IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 September 2023, accepted 11 October 2023, date of publication 16 October 2023, date of current version 20 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3325130

RESEARCH ARTICLE

An Efficient Lightweight Provably Secure Authentication Protocol for Patient Monitoring Using Wireless Medical Sensor Networks

GARIMA THAKUR[1], SUNIL PRAJAPAT[1], (Associate Member, IEEE), PANKAJ KUMAR[1],
ASHOK KUMAR DAS[2], (Senior Member, IEEE),
AND SACHIN SHETTY[3], (Senior Member, IEEE)
[1]Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Dharamshala 176206, India
[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
[3]Virginia Modeling, Analysis and Simulation Center, Department of Computational Modeling and Simulation Engineering, Old Dominion University, Suffolk, VA 23435, USA

Corresponding author: Ashok Kumar Das (iitkgp.akdas@gmail.com)

This work was supported in part by the DoD Center of Excellence in AI and Machine Learning (CoE-AIML) through the U.S. Army Research Laboratory under Contract W911NF-20-2-0277.

ABSTRACT The refurbishing of conventional medical network with the wireless medical sensor network has not only amplified the efficiency of the network but concurrently posed different security threats. Previously, Servati and Safkhani had suggested an Internet of Things (IoT) based authentication scheme for the healthcare environment promulgating a secure protocol in resistance to several attacks. However, the analysis demonstrates that the protocol could not withstand user, server, and gateway node impersonation attacks. Further, the protocol fails to resist offline password guessing, ephemeral secret leakage, and gateway-by-passing attacks. To address the security weaknesses, we furnish a lightweight three-factor authentication framework employing the fuzzy extractor technique to safeguard the user's biometric information. The Burrows-Abadi-Needham (BAN) logic, Real-or-Random (ROR) model, and Scyther simulation tool have been imposed as formal approaches for establishing the validity of the proposed work. The heuristic analysis stipulates that the proposed work is impenetrable to possible threats and offers several security peculiarities like forward secrecy and three-factor security. A thorough analysis of the preexisting works with the proposed ones corroborates the intensified security and efficiency with the reduced computational, communication, and security overheads.

INDEX TERMS Wireless medical sensor network, authentication, key agreement, security, ROR model, scyther tool.

I. INTRODUCTION

The leverage of Wireless Sensor Networks (WSNs) in the medical network has refined the potential of the healthcare network with the offered sensing and disseminating information benedictions and surfaced as the premier research paradigm. The encapsulation of WSN and medical network formulates a wireless medical sensor network (WMSN) and is an appealing solution to substantially boost healthcare services. Utilizing WMSN, the patient's health could be frequently monitored by the medical workers in WMSN-based healthcare systems. Such healthcare systems collect patient's physiological parameters, including their temperature, blood pressure, serum cholesterol, heart rate, and glucose level, utilizing the wearable sensors [1]. Thus, medical professionals can promptly examine and diagnose a patient by closely monitoring this data on a continuous basis. WMSNs incorporate users, gateways, and sensor nodes for medical devices like conventional WSNs. Users being medical professionals, can access the patient's

The associate editor coordinating the review of this manuscript and approving it for publication was Gyorgy Eigner.

bio-information via the medical sensor node after registering their pertinent details in the gateway node. However, due to the limited capabilities of devices incorporating medical sensors, such as storage capacity, transmission range, and computing power, protocols that require complex calculations may result in a system's communication failure. Additionally, as WMSN uses open, attackable wireless channels for information exchange, an attacker might get a patient's medical information by intercepting that communication or furnish the user with false medical information [2]. In light of this, a system communication breakdown combined with an attacker's alteration of medical data may make it impossible to establish the patient's status. Since this directly affects the patient's lives, therefore secure information exchange necessitates lightweight authentication across users, gateways, and sensor nodes based on a predetermined session key.

For this purpose, conventional WMSN-based medical systems have been recently recommended [3], [4] for assuring sustainable healthcare services. Lamentably, existing WMSN systems render inadequate healthcare services since they rely on a centralized infrastructure that could have several shortcomings, such as a single point of failure. Furthermore, aside from the centralized system issues, WMSN-based medical systems may be exposed to cyber security risks and be unable to provide the required levels of security if patient-sensitive data is made public. Therefore, an adversary may present a variety of unanticipated dangers and jeopardize the patient's life by providing inaccurate health information, such as prescriptions, assessments, and cures. Since WMSN entities interact with other entities utilizing a public wireless channel, they are subject to numerous network assaults and privacy breaches [2], [5]. Consequently, it is indispensable to ensure user privacy and communication security by confirming the identities of the communicating entities. Recently, Servati and Safkhani [6] proposed a three-factor authentication protocol for healthcare IoT systems. They professed that their scheme could fend off the majority of cryptographic attacks like offline password guessing, impersonation, ephemeral secret leakage, and privileged insider attacks. Unfortunately, our findings demonstrate that the framework suggested in [6] cannot withstand user, server, and gateway node impersonation attacks, in addition to offline password guessing and ephemeral secret leakage attacks. This motivates us to devise an enhanced authentication framework for WMSN that addresses the security weaknesses of Servati and Safkhani's protocol and can resist mentioned cryptographic attacks.

A. MAIN CONTRIBUTIONS

The contributions are summarized as follows:

- We thoroughly investigated Servati and Safkhani's scheme and encountered several security weaknesses. The findings reveal that the protocol fails to endure user, server, and gateway node impersonation attacks. Also, the protocol fails to resist offline password guessing, ephemeral secret leakage, and gateway-by-passing attacks.
- We devised a lightweight three-factor authentication framework employing the fuzzy extractor technique to safeguard the user's biometric information and address the security weaknesses of Servati and Safkhani's protocol.
- The suggested scheme's mutual authentication and session key security is ensured by formal security analysis, which employs the BAN logic [7], ROR model [8], and simulation utilizing the Scyther tool [9]. The security of our work has also been strengthened by informal security assessment.
- The extensively used Scyther tool is used to simulate our method. The outcome shows that our scheme is safe and secure against mentioned security threats. Lastly, analyzing the devised protocol with the pre-existing authentication systems substantiates the work's computational and communication efficiency.

B. PAPER OUTLINE

The remaining portions of the manuscript are systematized as follows. Sections II and III illustrate related work and a few relevant mathematical preliminaries required to implement the suggested method. Section IV gives a brief analysis of Servati and Safkhani's scheme. The comprehensive description of the devised approach with a novel architecture, including all its phases, is presented in section V. The correctness of the proposed protocol is exemplified by the formal and informal security analysis in section VI. Section VII propounds a meticulous comparison of the suggested work to the preexisting competitive protocols. Finally, the work is concluded in Section VIII.

II. RELATED WORK

In recent years, ''access control, authentication and key management'' are widely-used two main security mechanisms in providing security in IoT-enabled environments [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27].

For the purpose of safeguarding the transmitted data in the WMSN environment, Amin et al. [28] proposed a lightweight two-factor authentication protocol. However, Jiang et al. [29] found their protocol susceptible to sensor key exposure, de-synchronization, and stolen mobile device attacks. Then, Jan et al. [30] also highlighted the security flaws of Amin et al.'s protocol and unveiled a two-factor authentication system for WMSN. For healthcare monitoring systems, a lightweight two-factor authentication protocol was put forth by Fotouhi et al. [31]. Nevertheless, Nashwan [32] discovered that Fotouhi et al.'s approach is insufficient to allow complete mutual authentication. Next, Masud et al. [33] created a privacy-protected, lightweight authentication mechanism for IoT-based healthcare that utilizes a patient's IoT device's sensors. However, Kwon et al. [34] accentuated that the work cannot guard against several thwarts, including user impersonation, offline password guessing, and privileged insider attacks. The protocol further fails to preserve user anonymity. Since the two-factor authentication protocols are more prone to cryptographic attacks, thus to address the existing issues, numerous researchers proposed biometric-based authentication protocols.

In 2018, Ali et al. [36] identified issues with the Amin et al.'s [28] approach and developed a framework utilizing three-factor authentication to address the issue. Their suggested protocol, however, similarly falls short of achieving complete forward secrecy and defense against de-synchronization attacks [37]. The improved system developed by Shuai et al. [37] uses a pseudonymous identification approach to guarantee user anonymity, forward secrecy, and thwart de-synchronization attacks. Nashwan [32], however, found that the protocol cannot facilitate the sensor node's anonymous service and cannot defend against sensors' impersonation attacks. Additionally, Mo et al. [42] discovered a weakness in Shuai et al.'s approach during the password update phase. Then, they suggested an improved WMSN methodology. In the WMSN environment, Li et al.'s [38] proposed an authentication technique that employs a three-factor mechanism to provide perfect forward secrecy. Their system, however, is similarly unable to ensure the sensor node's security and is susceptible to sensor node spoofing attacks [43]. An RFID-based authentication mechanism was put forth by Kumar et al. [41] for vehicular cloud computing, and they asserted that it was secure. However, [44] highlighted the vulnerabilities of Safkhani et al. and demonstrated that it is susceptible to replay and impersonation attacks. Afterward, He et al. [35] presented an anonymous authentication protocol with provable security for Wireless Body Area Networks (WBAN), but Sowjanya et al. [45] analysis demonstrates that their devised framework is not resistant to insider and clock synchronization attacks. Similarly, Das et al. [39] devised a provably secure ECC-based authentication framework for IoT environment with access control and key agreement phase. Moreover, they asserted it to be secure against man-in-the-middle (MITM) and device impersonation attacks. Nevertheless, these assertions were refuted by Chaudhry et al. [46]. In 2018, Sureshkumar et al. [40] devised an authentication framework utilizing lightweight ECC for WMSN. Following that, Servati and Safkhani [6] reviewed the scheme proposed by and found it vulnerable to traceability, de-synchronization, and integrity contradiction attacks. Thus, to address the limitations of the protocol, Servati and Safkhani proposed an authentication protocol for healthcare IoT systems. Table 1 provides a summary of the advantages and limitations of the methods mentioned above.

III. PRELIMINARIES

A. FUZZY EXTRACTOR

A fuzzy extractor [47] takes the biometric Bio_a as input and outputs a pair of two random integers (σ, θ) in an error-tolerant manner. If Bio'_a is perceived as a change but is still closely connected to Bio_a, the retrieved data is unchanged because of the auxiliary string θ. The fuzzy extractor incorporates the following two procedures:

1) $Gen(.)$: A probabilistic generator known as Gen produces an extracted string σ and an auxiliary string θ in response to a biometric input Bio_a, i.e., $Gen(Bio_a) = (\sigma, \theta)$.
2) $Rep(.)$: If Bio_a and Bio'_a are relatively close to each other, then Rep denotes the deterministic reproduction technique that enables recovery of σ from the matching auxiliary string θ and Bio'_a, i.e., $Rep(Bio'_a, \theta) = \sigma$.

B. ADVERSARY MODEL

This section demonstrates the security of the suggested approach employing the extensively utilized "Dolev-Yao (DY) model" [48] and "Canetti-Krawczyk (CK) model" [49]. The attributes of an evil adversary $\mathcal{A}$ according to the DY and CK paradigm are as follows:

- The messages sent through an open channel is susceptible to interception by an $\mathcal{A}$. Additionally, $\mathcal{A}$ has the ability to obstruct, replay, and alter messages sent over the open channel.
- An $\mathcal{A}$ can acquire a smart card belonging to an authorized user and apply a power analysis attack to retrieve the smart card's stored values [50].
- An $\mathcal{A}$ can concurrently attempt to guess a valid user's identity and password utilizing the dictionary space.
- An $\mathcal{A}$ has the potential to compromise session-specific temporary credentials as well as any flimsy data that could expose the session key formed between the interacting entities.

C. SYSTEM MODEL

The proposed healthcare system model is shown in Fig. 1. In this paradigm, the patient's body is implanted with wireless low-power intelligent medical sensors such pacemakers, brain neural simulators, blood glucose level sensors, etc. These sensors often use Zigbee, Bluetooth, or infrared technologies to refresh the data and send it to neighboring smart devices. In general, security considerations are unnecessary because the smart gadgets are close to the patient. Also, a doctor can connect to the gateway while the patient remains in the hospital to check on their condition and get information from the patient anywhere. However, since the patient's data is kept on a cloud server, it is necessary to set up a secure authentication system to guard against cryptographic attacks.

D. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

In contrast to other forms of traditional encryption like RSA and DSA, ECC offers smaller keys. An ECC over a finite field has the following characteristics. ECC is defined as $\rho^2 = \mu^3 + \gamma\mu + \alpha \pmod{p}$, where p is a big prime and $4\gamma^3 + 27\alpha^2 \neq 0$. It uses the elliptic curve $E_p(\gamma, \alpha)$ over the finite field F_p. The additive ECC group is denoted by the

TABLE 1. Comparative summary of authentication protocols.

Literature	Year	Limitations	Advantages
He *et al.* [35]	2016	• Insider attacks • ClocMalani8777170k synchronization attacks	• Impersonation attacks • Replay attacks • Modification attacks
Amin *et al.* [28]	2018	• Session key disclosure attacks • De-synchronization attacks • Stolen mobile device attacks • NO ROR model	• Untraceability • Offline password guessing attacks • Impersonation attacks
Ali *et al.* [36]	2018	• Ensures perfect forward secrecy • De-synchronization attacks • No ROR model	• Offline identity and password guessing attacks • Impersonation attacks • Replay attacks • Mutual authentication
Shuai *et al.* [37]	2019	• Cannot facilitate sensor node's anonymous service • Sensor node impersonation attacks • Wrong password update phase • No ROR model	• User anonymity • De-synchronization attacks
Li *et al.* [38]	2019	• Unable to ensure sensor node's security • Sensor node spoofing attacks	• Known key security • Impersonation attacks • Mobile device loss attacks
Das *et al.* [39]	2019	• Device impersonation attacks • MITM attacks	• Replay attacks • Malicious device deployment attacks • Device physical capture attacks
Sureshkumar *et al.* [40]	2019	• Traceability attacks • De-synchronization attacks • Integrity contradiction attacks	• Privileged insider attacks • User impersonation attacks • Perfect forward secrecy
Kumar *et al.* [41]	2020	• Replay attacks • Impersonation attacks	• Mutual authentication • Offline password guessing attacks • Parallel session attacks
Masud *et al.* [33]	2021	• User impersonation attacks • Offline password guessing attacks • Privileged insider attacks • User anonymity • No formal security analysis	• Replay attacks • MITM attacks • Ensures data privacy

expression $G = \{(\rho, \mu)|\rho, \mu \in F_p, (\rho, \mu) \in E(\gamma, \alpha) \cup \theta$, where θ is the additive identity of G. The scalar multiplication on the G, which forms a cyclic group, is described as $mR = R + R + R + \ldots + R$ (m times), where R is the base point on $E_p(\gamma, \alpha)$, and $m \in F_p$ is a positive integer. There are two primary challenging problems based on ECC:

- Elliptic Curve Discrete Logarithm Problem (ECDLP): Given $P, Q \in E_p$, such that $P = x.Q$. It is computationally hard to find x, where $x \in F_p$.
- Elliptic Curve Diffie-Hellman Problem (ECDHP): Given $P, a.P, b.P \in E_p$, where $a, b \in F_p$. It is computationally hard to find $a.b.P$.

IV. REVIEW AND CRYPTANALYSIS OF SERVATI AND SAFKHANI'S SCHEME

This section discusses the security weaknesses of Servati and Safkhani's protocol. They claimed that the bulk of cryptographic attacks, such as impersonation, ephemeral secret leakage, offline password guessing, and privileged insider, can be resisted by their scheme. Regrettably, our analysis shows that the framework suggested in [6] cannot withstand attacks that impersonate users, servers, and gateway nodes, along with offline password guessing, by-passing and ephemeral secret leakage attacks. The syllabary used in the paper are displayed in Table 2.

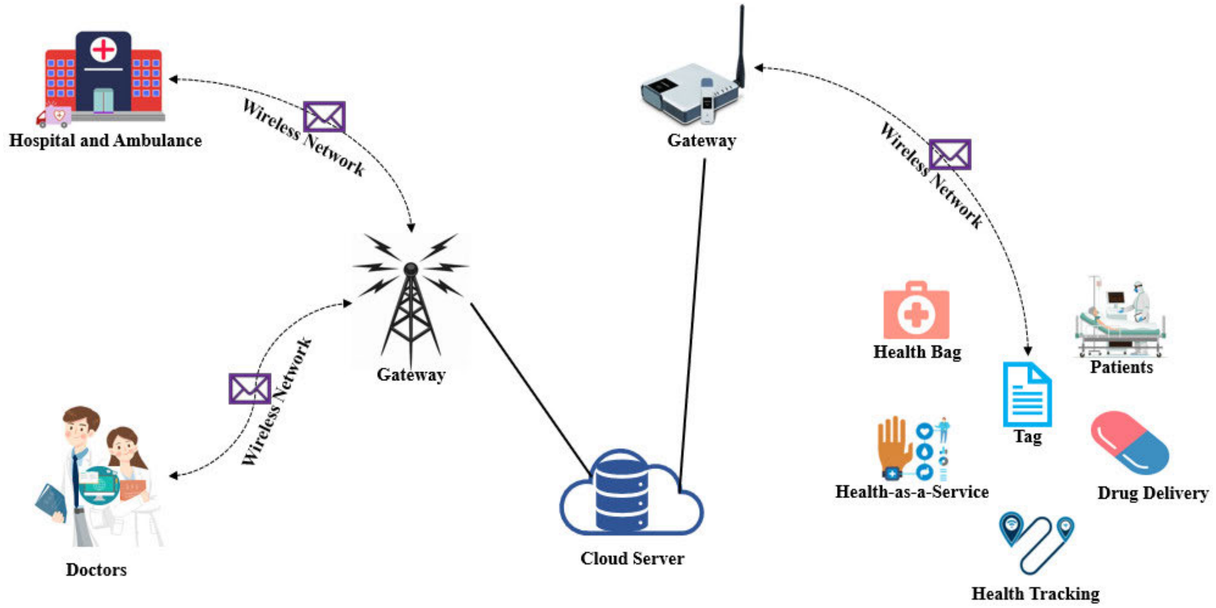


FIGURE 1. Proposed system model [6].

TABLE 2. Notations Table.

Symbol	Description
$E_p(a,b)$	Elliptic curve over F_p
p	Prime number
Z_p^*	Multiplicative group of order $p-1$
G	Additive group
SA	System administrator
U_a	User
GW_b	Gateway node
SN_c	Sensor node
ID_a	U_a's identity
PW_a	U_a's password
B_a	U_a's biometric
SC	U_a's smart card
x_a, x_b, x_c	Private keys of U_a, GW_b, SN_c
P_a, P_b, P_c	Public keys of U_a, GW_b, SN_c
$\mathcal{A}$	Adversary
T_i	Time stamp i=1,...,4
$h(.)$	Hash function
$\oplus, \|\|$	Bitwise XOR, Concatenation operation
$\Longrightarrow, \rightarrow$	Secure channel, Public channel
SK	Session key

A. REVIEW OF SERVATI AND SAFKHANI'S SCHEME

1) INITIALIZATION PHASE

Each entity on the cloud server is manually configured during this phase, and the unique credentials of all entities are saved on the server. This protocol uses lightweight ECC for usage in smart devices, and SA selects S_{SA} as his private key.

2) GATEWAY AND SENSOR NODE REGISTRATION PHASE

The SA completes this phase to register the gateway and sensor node by performing subsequent actions.

- Firstly, SA elects an identity GW_{ID_b} for GW_b and computes a secret value as $S_{GW_b} = h(S_{SA}||GW_{ID_b})$ by utilizing its secret key S_{SA}. Following that, the parameters $\{S_{GW_b}, GW_{ID_b}, A_4 = S_{GW_b}.P\}$ are stored in the gateways database. Additionally, SA keeps $\{S_{GW_b}\}$ in its database for further utilization.
- Next, SA chooses an identity SN_{ID_c} for SN_c and computes a secret value as $S_{SN_c} = h(S_{SA}||SN_{ID_c})$. Thereafter, SA stores $\{S_{SN_c}, SN_{ID_c}\}$ in the memory of both GW_b and SN_c. Also, SA stores GW_{ID_b} in the sensor node's memory.

Following registration, SA publishes the identities of registered gateway nodes keeping the identities of the sensor nodes private to ensure the sensor node's anonymity.

3) USER REGISTRATION PHASE

After successful user authentication, a trustworthy user is given access to the observed data. This happens when the sensor's observed data is read by the gateway node, and the user requests access to the data. As a result, we require a process for enrolling users.

- U_a selects ID_a, PW_a and B_a to register as a legitimate user and computes $b_a = H(B_a)$, $HID_a = h(ID_a||b_a)$ and $HPW_a = h(PW_a||b_a)$. Thus, $U_a \Longrightarrow SA : \{HID_a, HPW_a, GW_{ID_b}\}$.
- On receiving the message, SA reckons $A_1 = h(HID_a||HPW_a)$, $A_2 = h(HID_a||S_{GW_b})$, $A_3 = A_2 \oplus A_1$ and $A_4 = S_{GW_b}.P$. Then, SA invokes $SC = \{A_3, A_4, h(\cdot), P\}$ and transmits SC to U_a i.e., $SA \Longrightarrow U_a : SC = \{A_3, A_4, h(\cdot), P\}$.
- Then, U_a enumerates $HPID_a = h(HID_a||PW_a)$ and $A_5 = h(HID_a||HPID_a)$ employing pseudo identity HID_a, bio-hashing b_a and PW_a. Next, U_a computes $A_2^* = A_3 \oplus A_1$, $A_6 = A_2^* \oplus A_4$. Lastly, U_a stores $\{A_3, A_5, A_6, h(\cdot), P\}$ in SC.

4) LOGIN, AUTHENTICATION, AND KEY AGREEMENT PHASE

The user must login through the gateway node to access the patient's data collected by the sensor node's. Thereafter, the entities authenticate each other by generating a shared session key. The following steps must be followed by a user to complete the process:

- U_a inputs ID_a, PW_a and B_a into SC. Then, SC reckons $HID_a = h(ID_a||b_a)$, $HPID_a = h(HID_a||PW_a)$ and $A_5^* = h(HID_a||HPID_a)$. Then, verifies $A_5^* \overset{?}{=} A_5$. Following that, SC generates a random nonce $r_a \in F_p$ and evaluates $HPW_a = h(PW_a||b_a)$, $A_1^* = h(HID_a||HPW_a)$, $A_2 = A_3 \oplus A_1^*$, $A_4 = A_6 \oplus A_2$, $A_8 = r_a.P$, $A_7 = (A_2||HID_a||SN_{ID_c}) \oplus r_a.A_4$, and $A_9 = h(A_7||A_8||T_1)$. Therefore, $U_a \rightarrow GW_b : Msg_1 = \{A_7, A_8, A_9, T_1\}$.
- On receiving $Msg_1 = \{A_7, A_8, A_9, T_1\}$, GW_b verifies, $T_1 - T_1^* \leq \delta T$ and then calculates $(A_2^*||HID_a^*||SN_{ID_c}^*) = A_7 \oplus A_8.S_{GW_b}$. Next, GW_b verifies $A_2^* \overset{?}{=} h(HID_a^*||S_{GW_b})$ and $A_9 \overset{?}{=} h(A_7||A_8||T_1)$. If the equality holds, GW_b selects a random nonce $r_b \in F_p$ and reckons $A_{11} = r_b.A_8 = r_a.r_b.P$, $A_{12} = r_b.P$, $A_{13} = h(S_{SN_c}).A_{12}$, $A_{14} = h(S_{SN_c}||GW_{ID_b}).P$, $A_{15} = h(A_{14}||A_{12}||A_{11}||A_{16}||T_2)$, and $A_{16} = A_8 \oplus A_{13}$. Thereafter, $GW_b \rightarrow SN_c : Msg_2 = \{A_{12}, A_{11}, A_{15}, A_{16}, T_2\}$.
- Once the message has been received, SN_c verifies, $T_2 - T_2^* \leq \delta T$ and then calculates $A_{14}^* = h(S_{SN_c}||GW_{ID_b}).P$, $A_{15}^* = h(A_{14}^*||A_{12}||A_{11}||A_{16}||T_2)$, and corroborates $A_{15}^* \overset{?}{=} A_{15}$. If equality holds true, SN_c invokes $r_c \in F_p$ and evaluates $A_{17} = r_c.A_{12}$, $A_{13}^* = h(S_{SN_c}).A_{12}$, $A_8^{**} = A_{16} \oplus A_{13}^*$, $A_{19} = r_c.A_8^{**}$, $A_{20} = r_c.P$, $A_{18} = h(A_{17}||S_{SN_c}||A_{19}||A_{20}||T_3)$, and $SK = r_c.A_{11}$. Afterward, $SN_c \rightarrow GW_b : Msg_3 = \{A_{19}, A_{18}, A_{20}, T_3\}$.
- After receiving $\{A_{19}, A_{18}, A_{20}, T_3\}$, GW_b verifies $T_3 - T_3^* \leq \delta T$ and computes $A_{17}^* = r_b.A_{20}$, $A_{18}^* = h(A_{17}^*||S_{SN_c}||A_{19}||A_{20}||T_3)$. Thereafter, GW_b validates $A_{18}^* \overset{?}{=} A_{18}$ and evaluates $A_{21} = h(HID_a^*||A_{17}^*||A_8||A_4||T_4)$ and $SK = r_b.A_{19}$. Then, $GW_b \rightarrow U_a : Msg_4 = \{A_{17}^*, A_{21}, T_4\}$.
- Firstly, U_a validates whether $T_4 - T_4^* \leq \delta T$. Following the verification of timestamp condition, U_a evaluates $A_{21} = h(HID_a||A_{17}^*||A_8||A_4||T_4)$ and checks $A_{21}^* \overset{?}{=} A_{21}$. Next, U_a generates the session key as $SK = r_a.A_{17}^*$.

5) PASSWORD UPDATE PHASE

A legitimate user should be allowed to modify their password to maintain the protocol's security objectives. The steps to characterize this phase are as follows: U_a inputs ID_a, PW_a and B_a into SC. Then, SC reckons $HID_a = h(ID_a||b_a)$, $HPID_a = h(HID_a||PW_a)$ and $A_5^* = h(HID_a||HPID_a)$. Then, verifies $A_5^* \overset{?}{=} A_5$. Next, U_a enters a new password PW_a^{new} using his SC and computes $HPID_a^{new} = h(HID_a||PW_a^{new})$, $A_1^{new} = h(HID_a||HPW_a^{new})$, $A_3^{new} = (A_3 \oplus A_1) \oplus A_1^{new}$ and $A_5^{new} = h(HID_a||HPID_a^{new})$. Lastly, SC replaces A_3 and A_5 with A_3^{new} and A_5^{new}.

B. CRYPTANALYSIS OF SERVATI AND SAFKHANI'S SCHEME

1) OFFLINE PASSWORD GUESSING ATTACK

Suppose that $\mathcal{A}$ is some privileged insider of the system that has garnered the user's registration request $\{HID_a, HPW_a, GW_{ID_b}\}$ in addition to the smart card parameters $\{A_3, A_5, A_6, h(\cdot), P\}$ by employing the power analysis attack. Next, to attempt the offline password guessing attack, $\mathcal{A}$ guesses the users password PW_a^* through the dictionary and attempts to compute $HPID_a^* = h(HID_a||PW_a^*)$ and $A_5^* = h(HID_a||HPID_a^*)$. Afterward, $\mathcal{A}$ checks $A_5^* \overset{?}{=} A_5$. If equality holds, then $\mathcal{A}$ successfully guesses the user's password. Consequently, the protocol proposed by Servati and Safkhani cannot resist "offline password guessing attacks".

2) USER IMPERSONATION ATTACK

In this attack, the $\mathcal{A}$ aims to generate a valid message $Msg_1^* = \{A_7, A_8, A_9, T_1\}$ that passes the verification phase, once the message has been transmitted to GW_b. To do so, $\mathcal{A}$ generates a random nonce $r_a^* \in F_p$ and timestamp T_1^*. Additionally, the parameters HID_a, HPW_a, A_3, A_5 and A_6 are known to $\mathcal{A}$ by employing the aforementioned privileged insider and smart card stolen attack. Further, by capturing the sensor node, $\mathcal{A}$ can extract the parameters $\{S_{SN_c}, SN_{ID_c}, GW_{ID_b}\}$ from the memory of SN_c. Therefore, $\mathcal{A}$ enumerates $A_1 = h(HID_a||HPW_a)$, $A_2 = A_3 \oplus A_1$, and $A_4 = A_6 \oplus A_2$. Next, $\mathcal{A}$ evaluates $A_8^* = r_a^*.P$, $A_7^* = (A_2||HID_a||SN_{ID_c}) \oplus r_a^*.A_4$, and $A_9^* = h(A_7^*||A_8^*||T_1^*)$. Therefore, $\mathcal{A} \rightarrow GW_b : Msg_1^* = \{A_7^*, A_8^*, A_9^*, T_1^*\}$. Since the transmitted message Msg_1^* contains the original credentials of U_a, thus the generated message will pass the verification phase. Subsequently, the protocol in [6] is not immune to "user impersonation attack".

3) GATEWAY NODE IMPERSONATION ATTACK

This attack illustrates the impersonation of the gateway node by an $\mathcal{A}$. Here, the $\mathcal{A}$ impedes the message $Msg_2 = \{A_{12}, A_{11}, A_{15}, A_{16}, T_2\}$ transmitted by GW_b to SN_c, and attempts to generate a forged message Msg_2^*. For this purpose, $\mathcal{A}$ selects a random nonce $r_b^* \in F_p$, T_2^* and reckons $A_{11}^* = r_b^*.A_8$, $A_{12}^* = r_b^*.P$, $A_{13}^* = h(S_{SN_c}).A_{12}^*$, $A_{14} = h(S_{SN_c}||GW_{ID_b}).P$, $A_{16}^* = A_8 \oplus A_{13}^*$, and $A_{15}^* = h(A_{14}||A_{12}^*||A_{11}^*||A_{16}^*||T_2^*)$. Thereafter, $\mathcal{A} \rightarrow SN_c : Msg_2^* = \{A_{12}^*, A_{11}^*, A_{15}^*, A_{16}^*, T_2^*\}$. Once the message Msg_2^* reaches the sensor node, SN_c checks $T_2 - T_2^* \leq \delta T$. Further, SN_c calculates $A_{14}^* = h(S_{SN_c}|||GW_{ID_b}).P$, $A_{15}^* = h(A_{14}^*||A_{12}||A_{11}||A_{16}||T_2)$, and corroborates $A_{15}^* \overset{?}{=} A_{15}$. This inequality will hold true. Therefore, the protocol in [6] cannot withstand the "gateway node impersonation attacks".

4) SENSOR NODE IMPERSONATION ATTACK

This attack demonstrates how an $\mathcal{A}$ can pretend to be a sensor node. Here, the $\mathcal{A}$ intercepts the message $Msg_1 = \{A_7, A_8, A_9, T_1\}$, $Msg_3 = \{A_{19}, A_{18}, A_{20}, T_3\}$ transmitted by SN_c to GW_b, and attempts to generate a duplicate message

U_a		SA
Input ID_a, PW_a and B_a Enumerates $Gen(B_a) = (\sigma_a, \theta_a)$ $HID_a = h(ID_a\|\|\sigma_a)$ $HPW_a = h(PW_a\|\|\sigma_a)$		
	$\xrightarrow{\{HID_a,HPW_a,GW_{ID_b}\}}$	
		Computes $A_1 = h(HID_a\|\|HPW_a)$ $A_2 = h(HID_a\|\|S_{GW_b})$ $A_3 = A_2 \oplus A_1$
	$\xleftarrow{SC=\{A_3,h(\cdot),P\}}$	
Computes $HPID_a = h(HID_a\|\|PW_a\|\|\sigma_a)$ $A_4 = h(HID_a\|\|HPID_a\|\|\sigma_a)$ Stores $\{A_3, A_4, h(\cdot), P\}$ in SC.		

FIGURE 2. User Registration phase.

Msg_3^*. To accomplish this, SN_c invokes $r_c^* \in F_p$ and evaluates $A_{17}^* = r_c^*.A_{12}$, $A_{19}^* = r_c^*.A_8$, $A_{20}^* = r_c^*.P$, $A_{18}^* = h(A_{17}^*||S_{SN_c}||A_{19}^*||A_{20}^*||T_3^*)$, and $SK^* = r_c^*.A_{11}$. Afterward, $\mathcal{A} \rightarrow GW_b : Msg_3^* = \{A_{19}^*, A_{18}^*, A_{20}^*, T_3^*\}$. Thus, the protocol proposed in [6] is vulnerable to "sensor node impersonation attack".

5) EPHEMERAL SECRET LEAKAGE ATTACK

The perseverance against the Ephemeral secret leakage attack comprises the inability of the adversary to determine the session key when the ephemeral secrets like the session's random nonces are disclosed. Suppose that the session random nonces r_a, r_b and r_c are revealed. Further, the $\mathcal{A}$ captures the messages Msg_1, Msg_2, Msg_3 and Msg_4 transmitted through the unsecured channel. Therefore, the parameters A_{11}, A_{17} and A_{19} are also known to $\mathcal{A}$. Consequently, $\mathcal{A}$ can compute the session keys $SK = r_c.A_{11}$, $SK = r_b.A_{19}$, and $SK = r_a.A_{17}^*$. Hence, the protocol in [6] is susceptible to "ephemeral secret leakage attack".

6) BY-PASSING ATTACK

This attack demonstrates the case where the information or the message sent by the legitimate user does not pass through the verification phase of GW_b but rather is bypassed to SN_c directly. This can be achieved if the $\mathcal{A}$ plays the role of the GW_b and generates a forged message Msg_2^*. Thus, $\mathcal{A}$ selects a random nonce $r_b^* \in F_p$, timestamp T_2^* and reckons $A_{11}^* = r_b^*.A_8$, $A_{12}^* = r_b^*.P$, $A_{13}^* = h(S_{SN_c}).A_{12}^*$, $A_{14} = h(S_{SN_c}||GW_{ID_b}).P$, $A_{16}^* = A_8 \oplus A_{13}^*$, and $A_{15}^* = h(A_{14}||A_{12}^*||A_{11}^*||A_{16}^*||T_2^*)$. Thereafter, $\mathcal{A} \rightarrow SN_c : Msg_2^* = \{A_{12}^*, A_{11}^*, A_{15}^*, A_{16}^*, T_2^*\}$. Subsequently, the protocol in [6] is not robust against "by-passing attacks".

V. PROPOSED SCHEME

To address the security issues with Servati and Safkhani's approach, we suggest a reliable and effective authentication method for WMSN-based medical systems. Similar to Servati and Safkhani's five-phase framework, the enhanced system incorporates these phases as well.

A. INITIALIZATION PHASE

The initialization phase of the proposed scheme is similar to that of Servati and Safkhani's scheme. The in-depth explanation of the initialization phase is given in Section IV-A1.

B. GATEWAY AND SENSOR NODE REGISTRATION PHASE

The SA completes this phase to register the gateway and sensor node by performing subsequent actions.

- Firstly, SA elects an identity GW_{ID_b} for GW_b and computes a secret value as $S_{GW_b} = h(S_{SA}||GW_{ID_b})$ by utilizing its secret key S_{SA}. Following that, the parameters $\{S_{GW_b}, GW_{ID_b}\}$ are stored in the gateways database. Additionally, SA keeps $\{S_{GW_b}\}$ in its database for further utilization.
- Next, SA chooses an identity SN_{ID_c} for SN_c and computes a secret value as $S_{SN_c} = h(S_{SA}||SN_{ID_c})$. Thereafter, SA stores $\{S_{SN_c}, SN_{ID_c}\}$ in the memory of both GW_b and SN_c. Also, SA stores GW_{ID_b} in the sensor node's memory.

C. USER REGISTRATION PHASE

The user registration procedure is accomplished by the SA. The entire registration process takes place through a secure communication channel. The in-depth explanations are listed below.

- U_a selects ID_a, PW_a and B_a to register as a legitimate user and computes $Gen(B_a) = (\sigma_a, \theta_a)$, $HID_a = h(ID_a||\sigma_a)$ and $HPW_a = h(PW_a||\sigma_a)$. Thus, $U_a \Longrightarrow SA : \{HID_a, HPW_a, GW_{ID_b}\}$.
- On receiving the message, SA reckons $A_1 = h(HID_a||HPW_a)$, $A_2 = h(HID_a||S_{GW_b})$ and $A_3 = A_2 \oplus$

U_a/SC	GW_b	SN_c
Inputs ID_a^*, PW_a^* and B_a^* Computes $Rep(B_a^*, \theta_a) = \sigma_a^*$ $HID_a^* = h(ID_a^*\|\|\sigma_a^*)$ $HPID_a^* = h(HID_a^*\|\|PW_a^*\|\|\sigma_a^*)$ $A_4^* = h(HID_a^*\|\|HPID_a^*\|\|\sigma_a^*)$ Verifies $A_4^* \overset{?}{=} A_4$ Generates $r_a \in F_p^*$ Computes $HPW_a = h(PW_a\|\|\sigma_a)$ $A_1 = h(HID_a\|\|HPW_a)$ $A_2 = A_3 \oplus A_1$ $A_5 = h(HID_a\|\|r_a\|\|x_a\|\|T_1)$ $A_6 = A_5.P, A_7 = A_5.P_b$ $A_8 = (A_2\|\|HID_a\|\|SN_{ID_c}) \oplus h(A_7\|\|T_1)$ $A_9 = h(A_2\|\|A_7\|\|A_8\|\|HID_a\|\|SN_{ID_c})$ $\xrightarrow{\{A_6, A_8, A_9, T_1\}}$		
	Checks $T_1 - T_1^* \leq \delta T$ Calculates $A_7^* = A_6.x_b$ $(A_2\|\|HID_a\|\|SN_{ID_c}) = A_8 \oplus h(A_7^*\|\|T_1)$ $A_9^* = h(A_2\|\|A_7^*\|\|A_8\|\|HID_a\|\|SN_{ID_c})$ Verifies $A_9^* \overset{?}{=} A_9$ Invokes $r_b \in F_p^*$ Evaluates $A_{10} = h(GW_{ID_b}\|\|S_{SN_c}\|\|r_b\|\|x_b\|\|T_2)$ $A_{11} = A_{10}.P, A_{12} = A_{10}.P_c$ $A_{13} = h(S_{SN_c}\|\|A_{12}\|\|GW_{ID_b}\|\|T_2)$ $\xrightarrow{\{A_{11}, A_{13}, T_2\}}$	
		Checks $T_2 - T_2^* \leq \delta T$ Reckons $A_{12}^* = A_{11}.x_c$ $A_{13}^* = h(S_{SN_c}\|\|A_{12}^*\|\|GW_{ID_b}\|\|T_2)$ Verifies $A_{13}^* \overset{?}{=} A_{13}$ Generates $r_c \in F_p^*$ Enumerates $A_{14} = h(SN_{ID_c}\|\|r_c\|\|x_c\|\|T_3)$ $A_{15} = A_{14}.P, A_{16} = A_{14}.P_a$ $SK_c = h(A_{15}\|\|A_{16}\|\|x_c.P_a\|\|T_3)$ $A_{17} = h(SK_c\|\|A_{16}\|\|T_3)$ $\xleftarrow{\{A_{15}, A_{17}, T_3\}}$
	Verifies $T_3 - T_3^* \leq \delta T$ $\xleftarrow{\{A_{15}, A_{17}, T_3, T_4\}}$	
Validates $T_4 - T_4^* \leq \delta T$ Evaluates $A_{16}^* = A_{15}.x_a$ $SK_a = h(A_{15}\|\|A_{16}^*\|\|x_a.P_c\|\|T_3)$ $A_{17}^* = h(SK_a\|\|A_{16}^*\|\|T_3)$ Verifies $A_{17}^* \overset{?}{=} A_{17}$ Thus, $SK_a = SK_c = SK$		

FIGURE 3. Login, authentication, and key agreement phase.

A_1. Then, SA invokes $SC = \{A_3, h(\cdot), P\}$ and transmits SC to U_a i.e., $SA \Longrightarrow U_a : SC = \{A_3, h(\cdot), P\}$.

- Then, U_a enumerates $HPID_a = h(HID_a||PW_a||\sigma_a)$ and $A_4 = h(HID_a||HPID_a||\sigma_a)$ employing pseudo identity HID_a, biometric B_a and PW_a. Lastly, U_a stores $\{A_3, A_4, h(\cdot), P\}$ in SC.

The summary for this phase is shown in Fig. 2.

D. LOGIN, AUTHENTICATION, AND KEY AGREEMENT PHASE

A user enters his login information during this phase, which is validated by the GW_b. To carry out the phase, U_a does the following.

- U_a inputs ID_a^*, PW_a^* and B_a^* into SC. Then, SC reckons $Rep(B_a^*, \theta_a) = \sigma_a^*$, $HID_a^* = h(ID_a^*||\sigma_a^*)$, $HPID_a^* = h(HID_a^*||PW_a^*||\sigma_a^*)$ and $A_4^* = h(HID_a^*||HPID_a^*||\sigma_a^*)$. Then, verifies $A_4^* \overset{?}{=} A_4$. Following that, SC generates a random nonce $r_a \in F_p^*$ and evaluates $HPW_a = h(PW_a||\sigma_a)$, $A_1 = h(HID_a||HPW_a)$, and $A_2 = A_3 \oplus A_1$. Further, SC enumerates $A_5 = h(HID_a||r_a||x_a||T_1)$, $A_6 = A_5.P$, $A_7 = A_5.P_b$, $A_8 = (A_2||HID_a||SN_{ID_c}) \oplus h(A_7||T_1)$ and $A_9 = h(A_2||A_7||A_8||HID_a||SN_{ID_c})$. Thus, $U_a \rightarrow GW_b : \{A_6, A_8, A_9, T_1\}$.
- Once the message has been received, GW_b checks $T_1 - T_1^* \leq \delta T$ and determines $A_7^* = A_6.x_b$, $(A_2||HID_a||SN_{ID_c}) = A_8 \oplus h(A_7^*||T_1)$. After that

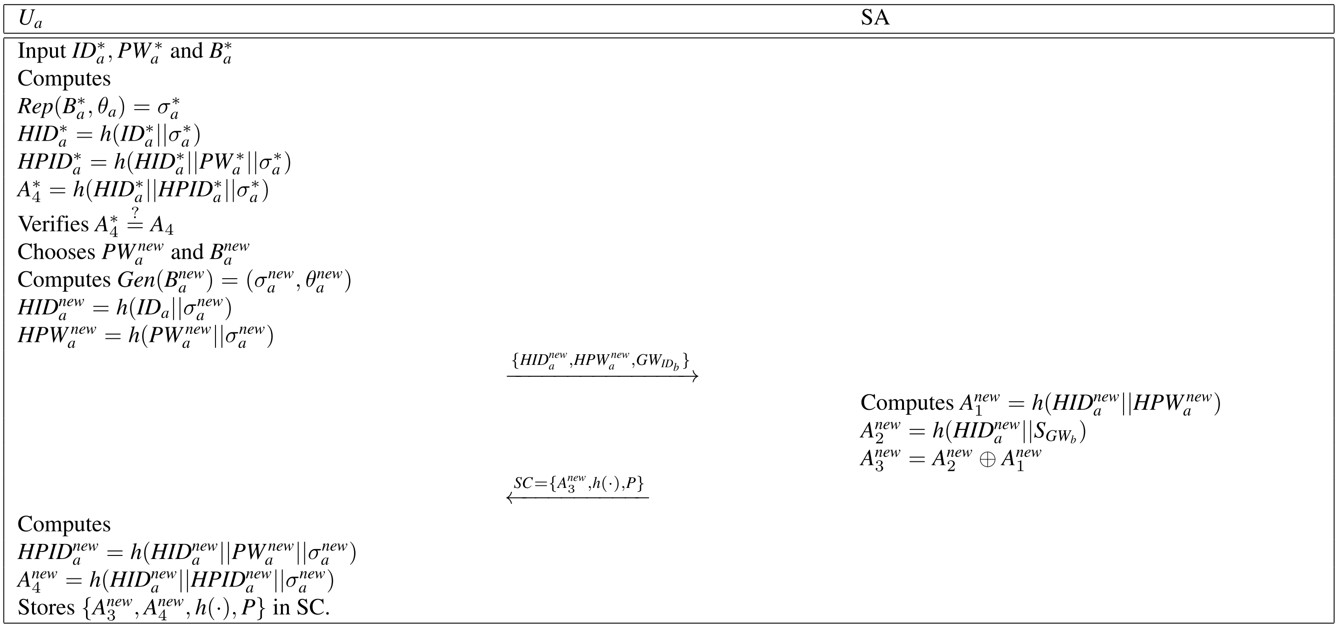


FIGURE 4. Password and biometric update phase.

GW_b computes $A_9^* = h(A_2||A_7^*||A_8||HID_a||SN_{ID_c})$ and corroborates $A_9^* \overset{?}{=} A_9$. If equality holds true, GW_b invokes $r_b \in F_p^*$ and evaluates $A_{10} = h(GW_{ID_b}||S_{SN_c}||r_b||x_b||T_2)$, $A_{11} = A_{10}.P$, $A_{12} = A_{10}.P_c$ and $A_{13} = h(S_{SN_c}||A_{12}||GW_{ID_b}||T_2)$. Afterward, $GW_b \rightarrow SN_c : \{A_{11}, A_{13}, T_2\}$.

- On receiving $\{A_{11}, A_{13}, T_2\}$, SN_c verifies, $T_2 - T_2^* \leq \delta T$ and then calculates $A_{12}^* = A_{11}.x_c$ and $A_{13}^* = h(S_{SN_c}||A_{12}^*||GW_{ID_b}||T_2)$. Thereafter, SN_c validates $A_{13}^* \overset{?}{=} A_{13}$. If true, SN_c prompts $r_c \in F_p^*$ and computes $A_{14} = h(SN_{ID_c}||r_c||x_c||T_3)$, $A_{15} = A_{14}.P$, $A_{16} = A_{14}.P_a$. Subsequently, SN_c enumerates the session key as $SK_c = h(A_{15}||A_{16}||x_c.P_a||T_3)$ and also computes $A_{17} = h(SK_c||A_{16}||T_3)$. Thus, $SN_c \rightarrow GW_b : \{A_{15}, A_{17}, T_3\}$. After receiving $\{A_{15}, A_{17}, T_3\}$, GW_b verifies $T_3 - T_3^* \leq \delta T$. Then, $GW_b \rightarrow U_a : \{A_{15}, A_{17}, T_3, T_4\}$.
- Firstly, U_a validates whether $T_4 - T_4^* \leq \delta T$. Following the verification of timestamp condition, U_a evaluates $A_{16}^* = A_{15}.x_a$ and the session key as $SK_a = h(A_{15}||A_{16}^*||x_a.P_c||T_3)$. Lastly, U_a computes $A_{17}^* = h(SK_a||A_{16}^*||T_3)$ and verifies $A_{17}^* \overset{?}{=} A_{17}$. Consequently, $SK_a = SK_c = SK$, thus the session key agreement holds.

The summary for this phase is shown in Fig. 3.

E. PASSWORD AND BIOMETRIC UPDATE PHASE

Due to security reasons, it is a good practice that a user should update his/her credential(s) frequently. In this phase, we explain the procedure for updating both the credentials, like password and biometrics of a registered user, say U_a. Note that U_a's biometric is not usually changed over the time. However, if U_a still wants to update the biometric, it is allowed in the proposed scheme. In case, if U_a desires to keep the old biometric, then it is taken as new biometric during this phase. The detailed procedure in step-wise is provided below.

- U_a inputs ID_a^*, PW_a^* and B_a^* into SC. Then, SC enumerates $Rep(B_a^*, \theta_a) = \sigma_a^*$, $HID_a^* = h(ID_a^*||\sigma_a^*)$, $HPID_a^* = h(HID_a^*||PW_a^*||\sigma_a^*)$ and $A_4^* = h(HID_a^*||HPID_a^*||\sigma_a^*)$. Then, verifies $A_4^* \overset{?}{=} A_4$. After successful authentication, U_a selects new password and biometric i.e., PW_a^{new}, B_a^{new} and computes $Gen(B_a^{new}) = (\sigma_a^{new}, \theta_a^{new})$, $HID_a^{new} = h(ID_a||\sigma_a^{new})$ and $HPW_a^{new} = h(PW_a^{new}||\sigma_a^{new})$. Thus, $U_a \rightarrow SA : \{HID_a^{new}, HPW_a^{new}, GW_{ID_b}\}$.
- On receiving the message, SA reckons $A_1^{new} = h(HID_a^{new}||HPW_a^{new})$, $A_2^{new} = h(HID_a^{new}||S_{GW_b})$ and $A_3^{new} = A_2^{new} \oplus A_1^{new}$. Then, SA invokes $SC = \{A_3^{new}, h(\cdot), P\}$ and transmits SC to U_a i.e., $SA \rightarrow U_a : SC = \{A_3, h(\cdot), P\}$.
- Then, U_a enumerates $HPID_a^{new} = h(HID_a^{new}||PW_a^{new}||\sigma_a^{new})$ and $A_4^{new} = h(HID_a^{new}||HPID_a^{new}||\sigma_a^{new})$. Lastly, U_a updates SC by superseding A_3 with A_3^{new} and A_4 with A_4^{new}.

The summary for this phase is shown in Fig. 4.

VI. SECURITY ANALYSIS

This section substantiates the security of the proposed work by performing the formal and the informal security analysis utilizing the BAN logic, ROR model, and scyther simulation tool.

A. FORMAL SECURITY ANALYSIS USING BAN LOGIC

We validate the mutual authentication and session key establishment of our approach using the BAN logic analysis.

TABLE 3. **BAN Logic notations.**

Symbol	Description
ρ_1, ρ_2	Principals
μ_1, μ_2	Statements
$\rho_1 \mid\equiv \mu_1$	ρ_1 believes μ_1
$\rho_1 \mid\sim \mu_1$	ρ_1 once said μ_1
$\rho_1 \lhd \mu_1$	ρ_1 receives μ_1
$\rho_1 \Rightarrow \mu_1$	ρ_1 controls μ_1
$(\mu_1)_k$	μ_1 is encrypted with key k
$\#\mu_1$	μ_1 is fresh
SK	Session Key
$\rho_1 \overset{k}{\leftrightarrow} \rho_2$	ρ_1 and ρ_2 communicate with shared key k

Furthermore, the authenticity and security of the information transmitted during the authentication phase are verified using the rules and assumptions mentioned below. Prior to establishing the goals, idealized forms, and assumptions, Table 3 displays the BAN logic notations.

1. Logical Postulates

- Nonce verification rule (NVR):

$$\frac{\rho_1 \mid\equiv \#(\mu_1),\ \rho_1 \mid\equiv \rho_2 \mid\sim \mu_1}{\rho_1 \mid\equiv \rho_2 \mid\equiv \mu_1}$$

- Message meaning rule (MMR):

$$\frac{\rho_1 \mid\equiv \rho_1 \overset{k}{\leftrightarrow} \rho_2,\ \rho_1 \lhd \{\mu_1\}_K}{\rho_1 \mid\equiv \rho_2 \mid\sim \mu_1}$$

- Jurisdiction Rule (JR):

$$\frac{\rho_1 \mid\equiv \rho_2 \mid\Rightarrow \mu_1,\ \rho_1 \mid\equiv \rho_2 \mid\equiv \mu_1}{\rho_1 \mid\equiv \mu_1}$$

- Freshness Rule (FR):

$$\frac{\rho_1 \mid\equiv \#(\mu_1)}{\rho_1 \mid\equiv \#(\mu_1, \mu_2)}$$

- Belief Rule (BR):

$$\frac{\rho_1 \mid\equiv (\mu_1, \mu_2)}{\rho_1 \mid\equiv \mu_1}$$

2. Goals

The following goals demonstrate the mutual authentication and session key agreement of the devised framework.

- G_1: $U_a \mid\equiv U_a \overset{SK}{\leftrightarrow} SN_c$
- G_2: $SN_c \mid\equiv U_a \overset{SK}{\leftrightarrow} SN_c$
- G_3: $U_a \mid\equiv SN_c \mid\equiv U_a \overset{SK}{\leftrightarrow} SN_c$
- G_4: $SN_c \mid\equiv U_a \mid\equiv U_a \overset{SK}{\leftrightarrow} SN_c$

3. Assumptions

The protocol is predicated on the following initial presumptions.

- $A_1 : GW_b \mid\equiv (U_a \overset{A_7}{\leftrightarrow} GW_b)$
- $A_2 : GW_b \mid\equiv \#(T_1)$
- $A_3 : SN_c \mid\equiv (GW_b \overset{A_{12}}{\leftrightarrow} SN_c)$
- $A_4 : SN_c \mid\equiv \#(T_2)$
- $A_5 : GW_b \mid\equiv (SN_c \overset{A_{16}}{\leftrightarrow} GW_b)$
- $A_6 : GW_b \mid\equiv \#(T_3)$
- $A_7 : U_a \mid\equiv (U_a \overset{A_{16}}{\leftrightarrow} GW_b)$
- $A_8 : U_a \mid\equiv \#(T_4)$
- $A_9 : SN_c \mid\equiv U_a \Rightarrow (U_a \overset{SK}{\leftrightarrow} SN_c)$
- $A_{10} : U_a \mid\equiv SN_c \Rightarrow (U_a \overset{SK}{\leftrightarrow} SN_c)$

4. Idealized Forms

The idealized forms of the devised protocol have been outlined as follows.

- $Msg^1 : U_a \rightarrow GW_b : \{A_6, A_8, A_9, T_1\}_{A_7}$
- $Msg^2 : GW_b \rightarrow SN_c : \{A_{11}, A_{13}, T_2\}_{A_{12}}$
- $Msg^3 : SN_c \rightarrow GW_b : \{A_{15}, A_{17}, T_3\}_{A_{16}}$
- $Msg^4 : GW_b \rightarrow U_a : \{A_{15}, A_{17}, T_3, T_4\}_{A_{16}}$

5. Proof Using Ban Logic

- D_1 is garnered from Msg^1.

$$D_1 : GW_b \lhd \{A_6, A_8, A_9, T_1\}_{A_7}$$

- According to D_1, A_1 and MMR, we have

$$D_2 : GW_b \mid\equiv U_a \mid\sim (A_6, A_8, A_9, T_1)$$

- According to D_2, A_2 and FR, we have

$$D_3 : GW_b \mid\equiv \#(A_6, A_8, A_9, T_1)$$

- Consolidating D_2, D_3 with NVR, we have

$$D_4 : GW_b \mid\equiv U_a \mid\equiv (A_6, A_8, A_9, T_1)$$

- According to D_4 and BR, we have

$$D_5 : GW_b \mid\equiv U_a \mid\equiv (A_6, A_8, A_9)$$

- D_6 is acquired from Msg^2.

$$D_6 : SN_c \lhd \{A_{11}, A_{13}, T_2\}_{A_{12}}$$

- According to D_6, A_3 and MMR, we have

$$D_7 : SN_c \mid\equiv GW_b \mid\sim (A_{11}, A_{13}, T_2)$$

- According to D_7, A_4 and FR, we have

$$D_8 : SN_c \mid\equiv \#(A_{11}, A_{13}, T_2)$$

- Amalgamating D_7, D_8 with NVR, we have

$$D_9 : SN_c \mid\equiv GW_b \mid\equiv (A_{11}, A_{13}, T_2)$$

- According to D_9 and BR, we have

$$D_{10} : SN_c \mid\equiv GW_b \mid\equiv (A_{11}, A_{13})$$

- Employing D_{10}, SN_c enumerates $A_{14} = h(SN_{ID_c}||r_c||x_c||T_3)$, $A_{15} = A_{14}.P$, $A_{16} = A_{14}.P_a$ and the session key as $SK_c = h(A_{15}||A_{16}||x_c.P_a||T_3)$. Therefore we have

$$D_{11} : SN_c \mid\equiv U_a \mid\equiv (U_a \overset{SK}{\leftrightarrow} SN_c)(Goal - 4)$$

- According to D_{11}, A_9 and JR, we have

$$D_{12} : SN_c \mid\equiv (U_a \overset{SK}{\leftrightarrow} SN_c)(Goal - 2)$$

- D_{13} is obtained from Msg^3.

$$D_{13} : GW_b \triangleleft \{A_{15}, A_{17}, T_3\}_{A_{16}}$$

- According to D_{13}, A_5 and MMR, we have

$$D_{14} : GW_b| \equiv SN_c| \sim (A_{15}, A_{17}, T_3)$$

- According to D_{14}, A_6 and FR, we have

$$D_{15} : GW_b| \equiv \#(A_{15}, A_{17}, T_3)$$

- Integrating D_{14}, D_{15} with NVR, we have

$$D_{16} : GW_b| \equiv SN_c| \equiv (A_{15}, A_{17}, T_3)$$

- According to D_{16} and BR, we have

$$D_{17} : GW_b| \equiv SN_c| \equiv (A_{15}, A_{17}, T_3)$$

- D_{18} is attained from Msg^4.

$$D_{18} : U_a \triangleleft \{A_{15}, A_{17}, T_3\}_{A_{16}}$$

- According to D_{18}, A_7 and MMR, we have

$$D_{19} : U_a| \equiv GW_b| \sim (A_{15}, A_{17}, T_3)$$

- According to D_{19}, A_8 and FR, we have

$$D_{20} : U_a| \equiv \#(A_{15}, A_{17}, T_3)$$

- Unifying D_{19}, D_{20} with NVR, we have

$$D_{21} : U_a| \equiv GW_b| \equiv (A_{15}, A_{17}, T_3)$$

- According to D_{21} and BR, we have

$$D_{22} : U_a| \equiv GW_b| \equiv (A_{15}, A_{17}, T_3)$$

- Employing D_{22}, U_a enumerates $A^*_{16} = A_{15}.x_a$ and the session key as $SK_a = h(A_{15}||A^*_{16}||x_a.P_c||T_3)$. Thus, we have

$$D_{23} : U_a| \equiv SN_c| \equiv (SN_c \overset{SK}{\leftrightarrow} U_a)(Goal - 3)$$

- According to D_{23}, A_5 and JR, we have

$$D_{24} : U_a| \equiv (SN_c \overset{SK}{\leftrightarrow} U_a)(Goal - 1)$$

B. INFORMAL ANALYSIS

In this part, we demonstrate the viability of our scheme against recognized threats and the accomplishment of the security functionalities.

1) REPLAY ATTACK

Assume that $\mathcal{A}$ intercepts and attempts to replay any message sent during the authentication phase. However, since all transmitted messages are equipped with fresh random nonces r_a, r_b, r_c and timestamps T_1, T_2, T_3, T_4, thus, $\mathcal{A}$ cannot replay any message, and the protocol is guarded against a "replay attack".

2) OFFLINE PASSWORD GUESSING ATTACK

Utilizing the user's smartcard data or the content of communications delivered across unsecured channels, $\mathcal{A}$ attempts to determine the user's password. Suppose that the $\mathcal{A}$ obstructs the messages Msg_1, Msg_2, Msg_3 and Msg_4. Also, $\mathcal{A}$ obtains the parameters $\{A_3, A_4, h(\cdot), P\}$ stored in the user's smart card by applying side-channel analysis attacks. Now, assume that $\mathcal{A}$ guesses user's password as PW^*_a. To further verify whether the guessed password is correct or not, $\mathcal{A}$ needs to compute $HPID_a = h(HID_a||PW_a||\sigma_a)$ and $A_4 = h(HID_a||HPID_a||\sigma_a)$. Nevertheless, the enumeration of both parameters requires the information of HID_a and σ_a, i.e., user's identity and biometrics, which are unknown to $\mathcal{A}$. As a result, $\mathcal{A}$ cannot verify the correctness of the guessed password PW^*_a. Thus, the devised framework is immune to "offline password guessing attack".

3) PRIVILEGED INSIDER ATTACK

In this attack, $\mathcal{A}$ obtains the user's registration message $\{HID_a, HPW_a, GW_{ID_b}\}$ and the smartcard parameters $\{A_3, A_4, h(\cdot), P\}$. Thereafter, $\mathcal{A}$ guesses users password as PW^*_a. However, to ensure the correctness of PW^*_a, $\mathcal{A}$ must compute $HPID_a = h(HID_a||PW_a||\sigma_a)$ and $A_4 = h(HID_a||HPID_a||\sigma_a)$. Since, the values HID_a and σ_a are unknown to $\mathcal{A}$, the computation of HID_a and σ_a is infeasible. Hence, our protocol is resistant to "privileged insider attack".

4) USER IMPERSONATION ATTACK

To impersonate the authentic user, an $\mathcal{A}$ must produce a duplicate message $\{A_6, A_8, A_9, T_1\}$, where $A_5 = h(HID_a||r_a||x_a||T_1)$, $A_6 = A_5.P$, $A_7 = A_5.P_b$, $A_8 = (A_2||HID_a||SN_{ID_c}) \oplus h(A_7||T_1)$ and $A_9 = h(A_2||A_7||A_8||HID_a||SN_{ID_c})$. Now, the computation of A_5 involves a fresh random nonce r_a and the user's private key x_a, both of which cannot be obtained by $\mathcal{A}$. Therefore, it is infeasible for $\mathcal{A}$ to calculate A_5 which makes the computation of A_6, A_7, A_8 and A_9 difficult. Resulting, our protocol is secure against "user impersonation attacks".

5) GATEWAY NODE IMPERSONATION ATTACK

To impersonate the gateway node, an $\mathcal{A}$ must produce a duplicate message $\{A_{11}, A_{13}, T_2\}$, where $A_{10} = h(GW_{ID_b}||S_{SN_c}||r_b||x_b||T_2)$, $A_{11} = A_{10}.P$, $A_{12} = A_{10}.P_k$ and $A_{13} = h(S_{SN_c}||A_{12}||GW_{ID_b}||T_2)$. Now, the computation of A_{10} involves a fresh random nonce r_b and the gateways private key x_b, both of which cannot be obtained by $\mathcal{A}$. Therefore, it is infeasible for $\mathcal{A}$ to calculate A_{10} which makes the computation of A_{11}, A_{12}, and A_{13} difficult. Resulting, our protocol is immunized against "gateway node impersonation attack".

6) SENSOR NODE IMPERSONATION ATTACK

To impersonate the sensor node, an $\mathcal{A}$ must produce a duplicate message $\{A_{15}, A_{17}, T_3\}$, where $A_{14} = h(SN_{ID_c}||r_c||x_c||T_3)$, $A_{15} = A_{14}.P$, and $A_{16} = A_{14}.P_a$. Now, the computation of A_{14} involves a fresh random nonce r_c and the sensor node's private key x_c, both of which cannot be obtained by $\mathcal{A}$. Therefore, it is infeasible for $\mathcal{A}$ to calculate A_{14} which makes the computation of A_{15}, A_{16}, and A_{17} difficult. Resulting, our protocol is protected against "sensor node impersonation attack".

7) PERFECT FORWARD SECRECY

Suppose that the $\mathcal{A}$ succeeds in obtaining the long term secrets x_a and x_c of U_a and SN_c. Further, the $\mathcal{A}$ impedes the messages transmitted through an insecure channel. Now, to compute SK, $\mathcal{A}$ requires the information of computed value A_{16}, private keys of both entities x_a, x_c and random nonces r_a, r_c. Since the random nonces are unknown to $\mathcal{A}$, computing A_{16} is equivalent to solving ECDHP. Thus, our scheme ensures "perfect forward secrecy".

8) SMART CARD STOLEN ATTACK

Assume that $\mathcal{A}$ can retrieve the information stored in users SC by applying a side-channel analysis attack and attempts to obtain ID_a and PW_a from A_4. Since A_4 is computed as $A_4 = h(HID_a||HPID_a||\sigma_a)$, where $HID_a = h(ID_a||\sigma_a)$ and $HPID_a = h(HID_a||PW_a||\sigma_a)$. Without the information of users ID_a and B_a, these parameters cannot be computed. Also, the users ID_a and PW_a have not been directly transmitted through public channels. Thus, there is no way to obtain users ID_a and PW_a. Hence, our protocol is secured against "smart card stolen attack".

9) ANONYMITY AND UNTRACEABILITY ATTACK

In our scheme, the identities of U_a and SN_c are not transmitted publicly and are masked using the biometric information of U_a. Therefore, the $\mathcal{A}$ cannot trace the identity through publicly transmitted messages. Thus, anonymity and untraceability are ensured.

10) SESSION KEY DISCLOSURE ATTACK

In the proposed protocol, both the entities, the U_a and SN_c evaluates the session key utilizing the computed parameters A_{15}, A_{16} with the private x_a, x_c and public keys P_a, P_c of both entities, where $A_{15} = A_{14}.P$, $A_{16} = A_{14}.P_a$ and $A_{14} = h(SN_{ID_c}||r_c||x_c||T_3)$. Since the computation of A_{14} involves the random nonce r_c and sensor node's private key x_c, therefore it is difficult for $\mathcal{A}$ to compute A_{14}. Without the information of A_{14}, $\mathcal{A}$ cannot compute A_{16} and so the session key SK_c. Thus, we can say that the direct computation of the session key is not possible.

11) EPHEMERAL SECRET LEAKAGE ATTACK

Suppose that the session random nonces r_a, r_b and r_c are revealed. Further, the $\mathcal{A}$ captures the messages $\{A_6, A_8, A_9, T_1\}$, $\{A_{11}, A_{13}, T_2\}$, $\{A_{15}, A_{17}, T_3\}$, and $\{A_{15}, A_{17}, T_3, T_4\}$. Now, the enumeration of $SK_c (= SK_a) = h(A_{15}||A_{16}||x_c.P_a||T_3)$ involves the computed values A_{15} and A_{16} in addition to the private keys of U_a and SN_c. Since the private keys cannot be obtained by $\mathcal{A}$, the protocol withstands "ephemeral secret leakage attack".

12) BY-PASSING ATTACK

Since our protocol is safeguarded from all types of impersonation attacks, therefore the $\mathcal{A}$ cannot by-pass any data. As a result, the protocol is protected against the "by-passing attack".

13) MUTUAL AUTHENTICATION

During the authentication phase, U_a transmits the login request message $\{A_6, A_8, A_9, T_1\}$ to GW_b. Then, GW_b verifies the timestamp condition and computes A_7^* and obtains $(A_2||HID_a||SN_{ID_c}) = A_8 \oplus h(A_7^*||T_1)$. Next, GW_b computes $A_9^* = h(A_2||A_7^*||A_8||HID_a||SN_{ID_c})$ and corroborates $A_9^* \overset{?}{=} A_9$. Thus, the user has been authenticated by the gateway. The gateway then sends the message $\{A_{11}, A_{13}, T_2\}$ to SN_c. Similarly, SN_c enumerates A_{12}^*, A_{13}^* and verifies $A_{13}^* \overset{?}{=} A_{13}$. Therefore, the U_a and GW_b both have been authenticated by the sensor node. Lastly, SN_c sends $\{A_{15}, A_{17}, T_3\}$ to GW_b, which on verifying the timestamp condition forwards the message $\{A_{15}, A_{17}, T_3, T_4\}$ to U_a. Thus, U_a evaluates A_{16}^*, SK_a, A_{17}^* and verifies $A_{17}^* \overset{?}{=} A_{17}$. Consequently, the devised framework ensures "mutual authentication".

14) SESSION KEY AGREEMENT

During the authentication phase, the SN_c computes the session key as $SK_c = h(A_{15}||A_{16}||x_c.P_a||T_3)$, whereas U_a evaluates $SK_a = h(A_{15}||A_{16}^*||x_a.P_c||T_3)$. Clearly, $SK_c = SK_a = SK$. Therefore, the "session key agreement" holds.

C. FORMAL SECURITY ANALYSIS USING ROR MODEL

The "Real-Or-Random (ROR) model" [8] leverages the extensively used DY model [48], which gives the attacker comprehensive control over all communications. Consequently, employing the below-discussed *Send*, *Execute*, *CorruptSC*, *Reveal*, and *Test* queries, $\mathcal{A}$ can eavesdrop, intercept, modify, insert, fabricate, or even delete messages that are transmitted between U_a and SN_c [25]. The entities $I_{U_a}^{y_1}, I_{SN_c}^{y_2}, I_{GN_b}^{y_3}$ delineates the user, sensor node, and gateway node where y_1, y_2 and y_3 indicates the y_1-th, y_2-th and y_3-th instance of the participants. The depiction of the above queries is as follows:

- $Execute(I_{U_a}^{y_1}, I_{SN_c}^{y_2})$: An $\mathcal{A}$ utilizes this query to simulate a passive eavesdropping attack and receives all messages exchanged between the two authorized communication parties, $I_{U_a}^{y_1}$ and $I_{SN_c}^{y_2}$.
- $CorruptSC$ $(I_{U_a}^{y_1}, I_{SN_c}^{y_2})$: This query enables the $\mathcal{A}$ to restore or extract the information stored on the $I_{U_a}^{y_1}$ or $I_{SN_c}^{y_2}$ smart device.
- $Send(I^y, message)$: The $\mathcal{A}$ sends a message to a participant instance I^y using this query in order to get a response from I^y, simulating an active attack.

- *Reveal*(I^y): The $\mathcal{A}$ can obtain the current session key SK, that I^{y_1} and I^{y_2} have agreed upon by executing this query.
- *Test*(I^y): The execution of this query examines the semantic security of the established SK between $I^{y_1}_{U_a}$ and $I^{y_2}_{SN_c}$ while adhering to the indistinguishability of the ROR paradigm. At first, an impartial coin c is flipped, and the result is kept confidential. If the $\mathcal{A}$ runs this query and creates a SK, the I^{y_1} will either return a random value when c equals 0 or SK when c equals 1.

Freshness: Instances $I^{y_1}_{U_a}$ or $I^{y_2}_{SN_c}$ are esteemed as fresh if the $\mathcal{A}$ acquires the negotiated session key between the U_a, SN_c via the $Reveal(I^y)$ query.

Partnering: If the three conditions listed below are met concurrently, two occurrences I^{y_1} and I^{y_2} are said to be paired.

1) Instances I^{y_1} and I^{y_2} are in acceptable states.
2) Instances I^{y_1} and I^{y_2} are each other's mutual partners.
3) Instances I^{y_1} and I^{y_2} have mutually authenticated one another and assigned the same session ID.

Semantic security: If the $\mathcal{A}$ can determine whether the result returned by the $Test(I^y)$ query is SK or not, then we say that the $\mathcal{A}$ has breached the semantic security. The outcome of the $Test(I^y)$ query must be consistent with regard to bit c. The experiment concludes with a bit c' being returned. If $c' = c$, $\mathcal{A}$ has a chance of winning. Further, if $Adv_{\mathcal{A},Game}$ indicates an outcome in which $\mathcal{A}$ successfully wins the game, $\mathcal{A}$'s advantage in breaching the semantic security of the proposed scheme, let's say s becomes $Adv_s(t) = |2Adv_{\mathcal{A},Game} - 1|$. Therefore, if $Adv_s(t) \leq \gamma$, for any sufficiently small $\gamma > 0$, s is secure in the ROR sense.

Theorem 1. *Suppose that $\mathcal{A}$ signifies the probabilistic polynomial time adversary intending to breach the semantic security of the protocol. The probability that the session key security of the suggested approach would be breached in running time t is given by $Adv_s(t)$. Additionally, $Adv_s^{ECDHP}(t)$ is defined as the $\mathcal{A}$'s advantage of breaking ECDHP. Therefore,*

$$Adv_s(t) \leq \frac{q_{hash}^2}{|Hash|} + \frac{q_s}{2^{l-1}|d_p|} + 2Adv_s^{ECDHP}(t)$$

where $q_s, q_{hash}, |Hash|, d_p, l$ indicates the number of send queries, hash queries, the size of the Hash query space, size of the password dictionary, the bits of U_a's biometric information respectively.

Proof: In the formal proof, $Game_n : n = 0, 1, 2, 3, 4$, there are five games that appear sequentially. The probability of $\mathcal{A}$ winning the game is defined as $Adv_{\mathcal{A},Game_n}$. The following provides an in-depth description of the game $Game_n$:

- $Game_0$: Here, in this game, $\mathcal{A}$ executes the first significant attack on the protocol and guesses c bits prior to the game's commencement to ensure the semantic security of the SK.

$$Adv_s(t) = |2Adv_{\mathcal{A},Game_0} - 1| \tag{1}$$

- $Game_1$: In $Game_1$, $\mathcal{A}$ runs the $Execute(I^{y_1}_{U_a}, I^{y_2}_{SN_c})$ query and intercepts the messages $\{A_6, A_8, A_9, T_1\}$, $\{A_{11}, A_{13}, T_2\}$, $\{A_{15}, A_{17}, T_3\}$, and $\{A_{15}, A_{17}, T_3, T_4\}$. After that, $\mathcal{A}$ runs $Reveal(I^y)$ and $Test(I^y)$ queries to determine if the derived SK is accurate. In the proposed protocol, the U_a or SN_c computes the session key as $SK_c = h(A_{15}||A_{16}||x_c.P_a||T_3)$ or $SK_a = h(A_{15}||A^*_{16}||x_a.P_c||T_3)$ where $A_{15} = A_{14}.P$, $A_{16} = A_{14}.P_a$ and $A_{14} = h(SN_{ID_c}||r_c||x_c||T_3)$. The enumeration of the session key relies on the ephemeral long and short-term secrets x_a, x_c and r_c, which are difficult for the $\mathcal{A}$ to obtain. Consequently, there is no difference in the probabilities of $Game_0$ and $Game_1$. Thus,

$$Adv_{\mathcal{A},Game_0} = Adv_{\mathcal{A},Game_1} \tag{2}$$

- $Game_2$: In $Game_2$, to retrieve the session key, $\mathcal{A}$ conducts *Hash* and $Send(I^y, message)$ queries. By altering the exchanged messages, $\mathcal{A}$ initiates an attack attempt. However, to forge any message generated by a legitimate entity, $\mathcal{A}$ requires the ephemeral short and long-term secrets such as random numbers and private keys of U_a, SN_c. Furthermore, $\mathcal{A}$ is unaware of the parameters like $HID_a, SN_{ID_c}, S_{SN_c}$ used to construct these messages as they are not conveyed through the public channel. Consequently, using the results of the birthday paradox, we can draw the following conclusion.

$$|Adv_{\mathcal{A},Game_2} - Adv_{\mathcal{A},Game_1}| \leq \frac{q_{hash}^2}{2|Hash|} \tag{3}$$

- $Game_3$: $Game_3$ necessitates the enforcement of *CorruptSC* $(I^{y_1}_{U_a}, I^{y_2}_{SN_c})$ query for the enumeration of SK. The side channel analysis attack allows $\mathcal{A}$ to retrieve data from the U_a or SN_c database. Resulting, $\mathcal{A}$ is aware of the values $\{S_{SN_c}, SN_{ID_c}, GW_{ID_b}\}$ and $\{A_3, A_4, h(\cdot), P\}$. Further, the evaluation of SK can be made feasible by $\mathcal{A}$ only if he can access ID_a, PW_a and B_a in addition to ephemeral short and long term secrets such as random numbers and private keys of U_a, SN_c. $\mathcal{A}$ can also attempt to obtain ID_a, PW_a by applying the thesaurus attack. However, the utilization of the fuzzy extractor function makes the probability of guessing l bits equivalent to $1/2^l$. In light of this, the following conclusion can be derived.

$$|Adv_{\mathcal{A},Game_3} - Adv_{\mathcal{A},Game_2}| \leq \frac{q_{send}}{2^l|d_p|} \tag{4}$$

- $Game_4$: In $Game_4$, $\mathcal{A}$ impedes $\{A_6, A_8, A_9, T_1\}$, $\{A_{11}, A_{13}, T_2\}$, $\{A_{15}, A_{17}, T_3\}$, and $\{A_{15}, A_{17}, T_3, T_4\}$ and utilizes A_{15} to enumerate SK. However, the utilization of the ECDHP complexity ensures the security of A_{16}, $x_a.x_c.P$, making it computationally hard for the $\mathcal{A}$ to enumerate SK. Therefore, we arrive at the following conclusion.

$$|Adv_{\mathcal{A},Game_4} - Adv_{\mathcal{A},Game_3}| \leq Adv_s^{ECDHP}(t). \tag{5}$$

Lastly, $\mathcal{A}$ estimates bit c by implementing $Test(I^y)$ query, and the outcome is as follows.

$$Adv_{\mathcal{A},Game_4} = \frac{1}{2} \tag{6}$$

We can arrive at the following equation by considering equations (1),(2), and (6).

$$\begin{aligned} \frac{1}{2}Adv_s(t) &= |Adv_{\mathcal{A},Game_0} - \frac{1}{2}| \\ &= |Adv_{\mathcal{A},Game_1} - \frac{1}{2}| \\ &= |Adv_{\mathcal{A},Game_1} - Adv_{\mathcal{A},Game_4}| \end{aligned} \tag{7}$$

The following result can be obtained from (7) by incorporating (3), (4), and (5) with the triangle inequality.

$$\begin{aligned} |Adv_{\mathcal{A},Game_1} - Adv_{\mathcal{A},Game_4}| &\leq |Adv_{\mathcal{A},Game_1} - Adv_{\mathcal{A},Game_3}| \\ &\quad + |Adv_{\mathcal{A},Game_3} - Adv_{\mathcal{A},Game_4}| \\ &\leq |Adv_{\mathcal{A},Game_1} - Adv_{\mathcal{A},Game_2}| \\ &\quad + |Adv_{\mathcal{A},Game_2} - Adv_{\mathcal{A},Game_3}| \\ &\quad + |Adv_{\mathcal{A},Game_3} - Adv_{\mathcal{A},Game_4}| \\ &\leq \frac{q_{hash}^2}{2|Hash|} + \frac{q_{send}}{2^l|d_p|} \\ &\quad + Adv_s^{ECDHP}(t). \end{aligned} \tag{8}$$

Consequently, by combining (7) and (8), we can arrive at

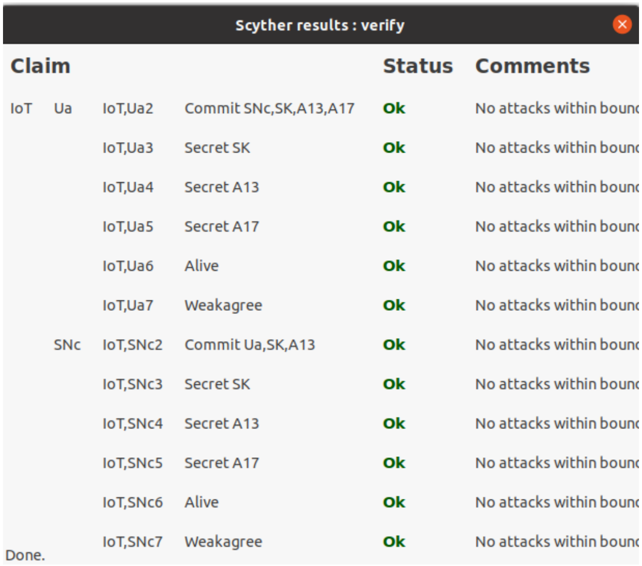
$$Adv_s(t) \leq \frac{q_{hash}^2}{|Hash|} + \frac{q_{send}}{2^{l-1}|d_p|} + 2Adv_s^{ECDHP}(t) \tag{9}$$

■

D. FORMAL SECURITY ANALYSIS VIA SCYTHER

The proposed scheme will be formally analysed in this part using the Scyther tool in the following configurations: CPU: 2.80 GHz Intel Core(TM) i7-1165G7; RAM:16 GB. Scyther is an automated security scheme verification tool that may be used to identify potential security issues and attacks. Many researchers have used it to assess various security systems in earlier related work. In this study, we use the Scyther tool to assess the proposed scheme's features, with a particular emphasis on confidentiality, defence against replay attacks, and man-in-the-middle attacks. The description of the scheme is written in Security Protocol Description Language (SPDL), and Scyther offers a graphical user interface, together with the Scyther command line tool and Python scripting interface. The DY model serves as the foundation for Scyther's adversary model, which is predefined. Scyther is utilised in the simulation results to make sure that the private information used by the suggested scheme is protected from attackers during scheme execution.

Finally, weakagree provides protection from impersonation attacks. The security verification and characterization results of the devised method using the scyther tool are shown in Fig. 5 and 6, respectively.

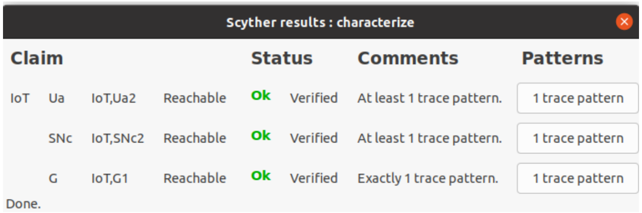


Scyther results : verify

Claim				Status	Comments
IoT	Ua	IoT,Ua2	Commit SNc,SK,A13,A17	Ok	No attacks within bounc
		IoT,Ua3	Secret SK	Ok	No attacks within bounc
		IoT,Ua4	Secret A13	Ok	No attacks within bounc
		IoT,Ua5	Secret A17	Ok	No attacks within bounc
		IoT,Ua6	Alive	Ok	No attacks within bounc
		IoT,Ua7	Weakagree	Ok	No attacks within bounc
	SNc	IoT,SNc2	Commit Ua,SK,A13	Ok	No attacks within bounc
		IoT,SNc3	Secret SK	Ok	No attacks within bounc
		IoT,SNc4	Secret A13	Ok	No attacks within bounc
		IoT,SNc5	Secret A17	Ok	No attacks within bounc
		IoT,SNc6	Alive	Ok	No attacks within bounc
		IoT,SNc7	Weakagree	Ok	No attacks within bounc

Done.

FIGURE 5. Security verification result of devised scheme.



Scyther results : characterize

Claim				Status		Comments	Patterns
IoT	Ua	IoT,Ua2	Reachable	Ok	Verified	At least 1 trace pattern.	1 trace pattern
	SNc	IoT,SNc2	Reachable	Ok	Verified	At least 1 trace pattern.	1 trace pattern
	G	IoT,G1	Reachable	Ok	Verified	Exactly 1 trace pattern.	1 trace pattern

Done.

FIGURE 6. Security characterization result of devised scheme.

VII. PERFORMANCE ANALYSIS

This section presents a thorough comparison of our proposed scheme with analogous schemes, such as the schemes of Servati and Safkhani [6], Li et al. [38], Sureshkumar et al. [40], Wang et al. [51], and Rangwani et al. [52] in terms of "security functionalities," "computation costs," and "computation costs."

A. SECURITY FEATURES

We contrast the proposed protocol's security properties with those of analogous protocols [6], [38], [40], [51], [52] in Table 4. The following lists the security characteristics utilized for comparison and the notations used to represent them. A_1 : Replay attack; A_2 : Offline password guessing attack; A_3 : Privileged insider attack; A_4 : User impersonation attack; A_5 : Gateway impersonation attack; A_6 : Sensor node impersonation attack; A_7 : By-passing attack; A_8 : Ephemeral secret leakage attack; A_9 : Mutual authentication and key agreement; A_{10} : Perfect forward secrecy; A_{11} : User anonymity and untraceability attack; A_{12} : Smart card stolen attack; A_{13} : Session key disclosure attack. Table 4 clearly indicates that in contrast to earlier schemes, the

TABLE 4. Comparison based on resistance to various attacks.

Security features	[6]	[38]	[40]	[51]	[52]	Proposed
A_1	✓	×	✓	✓	×	✓
A_2	×	✓	✓	✓	✓	✓
A_3	✓	×	✓	✓	✓	✓
A_4	×	✓	✓	–	×	✓
A_5	×	✓	✓	–	×	✓
A_6	×	✓	✓	–	✓	✓
A_7	×	–	–	–	✓	✓
A_8	×	×	–	–	✓	✓
A_9	✓	✓	✓	✓	✓	✓
A_{10}	✓	✓	✓	✓	✓	✓
A_{11}	✓	✓	×	✓	✓	✓
A_{12}	✓	–	✓	✓	✓	✓
A_{13}	✓	–	×	–	✓	✓

Note: ✓: Secure; ×: Insecure; -: Not considered

TABLE 5. Execution time of the cryptographic operations.

Operations	Notations	Time (*ms*)
Hash function (*h*)	T_h	0.5
ECC point addition (*pa*)	T_{pa}	7.01
ECC point multiplication (*pm*)	T_{pm}	0.442
Modular exponentiation (mod)	T_{mod}	3.85
Fuzzy extractor (*fe*)	T_{fe}	0.442

proposed method provides better security and functionality characteristics.

B. COMPUTATION COST

We examine and contrast the computation costs of the suggested approach with those of analogous techniques. We concentrate on the login and authentication phases and do not take into account XOR or concatenation operations because of their brief execution times. We employ the execution times of several operations from [6], [38], and [53], displayed in Table 5, to examine the computation cost. In the proposed work, the user utilizes ten hash ($10T_h$), four point multiplication ($4T_{pm}$), and one fuzzy extractor function (T_{fe}) operation, which adds up to a total cost of 7.21 ms, i.e., $4T_{pm} + 10T_h + T_{fe}$ (=7.21 ms). Next, the gateway employs four hash ($4T_h$) and three point multiplication ($3T_{pm}$) operation, which gives a total of 3.326 ms, i.e., $3T_{pm} + 4T_h$ (=3.326 ms). Lastly, the sensor node exploits four hash ($4T_h$) and four point multiplication ($4T_{pm}$) operations, which gives a total of 3.768 ms, i.e., $4T_{pm} + 4T_h$ (=3.768 ms). Thus, the total cost of all three entities is 14.304 ms. Further, the computational operations utilized by [6], [38], [40], [51], and [52] are presented in Table 6. From Table 6 and Fig. 7, it can be seen that the devised framework offers the lowest computational overheads of all alternatives. The proposed approach is hence effective in terms of computation.

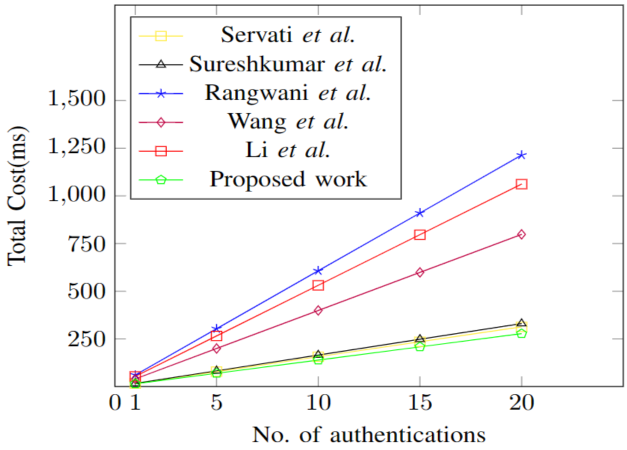


FIGURE 7. Computational cost concerning the number of authentications.

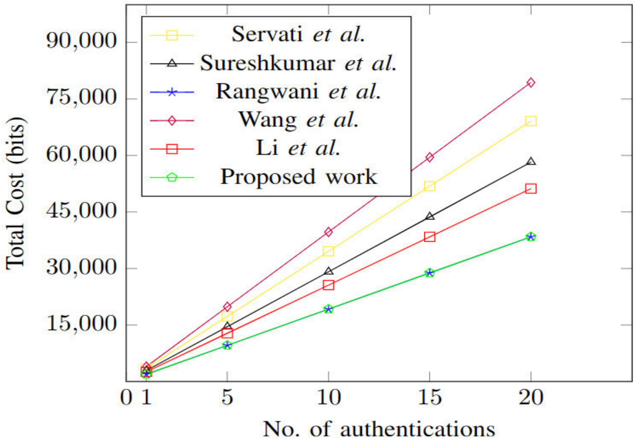


FIGURE 8. Communication cost concerning the number of authentications.

C. COMMUNICATION COST

Here, we examine the communication cost of the proposed work with [6], [38], [40], [51], and [52]. The communication cost of the various parameters mentioned below is given in accordance with [6]. The identities (U_a, SN_c), password, and symmetric encryption/decryption operation each require a length of 128 bits, whereas the hash function, random nonce, and elliptic curve point require 256 bits. Additionally, the time stamp uses 32 bits, respectively. In the proposed work, the user employs one elliptic curve point, one hash value, one mixed-bit message, and one timestamp operation to transmit

TABLE 6. Cost comparison.

S.No	Protocol	Computational operations	Computation cost	Communication cost
1	Servati and Safkhani [6]	$15T_{pm} + 18T_h$	15.63 ms	3456 bits
2	Li *et al.* [38]	$22T_h + 6T_{pa}$	53.06 ms	2560 bits
3	Sureshkumar *et al.* [40]	$17T_{pm} + 18T_h$	16.514 ms	2912 bits
4	Wang *et al.* [51]	$25T_h + T_{fe} + 7T_{mod}$	39.892 ms	3968 bits
5	Rangwani *et al.* [52]	$7T_{pm} + 17T_h + 7T_{pa}$	60.664 ms	1920 bits
6	Proposed	$11T_{pm} + 18T_h + T_{fe}$	14.304 ms	1920 bits

message $\{A_6, A_8, A_9, T_1\}$. Thus, the communication cost for U_a is $256+256+256+32 = 800$ bits. Similarly, the gateway utilizes one elliptic curve point, one hash value, and two time stamp operations to transmit messages $\{A_{11}, A_{13}, T_2\}$, $\{A_{15}, A_{17}, T_3, T_4\}$, which adds to a total cost of $256 + 256 + 32+32 = 576$ bits. Lastly, the sensor node utilizes one elliptic curve point, one hash value, and one timestamp operation to transmit messages $\{A_{15}, A_{17}, T_3\}$ which gives a total cost of $256 + 256 + 32 = 544$ bits. Consequently, the total cost for the proposed work is $800 + 576 + 544 = 1920$ bits. It is abundantly clear from Table 6 and Fig. 8 that the proposed work delivers the lowest cost among all competing techniques.

VIII. CONCLUSION

In this article, we scrutinize the scheme proposed by Servati and Safkhani and discuss its security weaknesses. Our findings exemplify that the proposed work is insecure against user, server, and gateway node impersonation attacks. Additionally, the protocol fails to resist offline password guessing, ephemeral secret leakage, and gateway-by-passing attacks. Therefore, to alleviate the security threats, we devised an enhanced framework by employing the benefits of ECC and the fuzzy extractor technique. The state-of-art formal and informal security analysis of the proposed work utilizing BAN logic, ROR model, and scyther simulation epitomizes the sturdiness of the devised scheme concerning the venomous attacks. Furthermore, the complexity evaluation of the devised protocol concerning the preexisting works substantiates that it outperforms them. Consequently, the presented work is practically implementable in real-world situations due to its low computation overheads. In future, we would like to design the testbed experiments of the proposed scheme and want to evaluate the performance parameters in a real-world environment. In addition, we would also like to apply blockchain technology to provide tamper-proof and transparent authentication records, decentralized identity management, and secure data sharing while ensuring privacy and data integrity.

REFERENCES

[1] S. Yu and Y. Park, "A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions," *IEEE Internet Things J.*, vol. 9, no. 20, pp. 20214–20228, Oct. 2022.

[2] L. Zhang, Y. Zhang, S. Tang, and H. Luo, "Privacy protection for E-health systems by means of dynamic authentication and three-factor key agreement," *IEEE Trans. Ind. Electron.*, vol. 65, no. 3, pp. 2795–2805, Mar. 2018.

[3] O. S. Albahri, A. A. Zaidan, B. B. Zaidan, M. Hashim, A. S. Albahri, and M. A. Alsalem, "Real-time remote health-monitoring systems in a medical centre: A review of the provision of healthcare services-based body sensor information, open challenges and methodological aspects," *J. Med. Syst.*, vol. 42, no. 9, pp. 1–47, Sep. 2018.

[4] H. Taleb, A. Nasser, G. Andrieux, N. Charara, and E. M. Cruz, "Wireless technologies, medical applications and future challenges in WBAN: A survey," *Wireless Netw.*, vol. 27, no. 8, pp. 5271–5295, Nov. 2021.

[5] C.-C. Chang, W.-Y. Hsueh, and T.-F. Cheng, "A dynamic user authentication and key agreement scheme for heterogeneous wireless sensor networks," *Wireless Pers. Commun.*, vol. 89, no. 2, pp. 447–465, Jul. 2016.

[6] M. R. Servati and M. Safkhani, "ECCbAS: An ECC based authentication scheme for healthcare IoT systems," *Pervas. Mobile Comput.*, vol. 90, Mar. 2023, Art. no. 101753.

[7] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990.

[8] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. 8th Int. Workshop Theory Pract. Public Key Cryptogr.*, Les Diablerets, Switzerland: Springer, Jan. 2005, pp. 65–84.

[9] C. J. Cremers, "The scyther tool: Verification, falsification, and analysis of security protocols: Tool paper," in *Proc. 20th Int. Conf. Comput. Aided Verification (CAV)*, Princeton, NJ, USA: Springer, Jul. 2008, pp. 414–418.

[10] N. Radhakrishnan and M. Karuppiah, "An efficient and secure remote user mutual authentication scheme using smart cards for telecare medical information systems," *Informat. Med. Unlocked*, vol. 16, 2019, Art. no. 100092.

[11] A. K. Das and B. Bruhadeshwar, "An improved and effective secure password-based authentication and key agreement scheme using smart cards for the telecare medicine information system," *J. Med. Syst.*, vol. 37, no. 5, p. 9969, Oct. 2013.

[12] S. Chatterjee and A. K. Das, "An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks," *Secur. Commun. Netw.*, vol. 8, no. 9, pp. 1752–1771, Jun. 2015.

[13] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card," *Peer-Peer Netw. Appl.*, vol. 9, no. 1, pp. 171–192, Jan. 2016.

[14] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K. R. Choo, and Y. Park, "Certificateless-signcryption-based three-factor user access control scheme for IoT environment," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3184–3197, Apr. 2020.

[15] M. Wazid, S. Thapliyal, D. P. Singh, A. K. Das, and S. Shetty, "Design and testbed experiments of user authentication and key establishment mechanism for smart healthcare cyber physical systems," *IEEE Trans. Netw. Sci. Eng.*, vol. 10, no. 5, pp. 2697–2709, Sep. 2023.

[16] B. Bera, A. K. Das, W. Balzano, and C. M. Medaglia, "On the design of biometric-based user authentication protocol in smart city environment," *Pattern Recognit. Lett.*, vol. 138, pp. 439–446, Oct. 2020.

[17] A. K. Das, N. R. Paul, and L. Tripathy, "Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem," *Inf. Sci.*, vol. 209, pp. 80–92, Nov. 2012.

[18] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100075.

[19] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018.

[20] S. Roy, S. Chatterjee, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services," *IEEE Access*, vol. 5, pp. 25808–25825, 2017.

[21] S. Banerjee, V. Odelu, A. K. Das, J. Srinivas, N. Kumar, S. Chattopadhyay, and K. R. Choo, "A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8739–8752, Oct. 2019.

[22] B. Bera, A. K. Das, and A. K. Sutrala, "Private blockchain-based access control mechanism for unauthorized UAV detection and mitigation in Internet of Drones environment," *Comput. Commun.*, vol. 166, pp. 91–109, Jan. 2021.

[23] A. K. Das, "A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks," *Int. J. Inf. Secur.*, vol. 11, no. 3, pp. 189–211, Jun. 2012.

[24] A. K. Das, "A secure and effective user authentication and privacy preserving protocol with smart cards for wireless communications," *Netw. Sci.*, vol. 2, nos. 1–2, pp. 12–27, May 2013.

[25] G. Thakur, P. Kumar, Deepika, S. Jangirala, A. K. Das, and Y. Park, "An effective privacy-preserving blockchain-assisted security protocol for cloud-based digital twin environment," *IEEE Access*, vol. 11, pp. 26877–26892, 2023.

[26] S. Malani, J. Srinivas, A. K. Das, K. Srinathan, and M. Jo, "Certificate-based anonymous device access control scheme for IoT environment," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9762–9773, Dec. 2019.

[27] M. Wazid, A. K. Das, and A. V. Vasilakos, "Authenticated key management protocol for cloud-assisted body area sensor networks," *J. Netw. Comput. Appl.*, vol. 123, pp. 112–126, Dec. 2018.

[28] 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.

[29] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, "Efficient end-to-end authentication protocol for wearable health monitoring systems," *Comput. Electr. Eng.*, vol. 63, pp. 182–195, Oct. 2017.

[30] S. U. Jan, S. Ali, I. A. Abbasi, M. A. A. Mosleh, A. Alsanad, and H. Khattak, "Secure patient authentication framework in the healthcare system using wireless medical sensor networks," *J. Healthcare Eng.*, vol. 2021, pp. 1–20, Jul. 2021.

[31] M. Fotouhi, M. Bayat, A. K. Das, H. A. N. Far, S. M. Pournaghi, and M. A. Doostari, "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT," *Comput. Netw.*, vol. 177, Aug. 2020, Art. no. 107333.

[32] S. Nashwan, "An end-to-end authentication scheme for healthcare IoT systems using WMSN," *Comput., Mater. Continua*, vol. 68, no. 1, pp. 607–642, 2021.

[33] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet Things J.*, vol. 9, no. 4, pp. 2649–2656, Feb. 2022.

[34] D. Kwon, Y. Park, and Y. Park, "Provably secure three-factor-based mutual authentication scheme with PUF for wireless medical sensor networks," *Sensors*, vol. 21, no. 18, p. 6039, Sep. 2021.

[35] D. He, S. Zeadally, N. Kumar, and J.-H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017.

[36] R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li, and F. Wu, "An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring," *J. Ambient Intell. Humanized Comput.*, pp. 1–22, Sep. 2018

[37] M. Shuai, B. Liu, N. Yu, and L. Xiong, "Lightweight and secure three-factor authentication scheme for remote patient monitoring using on-body wireless networks," *Secur. Commun. Netw.*, vol. 2019, pp. 1–14, Jun. 2019.

[38] 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.

[39] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, "Provably secure ECC-based device access control and key agreement protocol for IoT environment," *IEEE Access*, vol. 7, pp. 55382–55397, 2019.

[40] V. Sureshkumar, R. Amin, V. R. Vijaykumar, and S. R. Sekar, "Robust secure communication protocol for smart healthcare system with FPGA implementation," *Future Gener. Comput. Syst.*, vol. 100, pp. 938–951, Nov. 2019.

[41] V. Kumar, M. Ahmad, D. Mishra, S. Kumari, and M. K. Khan, "RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing," *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100213.

[42] J. Mo, Z. Hu, and Y. Lin, "Cryptanalysis and security improvement of two authentication schemes for healthcare systems using wireless medical sensor networks," *Secur. Commun. Netw.*, vol. 2020, pp. 1–11, Feb. 2020.

[43] M. A. Saleem, S. Shamshad, S. Ahmed, Z. Ghaffar, and K. Mahmood, "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.2019.2899580.

[44] M. Safkhani, C. Camara, P. Peris-Lopez, and N. Bagheri, "RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing," *Veh. Commun.*, vol. 28, Apr. 2021, Art. no. 100311.

[45] K. Sowjanya, M. Dasgupta, and S. Ray, "Elliptic curve cryptography based authentication scheme for Internet of medical things," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102761.

[46] S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang, "A secure and reliable device access control scheme for IoT based sensor cloud systems," *IEEE Access*, vol. 8, pp. 139244–139254, 2020.

[47] 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: Springer, May 2004, pp. 523–540.

[48] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[49] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Amsterdam, The Netherlands: Springer, Apr./May 2002, pp. 337–351.

[50] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptol. Conf.* Santa Barbara, CA, USA: Springer, Aug. 1999, pp. 388–397.

[51] C. Wang, G. Xu, and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks," *Sensors*, vol. 17, no. 12, p. 2946, Dec. 2017.

[52] D. Rangwani, D. Sadhukhan, S. Ray, M. K. Khan, and M. Dasgupta, "A robust provable-secure privacy-preserving authentication protocol for industrial Internet of Things," *Peer-Peer Netw. Appl.*, vol. 14, no. 3, pp. 1548–1571, May 2021.

[53] S. Itoo, M. Ahmad, V. Kumar, and A. Alkhayyat, "RKMIS: Robust key management protocol for industrial sensor network system," *J. Supercomput.*, vol. 79, pp. 1–29, Jan. 2023.

GARIMA THAKUR received the M.Sc. degree from the Central University of Himachal Pradesh, Dharamshala, India, where she is currently pursuing the Ph.D. degree. Her research interests include authentication, post-quantum cryptography, the IoT, and blockchain technology.

SUNIL PRAJAPAT (Associate Member, IEEE) received the M.Sc. degree in mathematics from the Central University of Himachal Pradesh, Dharamshala, Himachal Pradesh, India, where he is currently pursuing the Ph.D. degree with the Srinivasa Ramanujan Department of Mathematics. His research interests include quantum cryptography, post-quantum cryptography, coding theory, blockchain, and various applications of cryptographic primitives in the real world. He is a CSIR Fellow.

PANKAJ KUMAR received the M.Sc. degree from CCS University, Meerut, India, in 2005, and the Ph.D. degree from Galgotias University, in 2020. He has been an Assistant Professor with the Srinivasa Ramanujan Department of Mathematics, Central University of Himachal Pradesh, Dharamshala, Himachal Pradesh, India. He has published over 40 international academic research articles on information security and privacy preservation. His current research interests include cryptography, wireless network security, information theory, and network coding.

ASHOK KUMAR DAS (Senior Member, IEEE) received the M.Sc. degree in mathematics, the M.Tech. degree in computer science and data processing, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently a Full Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India, and a Visiting Faculty with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA, USA. His current research interests include cryptography, system and network security including security in smart grids, the Internet of Things (IoT), the Internet of Drones (IoD), the Internet of Vehicles (IoV), cyber-physical systems (CPS), cloud computing, intrusion detection, blockchain, AI/ML security, and post-quantum cryptography. He has authored over 375 papers in international journals and conferences in the above areas, including over 320 reputed journal articles. His Google Scholar H-index is 80 and his i10-index is 237 with more than 18 500 citations. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He served as one of the Technical Program Committee Chairs for the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, in June 2019, the International Conference on Applied Soft Computing and Communication Networks (ACN'20), Chennai, India, in October 2020, and the Second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, in October 2020. He has been listed as a Highly Cited Researcher (2022) from the Web of Science (Clarivate[1]) in recognition of his exceptional research performance. He served/serves on the editorial board for IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *Journal of Cloud Computing* (Springer), *Cyber Security and Applications* (Elsevier), *IET Communications*, *KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience).

SACHIN SHETTY (Senior Member, IEEE) received the Ph.D. degree in modeling and simulation from Old Dominion University, in 2007. He was an Associate Professor with the Department of Electrical and Computer Engineering, Tennessee State University, USA. He is currently a Professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University. He holds a joint appointment with the Department of Modeling, Simulation and Visualization Engineering and the Center for Cybersecurity Education and Research. He has authored or coauthored over 200 research articles in journals and conference proceedings and two books. His research interests include the intersection of computer networking, network security, and machine learning. He was a recipient of the DHS Scientific Leadership Award. He has served as the Technical Program Committee Member for ACM CCS, IEEE INFOCOM, IEEE ICDCN, and IEEE ICCCN.

• • •

---

[1] Trademarked.