in WSNs are addressed with mutual authentication using hash and XOR operations proposed by author [25]. However, the author [26] identified security flaws in this technique, which were addressed by presenting a user authentication mechanism optimized for WSNs. Nonetheless author [27] reported that author [26] approach was unsafe against various attacks and breached the anonymity of users and sensor nodes.

Conventional two-factor authentication techniques are unsafe in real-world scenarios, as per authors research [6]. Based on the IoT network architecture, they established a lightweight multi-factor authentication system that employs passwords, biometrics, and mobile devices. Their technique resists password guessing, DoS, 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 exploiting stolen mobile devices. In this paper, we evaluate the weaknesses in the security system in Dhillon and Kalra's approach [6] and introduce an improved lightweight authentication method suitable for IoT contexts that utilizes only Cryptography with symmetry, hashing, and XOR methods.

B. Preface

IoT architecture models offer security, scalability, and low computing cost benefits. The author [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 analysing the message received fromSn_i, verifies Mn_i, and responds to Sn_i.

(4) After Mn_i responds to Sn_i, authentication establishes a session key.

II 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.

The author [24] developed a 2FA system in 2004 that utilizes fingerprint traits unique to each user and inner products of tokenized pseudo-random integers. They created a bio-hash code, a unique and compact code set for each user. They used a user-specific token of pseudo-random digits to convert the random binary string with a biometric characteristic. The use of bio-hash technology has been proposed in recent methods [30, 31] due to its suitability for tiny-capacity devices, making it a practical choice for biometrics-based multi-factor authentication schemes [32]. An anonymous user authentication scheme for IoT environments with three factors and four phases has been developed.

(1) Registration

(2) Login and authentication

(3) Password change

(4) user-revocation phase.

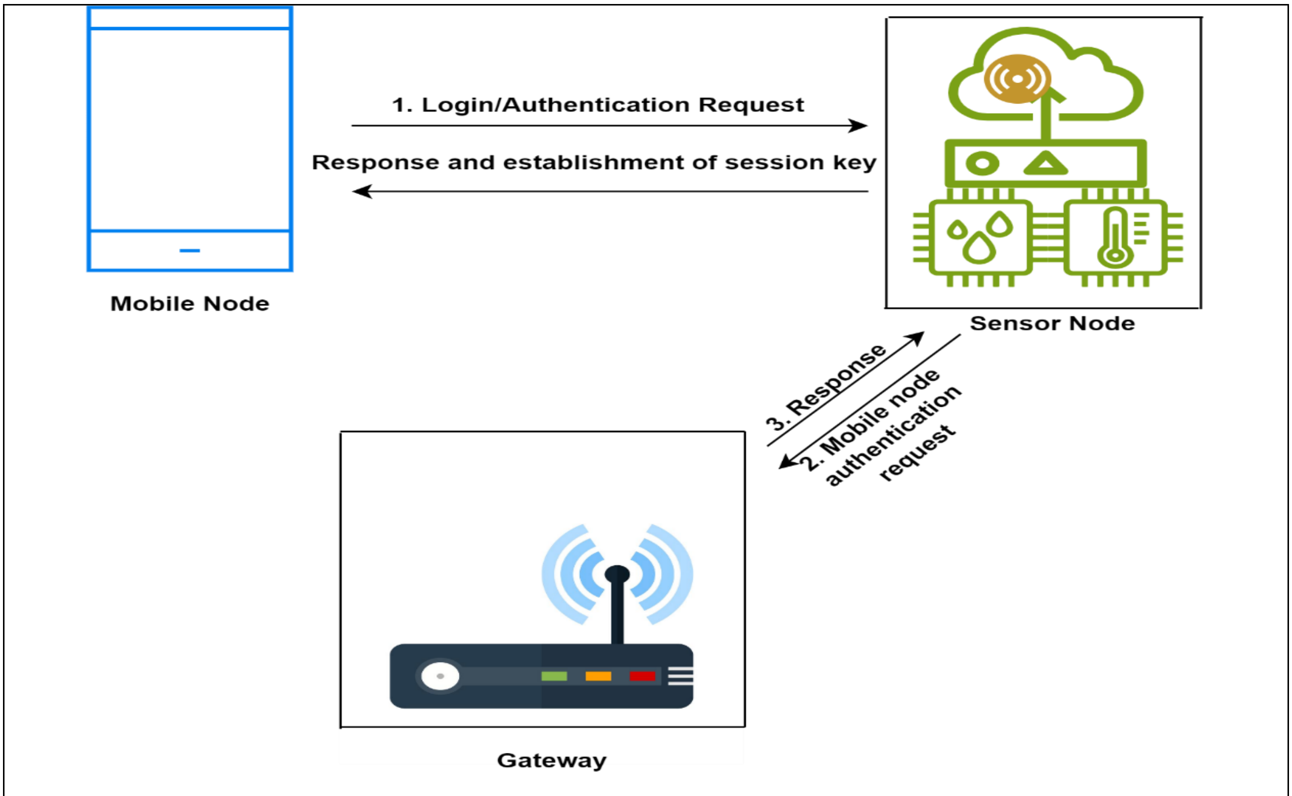

Figure 1. The proposed technique offers a user authentication model for IoT

A. Registration of a User

The registration phase for Mn_i is illustrated in Figure 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 $< Id_i, PwB_i, Mid_i >$ to GW via the secure channel.

(c) GW randomly selects numbers r_{GU} and r_D, and computes $Rid_i = E_{kg}(Id_i), Pid_i = E_{k_g}(Id_i \parallel r_{gu}), x_i = h(Id_i \parallel PwB_i)$, and $y_i = h(Id_i \| PwB_i \| r_{gj}) \oplus h(K_{gu} \parallel Id_i)$. A pair is stored by GW $(Rid_i \quad Mid_i \quad)$ in the database.
(d) GW sends $< Pidi, x_i, y_i, r_{gu} >$ to Mn_i.
(e) In the final step, Mn_i saves the parameters received

$< Pid_i\ x_i\ y_i, r_{gu} >$, in the mobile device.

B. Registration of IoT node

The process of registering sensor node N_j is shown in Figure 3 and involves the following steps:
(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.

C. Login and authentication phase

MN_i and Sn_i mutually authenticate with the help of GW to create a session key. As shown in Figure 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.

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

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

(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 $UN_i^* = h(a_i^* \Vert Pid_i \Vert n_i^*)$ 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 $F_j = h(Id_i \parallel n_i^*), G_j = F_j \oplus x_j^*, R_{ij} = n_j^* \oplus n_i^*, H_j = h(x_j^* \Vert n_j^* \Vert n_i^* \parallel F_j)$, and $PID_i^{\text{new}} = E_{kg}\left(Id_i, r_d^{\text{new}}\right)$.

(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 $H_j^* = h(x_j \Vert n_j \Vert n_i^* \parallel F_j^*)$ 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, $L_j = h(Nid_j \parallel n_i^*) \oplus m_j$, $Sk_{ji} = h(F_j^* \Vert n_i^* \Vert m_j)$ and $Sv_j = h(Sk_{ji} \Vert T_1 \Vert T_2)$.

(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 $m_j^* = L_j \oplus h(Nid_j \parallel n_i)$, $Sk_{ij} = h(h(I_i \parallel n_i) \Vert n_i \Vert m_j^*)$, and $Sv_i = h(Sk_{ij} \Vert T_1 \Vert T_2)$. If Sv_i and Sv_j are the same, Mn_i and Sn_i produce the same session key successfully.

D. 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 $PWB_i^{\text{old}} = h\left(Pw_i || h(Bio_i)\right)$ and $x_i^* = h\left(Id_i \parallel PwB_i^{\text{old}}\right)$.
(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 $A_i = y_i \oplus h(ID_i || PwB_i^{dd} || r_{gj})$, $PwB_i^{\text{new}} = h\left(PW_i^{\text{new}} \parallel H(Bio_i)\right)$, $x_i^{\text{new}} = h\left(Id_i \parallel PwB_i^{\text{new}}\right)$, and $y_i^{\text{new}\ i} = h\left(ID_i \left\| Pw^i B_i^{\text{new}} \right\| r_{gu}\right) \oplus A_i \oplus y_i$.

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

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

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

E. 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

$PwB_i^{\text{new}} = h\left(Pw_i^{\text{new}} \parallel H(Bio_i)\right)$, $Mid_i^{\text{old}} = h\left(Id_i^{\text{old}} \parallel H(Bio_i)\right)$, and $Mid_i^{\text{new}} = h\left(Id_i^{\text{new}} \parallel H(Bio_i)\right)$.

(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 $RID_i^{\text{old}} = E_{K_G}\left(Id_i^{\text{old}}\right)$ The system first verifies the identity of $Mn_i$and then searches for a pair. (Rid_i^{old} ,Mid_i^{old}) to locate a registered user in the database. If the pairs (Rid_i, Mid_i) and $\left(RID_i^{\text{old}}, MID_i^{\text{old}}\right)$ are equal, GW produces new random numbers r_d^{new} and r_{gu}^{new}, computes $Pid_i^{\text{new}} =$

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

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

Table 4. Login and authentication phase

III. BAN Logic Authentication Proof

In this section, we utilized Burrows-Abadi-Needham (BAN) logic [55] to demonstrate that Mn_i and Sn_i mutually 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 [56–59]. 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) $\stackrel{K}{\leftrightarrow} S$: 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: $\frac{U]\equiv\#(C), U|\equiv S\sim C}{U(\equiv)=C}$: 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 U believes C and M, then (C,M) is also believed by U.

(4) Rule 4: Freshness-concatenation rule: $\frac{U_{\|}=\nexists(C)}{A_{\|}=+(C,M)}$: 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: $Sn_i \mid\equiv \left(Mn_i \overset{SK}{\longleftrightarrow} Sn_i\right)$
(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 $M_4 =< Pid_i^{new}, L_j, Sv_j, T_2 >, Sn_i \rightarrow Mn_i:\ L_j = h(Nid_j \parallel n_i^*) \oplus m_j t, Sv_j = h(SK_{ji} \| T_1 \| T_2)$. This decreases as: $\text{MSG}_4: (\text{Pid}_i, \text{m}_j, T_1, T_2)_{m_i}$

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) $A_B: Mn_i \mid\equiv \left(Mn_i \overset{\pi_i}{\longleftrightarrow} Sn_i\right)$
(9) $A_g: Mn_i \mid\equiv Sn_i \Rightarrow \left(Mn_i \overset{\mathcal{K}}{\leftrightarrow} Sn_i\right)$
(10) $A_{10}: Sn_i \mid\equiv Mn_i \Rightarrow \left(Mn_i \overset{\leftrightarrow}{\longleftrightarrow} Sn_i\right)$

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 $V_3: Sn_i \mid\equiv \sharp(Pid_i, A_i, T_1)_{n_j}$
(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 $V_7: GW \mid\equiv \sharp(M_1, Nid_j, sn_i)x.$
(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: $\text{Sn}_i \triangleleft (F_j, n_j, n_i, K_{cn})x_j$
(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 $V_{11}: Sn_i \mid\equiv \pm(F_j, Sn_i, n_i, K_{cn})x_j$
(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 $V_{15}: Mn_i \mid\equiv \sharp(Pid_i, m_j, T_1, T_2)_{m_i}$
(16) From $V_{13}.V_{14}$ and Rule 2 , we get $V_{16}: Mn_i \left|\equiv Sn_{i\,j}\right| \equiv (Pid_i, m_j, T_1, T_2)_{n_i}$
(17) From V_{12}, V_{16}, and $SK = h(F_j \| n_i \| m_j)$. we get $V_{17}: Mn_i \mid\equiv \left(Mn_i \overset{SK}{\leftrightarrow} N_j\right)$ (Goal1)
(18) From V_4, V_8, and $SK = h(h(Id_i \parallel\mid n_i) || n_i \parallel m_j)$, we get $V_{18}: Sn_i \mid\equiv \left(Mn_i \overset{\leftrightarrows}{\longleftrightarrow} Sn_i\right)$ (Goal2)
(19) From A_9, V_{17} and Rule 5, we get $V_{19}: Mn_i|\equiv Sn_i| \equiv \left(Mn_i \overset{SK}{\leftrightarrow} Sn_i\right)$(Goal3)
(20) From A_{10}, V_{18} and Rule 5 , we get V_{20}: $Sn_i|\equiv Mn_i| \equiv \left(Mn_i \overset{sK}{\longleftrightarrow} Sn_i\right)$(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.

IV. 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

Scheme	[7]	[25]	[42]	[43]	[44]	[45]	[46]	Proposed
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	2592

Table 5 Comparison of the communication cost

Scheme	[7]	[25]	[42]	[43]	[44]	[45]	[46]	Proposed
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	$7T_h$	$7T_h$	$10T_h$	$9T_h$	$20T_h$	$6T_h$	$15T_h$	$8T_h + 2T_s$
Total	$22T_h$	$19T_h$	$27T_h + 3T_e$	$21T_h + 4T_e$	$52T_h$	$21T_h$	$31T_h$	$24T_h + 2T_s$
Time	$\approx 1085\mu s$	$\approx 856\mu s$	$\approx 1323\mu s$	$\approx 2585\mu s$	$\approx 2049\mu s$	$\approx 1080\mu s$	$\approx 1321\mu s$	$\approx 1115\mu s$

Table 6 Comparison of Computation

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. 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.

A. 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 [60]. The mobile node was a Galaxy Note 9 Device, with an Octa-Core processor clocked at 2.7GHz+1.7GHz, 8GB memory, and operating on Android 9.0. Android Studio and Software Development Kits (SDK) were the software development tools. The sensor node was an LPC1768 Device, with an ARM Cortex-M3 processor clocked at up to 100MHz, 512KB flash memory, and 64KB SRAM. The Gateway was a CPU with an Intel(R) Pentium(R) processor G4600 clocked at 3.60 GHz, 8GB memory, and operating on Win10 64bit. The Crypto++ Library 8.1 was used with Visual Studio 2017. Our measurements, along with Abbasinezhad-Mood and Nikooghadam's [60] experiments, reveal the cryptographic times for the mobile node, sensor node, and gateway:

1) Mobile node: $T_e \approx 28.48\mu s$, $T_s \approx 74.2\mu s$, and $T_h \approx 104.38\mu s$
(2) Sensor node: $T_e \approx 1264\ \mu s$ and $T_h \approx 14.5\mu s$
(3) Gateway: $T_e \approx 2224\ \mu s$, $T_s \approx 5.4094\mu s$, and $T_h \approx 4.9464\mu s$

Table 3 summarizes the performance comparison results of various schemes. Our analysis found that Turkanovic et al.'s approach [25] has a much lower computational complexity than other systems. However, this approach has previously been shown to be vulnerable to several attacks by Farash et al. [26]. Our proposed system has lower computing costs than the schemes by Das et al. [42], Chang et al. [43], Yang et al. [44], and Wu et al. [46]. Banerjee et al.'s scheme [45] performs the best, but lacks a revocation step, as shown in Table 4. Communication costs of login and authentication were analyzed using methodology [61, 62]. Identity, timestamp, and random number values were estimated to be 128, 32, and 64 bits long. Our proposed method of communication and computation costs are shown in Tables 5 and 6. The hash function, elliptic multiplication, and symmetric key encryption each yield 256, 360, and 160 bits, respectively. Our Scheme also discusses the reliability of the proposed scheme against different attacks, such as User anonymity(UAA), User untraceability (UUA), stolen mobile device attack (SMDA), mutual authentication (MAA), user impersonation attack(UIA), replay attack(RA), user verification(UVA), stolen-verifier attack(SVA), privileged-insider attack(PIA) etc as shown in Table 7.

```
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

```
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

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

Table 7. Comparison Functionality and Security attribute

V. Conclusion

Our research paper presents a significant breakthrough in user authentication techniques. We identified several security flaws in Dhillon and Kalra's approach, and we developed an improved scheme that addresses these issues and significantly enhances security. After conducting extensive security studies using the random oracle model, BAN logic, and AVISPA, we have found that our proposed authentication scheme is secure against a range of known attacks and meets all security requirements. Furthermore, we evaluated the performance of our system with other relevant schemes considering hardware specifications of mobile and sensor devices in IoT to ensure optimal performance and integration. Our study indicates that our system is fully compatible with IoT devices that are extremely low-cost. We are confident that our proposed technique is the most suitable and secure method for user authentication in IoT contexts.

Conflict of Interest: The author has declared no conflicts of interest.

Financial Disclosure: The study received no funding, according to the author.

References

[1] Park O , Hwang H, Lee C, Shin J . Trends of 5g massive lot, electronics and telecommunications. Trends 2016;31(1):68–77.
[2] Series M . Imt vision–framework and overall objectives of the future development of it for 2020 and beyond. Recommendation ITU 2015. 2083–0
[3] Ahmad I , Shahabuddin S , Kumar T , Okwuibe J , Gurtov A , Ylianttila M Security for 5g and beyond. IEEE Communications Surveys & Tutorials 2019.
[4] Mishra D . Efficient and secure two-factor dynamic id-based password authentication scheme with provable security. Cryptologia 2018;42(2):146–75.
[5] Srinivas J , Mukhopadhyay S , Mishra D . A self-verifiable password-based authentication scheme for multi-server architecture using a smart card. Wireless Personal Communications 2017;96(4):6273–97.
[6] 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.
[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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] Chung Y , Choi S , Won D . Anonymous authentication scheme for an intercom- communication in the Internet of things environments. Int J Distrib Sens Netw 2015;11(11):305785.
[13] Park Y , Park Y . Three-factor user authentication and key agreement using elliptic curve cryptosystem in wireless sensor networks. Sensors 2016;16(12): 2123 .
[14] 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.
[15] Khan MK , Alghathbar K . Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks. Sensors 2010;10(3):2450–9 .
[16] 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 .
[17] 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 .
[18] 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.
[19] 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 .
[20] Li C-T , Weng C-Y , Lee CC . An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. Sensors 2013;13(8):9589–603 .
[21 C.-Y. Chen, P. H. Chou, "DuraCap: a supercapacitor-based, power-bo-outstripping, maximum power point tracking energy-harvesting system", in ACM/IEEE International Symposium on Low-Power Electronics Design, TX, USA, 2010, pp. 313-318. [CrossRef] [22] X. Jiang, J. Polastre, D. Culler, "Perpetual environmentally powered sensor networks," in The 4th International Symposium on Informa- tion Processing in Sensor Networks, ID, USA, 2005, pp. 463-468.
[23] M. Habibzadeh, M. Hassanalieragh, A. Ishikawa, T. Soyata, G. Shar- ma, "Hybrid solar-wind energy harvesting for embedded appli- cations: supercapacitor-based system architectures and design tradeoffs", IEEE Circuits and Systems Magazine, vol. 17, no. 4, pp. 29-63, Nov, 2017. [CrossRef]
[24] M. Hassanalieragh, T. Soyata, A. Nadeau, G. Sharma, "UR-SolarCap: an open source intelligent auto-wakeup solar energy harvesting system for supercapacitor based energy buffering", IEEE Access, vol. 4, pp. 542-557, Jan, 2016. [CrossRef]
[25] Turkanovi ´c 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.
[26] Farash MS , Turkanovi ´c M , Kumari S , Hölbl M . An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment. Ad Hoc Netw 2016;36:152–76.
[27] Brunelli, C. Moser, L. Thiele, L. Benini, "Design of a solar-harvesting circuit for batteryless embedded systems", IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 56, no. 11, pp. 2519-2528, Feb, 2009. [CrossRef]
[28] C. Park, P. H. Chou, "AmbiMax: autonomous energy harvestingplatform for multi-supply wireless sensor nodes" in The 3rd Annual IEEE Communications Society Conference on Sensor and AdHoc Communications and Networks, VA, USA, 2006, pp. 168-177. [CrossRef]
[29] F. I. Simjee, P. H. Chou, "Efficient charging of supercapacitors forextended lifetime of wireless sensor nodes", IEEE Transactionson Power Electronics, vol. 23, no. 3, pp. 1526-1536, May 2008.[CrossRef]
[30] P. Bhatnagar, R. K. Nema, "Maximum power point tracking cont- rol techniques: state-of-the-art in photovoltaic applications", Re- newable and Sustainable Energy Reviews, vol. 23, pp. 224-241,July 2013. [CrossRef]
[31] H. Islam, S. Mekhilef, N. B. M. Shah, T. K. Soon, M. Seyedmahmousi- an, B. Horan, A. Stojcevski, "Performance evaluation of maximumpower point tracking approaches and photovoltaic systems", Energies, vol. 11, no. 2, pp. 365-389, Feb, 2018. [CrossRef]
[32] T. Esram, P. L. Chapman, "Comparison of photovoltaic array maximum power point tracking techniques", IEEE Transactions on Energy Conversion, vol. 22, no. 2, pp. 439-449, June 2007. [CrossRef]
[33] S. Kim, K.-S. No, P. H. Chou, "Design and performance analysis of supercapacitor charging circuits for wireless sensor nodes", IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 1, no. 3, pp. 391-402, Sep, 2011. [CrossRef]
[34] D. Dondi, A. Bertacchini, D. Brunelli, L. Larcher, L. Benini, "Modeling and optimization of a solar energy harvester system for self-powe-red wireless sensor networks", IEEE Transactions on Industrial Electronics, vol. 55, no. 7, pp. 2759-2766, July, 2008.[CrossRef]
[35] C. Moser, L. Thiele, D. Brunelli, L. Benini, "Adaptive power management for environmentally powered systems", IEEE Transactions onComputers, vol. 59, no. 4, pp. 478-491, Apr, 2010. [CrossRef]
[36] C. Bergonzini, D. Brunelli, L. Benini, "Comparison of energy intakeprediction algorithms for systems powered by photovoltaic har-vesters", Microelectronics Journal, vol. 40, no. 11, pp. 766-777, Nov,2010. [CrossRef]
[37] A. Kansal, D. Potter, M. B. Srivastava, "Performance aware tasking for environmentally powered sensor networks", in Joint Interna-tional Conference on Measurement and Modeling of Computer Systems, NY, USA, 2004, pp. 223-234. [CrossRef]
[38] J. Hsu, S. Zahedi, A. Kansal, M. B. Srivastava, V. Raghunathan,"Adaptive duty cycling for energy harvesting systems", in The International Symposium on Low Power Electronics and Design, Tegernsee, Germany, 2006, pp.180-185. [CrossRef]
[39] A. Kansal, M. B. Srivastava, "Energy harvesting aware power management", Wireless Sensor Networks: A Systems Perspective, ch. 9,pp. 1-10, Artech House, MA, USA, 2005.
[40] A. Kansal, J. Hsu, S. Zahedi, M. B. Srivastava, "Power managementin energy harvesting sensor networks", ACM Transactions on Em- bedded Computing Systems, vol. 6, no. 4, pp. 1-35, Sep, 2007. [CrossRef]
[41] Kumari S , Khan MK , Li X . A more secure digital rights management authentication scheme based on smart card. Multimed Tools Appl 2016;75(2):1135–58 .
[42] Das AK , Kumari S , Odelu V , Li X , Wu F , Huang X . Provably secure user authen- tication and key agreement scheme for wireless sensor networks. Security and Communication Networks 2016;9(16):3670–87 .
[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 .
[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 ..
[45] Banerjee S , Chunka C , Sen S , Goswami RS . An enhanced and secure biomet- ric based user authentication scheme in wireless sensor networks using smart cards. Wireless Personal Communications 2019:1–28 ..
[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 .
[47] Das AK , Sutrala AK , Kumari S , Odelu V , Wazid M , Li X . An efficient multi–gateway-based three-factor user authentication and key agreement scheme in hierarchical wireless sensor networks. Security and Communication Networks 2016;9(13):2070–92 .
[48] Li X , Peng J , Obaidat MS , Wu F , Khan MK , Chen C . A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor net- work systems. IEEE Syst J 2019 .
[49] Das AK , Kumari S , Odelu V , Li X , Wu F , Huang X . Provably secure user authen- tication and key agreement scheme for wireless sensor networks. Security and Communication Networks 2016;9(16):3670–87 .
[50] O. Samuel, A. B. Omojo, A. M. Onuja, Y. Sunday, P. Tiwari, D. Gupta, G. Hafeez, A. S. Yahaya, O. J. Fatoba, and S. Shamshirband, "Iomt: A covid-19 healthcare system driven by federated learning and blockchain," IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 823–834, 2022.
[51] S. Uppuluri and G. Lakshmeeswari, "Secure user authentication and key agreement scheme for iot device access control based smart home communications," Wireless Networks, vol. 29, no. 3, pp. 1333–1354, 2023.
[52] L. Bai, C. Hsu, L. Harn, J. Cui, and Z. Zhao, "A practical lightweight anonymous authentication and key establishment scheme for resourceasymmetric smart environments," IEEE Transactions on Dependable and Secure Computing, 2022.