A Three-Factor-Based Authentication Scheme of 5G Wireless Sensor Networks for IoT System

Shreeya Swagatika Sahoo, *Member, IEEE*, Sujata Mohanty, Kshira Sagar Sahoo, *Senior Member, IEEE*, Mahmoud Daneshmand, *Life Senior Member, IEEE*, and Amir H. Gandomi, *Senior Member, IEEE*

***Abstract*—Internet of Things (IoT) is an expanding technology that facilitate physical devices to interconnect each other over a public channel. Moreover, the security of the next-generation wireless mobile communication technology, namely, 5G with IoT, has been a field of much interest among researchers in the last several years. Previously, Sharif et al. have suggested an IoT-based lightweight three-party authentication scheme proclaiming a secured scheme against different threats. However, it was found that the scheme could not achieve user anonymity and guarantee session key security. Additionally, the scheme fails to provide proper authentication in the login phase, and it s unable to update a new password in the password change phase. Thus, we propose an improved three-factor-based data transmission authentication scheme (TDTAS) to address the weaknesses. The formal security analysis has been proved using the Real-or-Random (RoR) model. The informal security analysis demonstrates that the scheme is secure against several known attacks and achieves more security features. In addition, the comparison of the work with other related schemes demonstrates the proposed scheme has less communicational and storage costs.**

***Index Terms*—5G, authentication, biometric, elliptic curve cryptography (ECC), Internet of Things (IoT), Real-or-Random (RoR).**

I. Introduction

WIRELESS sensor networks (WSNs) have played an important role in the daily life of modern society and are widely used in several applications. 5G with WSN is essential for the establishment of Internet of Things (IoT) applications, such as smart grid [1], smart healthcare [2], [3], vehicular ad-hoc networks [4], [5], [6], and intelligent transportation system [7], [8], [9], [10]. By the support of 5G technology, the sensors are interconnected for sharing and collecting the data through WSNs over public channels in IoT environment [11]. The IoT devices gathered the data from their surrounding environment and sent them to the server. However, secure information exchange among the participants of the IoT environment is a challenging problem due to the open nature of the wireless channel and resource-constrained features of sensor nodes. Thus, key agreement and mutual authentication become essential security mechanisms to authenticate the participants.

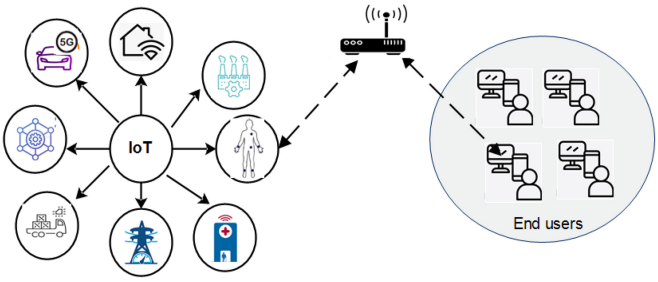


Fig. 1. Communication of data in IoT framework.

The communication in WSN consists of sensor nodes, gateway nodes, and users. It is becoming critical for monitoring and data collection in a variety of industrial environments. Industrial IoT (IIoT), a subset of the larger IoT, focuses on the specialized requirements of industrial applications, such as health monitoring, agriculture, military, industrial and consumer applications, etc. [12], [13], [14], [15], [16], [17], [18], [19]. WSNs have a significant role in the IIoT to create a smart environment.

The basic communication architecture of the IoT framework is illustrated in Fig. 1. The sensor nodes are distributed randomly in the selected or inaccessible environments and constantly monitor the area to collect information, such as humidity, pressure, sound, motion, light, temperature, etc. However, the sensor node faces several issues, such as low memory, low power, and battery limitations. A user can access the sensor with the help of a gateway node which acts as an intermediate between user and sensor nodes. Moreover, WSN in IoT architecture is of prominent use in 5G-enabled applications. The development 5G promises to fulfill the needs of complex IoT system. The 5G technology with IoT can be

Manuscript received 22 November 2022; revised 20 January 2023 and 11 March 2023; accepted 24 March 2023. Date of publication 1 May 2023; date of current version 24 August 2023. This work was supported in part by the Kempe Postdoctoral Fellowship under Project SMK21-0061, Sweden, and in part by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by Knut and Alice Wallenberg Foundation. *(Corresponding author: Amir H. Gandomi.)*

Shreeya Swagatika Sahoo is with the Department of CSE, Siksha 'O' Anusandhan University, Bhubaneswar 751019, India (e-mail: shreeya.swagatika@gmail.com).

Sujata Mohanty is with the Department of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela 769008, India (e-mail: sujatam@nitrkl.ac.in).

Kshira Sagar Sahoo is with the Department of Computing Science, Umeå University, 901 87 Umeå, Sweden (e-mail: ksahoo@cs.umu.se).

Mahmoud Daneshmand is with the School of Engineering and Science, Stevens Institute of Technology, Hoboken, NJ 07030 USA (e-mail: mdaneshm@stevens.edu).

Amir H. Gandomi is with the Faculty of Engineering and Information Technology, University of Technology Sydney, Sydney, NSW 2007, Australia, and also with the University Research and Innovation Center, Obuda University, 1034 Budapest, Hungary (e-mail: gandomi@uts.edu.au).

Digital Object Identifier 10.1109/JIOT.2023.3264565

easily access through all sort of low-power wide area network, such as WiFi and ZigBee [19].

It is obvious that the combination of 5G-enabled IoT devices and WSN steadily become closer and getting deeper into the private lives of human beings. If human personal data are breached by any means it may pose serious threats to human life. To make the system more robust, privacy preservation anonymity along with untraceability is a common approach. Anonymity conceals the identities of any type of participant so that they do not know who accesses data at a particular time. On the other hand, untraceability does not allow to trace of different sessions of publicly exchanged messages. Furthermore, the two phenomena, such as authorization and access control grant additionally check access rights and privileges according to the sensitivity of the data. Therefore, privacy preservation anonymity, authorization, and access control mechanisms are important issues for securing the WSN with a 5G-enabled IoT system.

A. Related Work

Das [20] introduced a smart card (SC)-based user authentication scheme for WSNs with high efficiency, which opens a new research direction in WSN environments. Later, Das's scheme was found vulnerable to an insider attack, impersonation attack, Denial-of-Service (DoS) attack, password guessing attack, and sensor node capture attack. In addition, the scheme could not achieve key agreement, mutual authentication, and user anonymity [21], [22], [23]. Yeh et al. presented a SC-based user authentication scheme for WSNs using elliptic curve cryptography (ECC), as it requires less key size and better security features compared to other public cryptosystems. Later several authentication schemes have been proposed for different applications based on ECC [24], [25], [26]. However, Han showed that the scheme presented by Yeh et al. could not achieve mutual authentication, perfect forward secrecy, and did not support key agreement among user, server, and sensor [27]. To overcome the above weaknesses, Shi and Gong [28] came up with an improved ECC-based authentication scheme and claimed that their scheme is efficient and can resist several attacks. However, Shi and Gong analyzed and pointed out that the scheme in [28], fails to preserve the stolen SC attack, sensor energy exhausting attack, and key sharing attack [29]. They have proposed an ECC-based authentication scheme for wireless network with high security and better efficiency.

In 2012, Xue et al. [30] suggested a lightweight temporal-credential-based mutual authentication scheme for WSNs. In the same year, Das et al. [31] suggested a dynamic password-based authentication scheme for hierarchical WSNs in which real-time data can be accessed directly by the authorized users. However, Turkanovic and Holbl [32] pointed out the flaws in [31], scheme and came up with an enhanced scheme to overcome these flaws. Meanwhile, Li et al. [33] found that the scheme in [30], is susceptible to stolen-verifier, insider attack, off-line password guessing attack, and SC loss attack. Furthermore, the scheme suffers from several logged-in user's attacks. Turkanović et al. [34] proposed a user authentication scheme for WSN. Nevertheless, the scheme was vulnerable to SC attack, sensor node spoofing attack, impersonation attack, and stolen verifier attack [35]. In addition, the scheme could not achieve forward and backward secrecy. He et al. [36] demonstrated that Xu et al.'s scheme could not resist user impersonation attack, sensor node impersonation attack, modification attack, and fail to achieve user anonymity. He et al. suggested a new temporal-based mutual authentication scheme to overcome these weaknesses. Later, Jiang et al. [37] found that He et al.'s scheme suffers from user impersonation attack, stolen SC attack, tracing attack, and failed to provide user untraceability. They proposed an improved ECC-based authentication scheme and claimed that the scheme could use for real-life applications. However, Li et al. [38] found some common flaws that are known-session specific temporary information attack, wrong password detection, and clock synchronization problem in schemes [30], [36], [37]. Recently, Ostad-Sharif et al. [39] pointed out that Amin et al.'s scheme and Jiang et al.'s scheme could not achieve perfect forward secrecy. Further, they proposed an authentication scheme pointing out that Amin et al.'s scheme suffers from a reply attack.

Chen et al. [40] proposed a temporal credential and dynamic ID-based secure authentication scheme for WSNs in IoT environments. In the same year, Kumar et al. [41] suggested an ECC-based three-factor authentication scheme for WSN. However, the scheme suffers from DoS attack, key compromise Impersonation attack, and lack of user revocation. Later, Vinoth et al. [42] proposed a multifactor authentication scheme using the secret sharing technology. The scheme is vulnerable to DoS attacks, Replay attack, and de-synchronization attacks. Recently, Wu et al. [43] proposed a lightweight biometric-based authentication for WSN providing session key security. The existing authentication schemes, used techniques, advantages, and the used domains are listed in Table I.

B. Research Contributions

Even though the schemes proposed by different researchers for WSN have advantages, but they are not completely suitable for 5G-enabled IoT environments. Further, the lack of proper standards for the IoT environment makes it susceptible to several security features. Recently, Ostad-Sharif et al. [39] proposed a lightweight three-factor-based authentication scheme for IoT networks. However, the scheme has a drawback in the session key computation, password change phase, and login phase. Thus, this study aims to improve Sharif et al.'s scheme by providing several security features while minimizing the overhead. In summary, the contributions are as follows.

1) We investigated Sharif et al.'s scheme and found various security flaws, such as violation of user anonymity, inefficient login and password change phase, and session key computation.
2) We presented an improved ECC-based authentication scheme called a three-factor-based data transmission authentication scheme (TDTAS), along with a fuzzy extractor to prevent the weakness of Sharif et al.'s scheme. Moreover, the proposed scheme provides sensor node addition and SC revocation phase.

TABLE I
COMPARISON OF EXISTING SCHEME

Year	Schema	Cryptographic Technique	Advantages	Tool Used	Domain
2018	Wazid *et al.* [44]	Hash Function	Three factor based Schema	AVISPA	Generic
2018	Shin *et al.* [45]	Hash function	Overhead is reduced	Cooja	Generic
2019	Chatterjee *et al.* [46]	Paillier cryptosystem	Three factor based Schema	AVISPA	WBAN
2019	Kumar *et al.* [47]	Hash Function	Overcome the limitation of Kumari et al.	AVISPA,NS2	Coal Mines
2020	Nikravan *et al.* [48]	Bilinear Pairing	Multi factor Authentication, Light weight	BAN Logic,ISPA	Generic
2020	Mirvaziri *et al.* [49]	Symmetric cryptography	HWSN	NS2	Generic
2021	Xie *et al.* [50]	Symmetric cryptography	Low Computing	ProVerif	Generic
2022	Hu *et al.* [51]	ECC	Light Weight	ProVerif	Generic

3) The Real-or-Random (RoR) model is used for formal security analysis, which ensures the session key security of the proposed scheme. Further, informal security analysis has been accomplished to strengthen the security of our scheme.
4) In terms of computational, communication, and storage costs, the TDTAS has been thoroughly compared to various existing schemes. Furthermore, the proposed system was formally validated using the AVISPA tool.

C. Organization

The remainder of the work is organized as follows. The next section demonstrates some related mathematical preliminaries to carry out the proposed scheme. A brief study on the Sharif et al.'s scheme is discussed in Section III. Section IV demonstrates the proposed scheme, along with its various phases. The formal security analysis using the RoR model and verification of the scheme using the AVISPA tool are presented in Sections V and VI, respectively. Section VII presents the performance analysis of the proposed scheme, and Section VIII concludes the study.

II. PRELIMINARIES

This section briefly presents some preliminaries which are used as the basis of the TDTAS.

A. Hash Function

The hash function is defined as $h : \{0, 1\}^* \rightarrow Z_p^*$, which takes a variable length of random input and gives a fixed length of the output. The one-way hash function has the following features.

1) It is difficult to find any input m that makes $y = h(m)$ for a given hash value y.
2) It is computationally infeasible to find any m_2 for a given m_1, such that $m_1 \neq m_2$, where $h(m_1) = h(m_2)$.
3) To find two different message (m_1, m_2) such that $h(m_1) = h(m_2)$ is an infeasible work.

Definition 1 (Collision-Resistant One-Way Function of Hash): It is a deterministic method that takes an arbitrary length of input and creates an output of fixed size l. If $Adv_A^{HASH}(t)$ is an advantage of $\mathcal{A}_v$ in identifying a collision, then we have

$Adv_A^{HASH}(t) = P[(m_1, m_2)\varepsilon_R A_v : m_1 \neq m_2, h(m_1) = h(m_2)]$ where $P[S]$ signifies the pair (m_1, m_2) randomly picked by $\mathcal{A}_v$ and $(m_1, m_2)\varepsilon_R A$ denotes the probability of the random event S. With execution time t, an $\mathcal{A}_v$ calculates the probability in advantage over the random value. If $Adv_A^{HASH}(t) \leq \varepsilon$, then hash function $h(\cdot)$ is collision resistant for any sufficiently small $\varepsilon \geq 0$.

B. Indistinguishability of Encryption Under Chosen Plaintext

The standard definitions of indistinguishability of encryptions (IND) due to Goldwasser and Micali [52] and Choo [53] and chosen-plaintext attack (CPA) is defined as follows. In CPA, an adversary is allowed to encrypt plaintexts of his choice. Thus, $\mathcal{A}_v$ can calculate a ciphertext for any plaintext with the knowledge of the public key.

Definition 2: Let, there are N different independent encryption oracles having several encryption keys. The advantages function of encryption is defined as $Adv_{P,E}^{IND-CPA}(k) = 2 \times |pr[(pk, sk) \leftarrow \mathcal{T}(k);\ (mg_0, mg_1, s) \leftarrow \mathcal{A}_1(k, pk);\ b \epsilon_R \{0, 1\};\ y \leftarrow \varepsilon_{pk}(m_b);\ b' \leftarrow \mathcal{A}_2(k, pk, y, s) : b = b']| - 1$, where (pk, sk) is the pair of public and secret keys of key generation algorithm T; E is the encryption algorithm which takes the public key pk and a message $x\ \varepsilon\{0, 1\}^*$ as input to produce a ciphertext y; and D is the decryption algorithm which takes secret key sk and cipher text y as input to produce message x. Two messages $\{mg_0, mg_1\}$ are provided by an adversary and bit b is choose by the challenger to compute the challenger cipher text y^*. $\mathcal{A}_v$ runs encryption algorithm on the input $\{y^*, pk\}$, which guess b' for b. If $b' = b$, then $\mathcal{A}v$ will win the indistinguishability game, and advantages in playing the game is $Adv_{P,\mathcal{A}_v}^{IND-CPA}(k) = |Pr[b' = b] - (1/2)|$.

C. Elliptic Curve Cryptography

The ECC provides less key size compared to other conventional cryptography, such as RSA, DSA, and DH. The properties of an ECC over a finite field as follows.

A nonsingular elliptic curve equation is defined as $y^2 = x^3 + ax + b \pmod p$ over a prime finite field Z_p, where $(a, b) \epsilon Z_p$ are constants such that $4a^3 + 27b^2 \pmod p \neq 0$, $Z_p = \{0, 1, 2 \ldots .(p - 1)\}$, p is a prime number greater than three. The scalar multiplication is obtained as $nP = P + P + P + \ldots P(n \text{ times}) = O$, where P be a base point on Z_p and O is called as the identity point at infinity or zero point.

Definition 3 [Elliptic Curve Discrete Logarithm Problem (ECDLP)]: Computing $Q = k \cdot P$ is relatively easy for given $k \epsilon Z_p$ and $Q \epsilon E_p$. However, given $P, Q \epsilon E_p$, to find an integer $k \epsilon [1, n - 1]$ such that $Q = k \cdot P$ is computational hard.

Definition 4 [Computational Diffie–Hellman Problem (ECDHP)]: Let P, aP, and bP are three points over an elliptic curve E_p. It is computational infeasible to find $abP \epsilon E_p$ without knowledge of a and b.

D. Fuzzy Extractor

A fuzzy extractor takes the biometric as input and outputs two random numbers. Using given biometric input ω, it can extract an almost random string σ [54]. The crucial thing about a fuzzy extractor is that it extracts the same output σ

TABLE II
NOTATIONS USED

Notation	Description
U_ι	ι^{th} User
GWN	Gateway Node
SN_k	Sensor Node
SA	System Administrator
SC	Smart Card
ID_ι	User Identity
PW_ι	User Password
$BM\iota$	User Biometric
ID_{gw}	GWN Identity
ID_{sj}	SN_k Identity
$\mathcal{A}_v$	Adversary
X_{GWN}, k	Master key of GWN
SK	Session key
$h(\cdot)$	One way hash function

when the input changes to ω' but the input remains near to ω. To recover σ, a uniformly random string θ will be produced from the ω'. It requires two procedures that are probabilistic generation procedure (*Gen*) and deterministic reproduction procedure (*Rep*).

1) *Gen* receives input $\omega \epsilon \psi$ and generates a random string $\sigma \epsilon \{0,1\}^l$ and a auxiliary string θ, $Gen(\omega) = (\sigma, \theta)$.
2) *Rep* procedure allows to receives input ω' close to input ω and corresponding random auxiliary string θ to recover σ, $Rep(\omega', \theta) = \sigma$.

E. Adversary Model

This section presents the adversarial model considering the following capabilities.

1) We have used the Dolev–Yao (DY) threat model in which two communicating parties can communicate with each other over an open channel [55]. An adversary $\mathcal{A}_v$ has control over the transmitted messages during the communication. He can eavesdrop, modify, or delete the message but cannot intercept a message over the secure channel.
2) The power analysis attack or reverse engineering procedures allow a $\mathcal{A}_v$ to easily compromise the secret parameters which are stored in the SC [56], [57].
3) An adversary can be an authorized entrusted entity or an outsider.
4) Moreover, $\mathcal{A}_v$ can guess a low entropy password, or master secret key but not simultaneously.

III. CRYPTANALYSIS ON SHARIF ET AL.'S SCHEME

Recently, Sharif et al.'s pointed out the flaws in Amin et al.'s and Jiang et al.'s scheme and proposed an improved authentication scheme for IoT networks. However, in this section, some security flaws of their scheme have been discussed. Table II listed the notation, which is used throughout this article.

A. Inefficient Login Phase

In the login phase, when a valid user needs to login, he inserts his SC into the card reader and get the parameter $D_\iota, C_\iota, E_\iota, SCN_\iota$. In addition he gives his biometric and compute $RN'_\iota = BK(H(B_\iota)) \oplus C_\iota$ and compare $C_\iota \stackrel{?}{=} C'_\iota$. However, he could not compute random number RN'_ι as C'_ι is not embedded in the SC. Thus, each time the login will fail, and the valid user could not get into the server.

B. Drawback in Password Change Phase

In this phase, U_ι needs to enter $ID_\iota, PW_\iota, B_\iota$ into the card reader. To complete the password change phase, SC checks the user validity by checking the condition $RPW_\iota \stackrel{?}{=} RPW'_\iota$, where $RPW'_\iota = h(ID_\iota \| PW_\iota \| RN_\iota)$. As discussed in the previous section, the computation of random number RN'_ι depends upon the C'_ι, which is unknown to the SC. As a result, a valid user could not change his password.

C. Drawback in the Computation of Session Key

The session key of user is calculated as $SK_\iota = h(ID_\iota \| ID_{sj} \| K_\iota \| K'_j)$, where K_ι and K'_j are two random numbers generated by user and sensor, respectively. The parameter ID_{sj} is not clearly mentioned, whether it is private or public. However, in both cases, the session key can be compromised.

Case-1: The assumption is ID_{sj} is private and only known to the sensor and gateway node. So, it is impossible for the U_ι to compute session key using ID'_{sj} as $SK_\iota = h(ID_\iota \| ID_{sj} \| K_\iota \| K'_j)$. Without a session key, the scheme is vulnerable to several attacks.

Case-2: Let, ID_{sj} is public and master key X_j is revealed. An adversary can eavesdrop the message $\{ID_{GWN}, M_6, M_7, M_8, T_4\}$ as it communicates through insecure channel. Now, he can compute $ID^*_\iota = M_7 \oplus h(ID_{GWN} \| X_j \| T_4)$, $K^*_\iota = M_8 \oplus h(ID^*_\iota \| X_j)$, $M'_6 = h(ID'_\iota \| ID_{sj} \| ID_{GWN} \| X_j \| K^*_\iota \| T_4)$ and checks $M_6 \stackrel{?}{=} M'_6$. The condition will get true and $\mathcal{A}_v$ generate a random number K^*_j of its own and computes $SK^*_j = h(ID^*_\iota \| ID_{sj} \| K^*_\iota \| K^*_j)$, $M^*_9 = h(SK_j \| X_j \| K^*_j \| T^*_5)$, $M^*_{10} = K^*_\iota \oplus K^*_j$. Finally, SN_k sends $\{M^*_9, M^*_{10}, T^*_5\}$ to the GWN through an insecure channel. Upon obtaining the parameters, GWN verifies the server by checking the condition $M'_9 \stackrel{?}{=} h(SK_{GWN} \| X_j \| K^*_j \| T_5)$, where $K^*_j = M_{10} \oplus K_\iota$, $SK^*_{GWN} = h(ID'_\iota \| ID_{sj} \| K'_\iota \| K'_j)$. Each time the verification will get true as ID_{sj} is public and $\mathcal{A}_v$ can easily fool the GWN. Thus, in case-1 the computation of session key is inefficient and in case-2 key is vulnerable.

1) Violation of User Anonymity: User anonymity is an important security features as it protects the real identity of a valid user. In Sharif et al.'s scheme, once an adversary obtain the public message $MSG_1 = \{M_1, M_2, M_3, T_1, SCT\iota, EID\iota\}$ and the secret key X_{GWN}, he tries to compute $SCN\iota^* = SCT\iota \oplus h(T\iota)$, $L^*_\iota = h(SCN^*_\iota \| X_{GWN})$, $ID^*_\iota = M_1 \oplus h(L^*_\iota \| T_1)$. Thus, the scheme could not achieve user anonymity.

IV. PROPOSED SCHEME

This section presents a three-party secure data transmission authentication scheme for the IoT network. The scheme involves three parties that are user U_ι, SN_k, and GWN and six phases. GWN is designed to be a trustworthy and a link between U_ι and SN_k. GWN selects a point P on an elliptic curve with a large prime order n from a finite field Zp. Then,

TABLE III
GRAPHICAL REPRESENTATION OF REGISTRATION PHASE

User(U_ι)		Gateway Node(GWN)
Choose $ID_\iota, PW_\iota, BM_\iota$ and random number b.		
$Gen(BM_i) = (\omega_\iota, \theta_\iota)$		
$PW_{\iota 1} = h(PW_\iota \| \omega_\iota)$		
$ID_{i1} = h(ID_\iota \| \omega_\iota)$		
	$\xrightarrow{\{ID_\iota, ID_{i1}, PW_{\iota 1}\}}$	
		$A_\iota = h(ID_\iota \| ID_{gw} \| X_{GWN})$
		$B_\iota = ID_{i1} \oplus PW_{\iota 1} \oplus h(A_\iota)$
		$UID_\iota = h(ID_{i1} \oplus h(ID_{gw} \| X_{GWN})$
	$\xleftarrow{\{B_\iota, UID_\iota, h(.)\}}$	
$B'_\iota = B_\iota \oplus h(ID_{i1}) \oplus h(ID_\iota \| \omega_\iota \| b)$		
$L_\iota = h(ID_\iota \| PW_{\iota 1} \| B'_\iota \| \omega_\iota)$		
Replace B'_ι with B_ι		
Stores $\{B'_\iota, L_\iota, UID_\iota, \theta_\iota\}$ into SC		

it chooses a master key pk and computes $P_{pub} = pk.P$. Finally, stores pk and publish $\{P, P_{pub}\}$ as public.

A. Initialization Phase

In this phase, *GWN* preloaded the secret credentials into the sensor's memory in off-line mode. The following steps are executed for initialization.

S1: *GWN* picks a unique identity ID_{sj} for each sensor, where $(sj = 0, 1, 2, 3 \ldots n)$ and generate a master key k. Now, *GWN* computes $PID_{sj} = h(ID_{sj} \| k)$, $NID_k = ID_{sj} \oplus h(ID_{gw} \| k)$, where ID_{gw} is the identity of *GWN*. Also, shared a key SK_{gs} with the sensor.

S2: The *GWN* now stores PID_{sj} and NID_k into the SN_k's memory. In addition, the sensor has some computation power which calculate the parameters [58], [59].

B. Registration Phase

The user registration is important who wants to gain access to a sensor. The description of this phase is as follows.

S1: User first picks his identity ID_ι, password PW_ι, and imprints the personal biometric BM_ι at the sensor of a particular terminal. Using fuzzy extractor *Gen* function U_ι computes $Gen(BM_\iota) = (\omega_\iota, \theta_\iota)$ and computed password $PW_{\iota 1} = h(PW_\iota \| \omega_\iota)$. U_ι further picks a random number b and computes ID_{i1} as $h(ID_\iota \| b)$. Afterwards, U_ι sends $\{ID_\iota, ID_{i1}, PW_{\iota 1}\}$ to the *GWN* through secure channel.

S2: Upon receiving the registration message from U_ι, the *GWN* computes $A_\iota = h(ID_\iota \| ID_{gw} \| X_{GWN})$, $B_\iota = ID_{i1} \oplus PW_{\iota 1} \oplus h(A_\iota)$, $UID_\iota = ID_\iota \oplus h(ID_{gw} \| X_{GWN})$, where ID_{gw}, X_{GWN} are the identity and master key of the *GWN*. The *GWN* records the $\{ID_{i1}, A_\iota\}$ in its database for future use and sends the *SC* to the U_ι with the information $\{B_\iota, UID_\iota, h(\cdot)\}$ into the *SC*.

S3: After receiving the *SC* from the gateway node, U_ι calculates $B'_\iota = B_\iota \oplus h(ID_{i1} \oplus h(ID_\iota \| \omega_\iota \| b))$, $L_\iota = h(ID_\iota \| PW_{\iota 1} \| B'_\iota \| \omega_\iota)$. Finally, U_ι stores $\{B'_\iota, L_\iota, \theta_\iota, UID_\iota, h(\cdot)\}$. The registration phase of the proposed scheme is summarized in Table III.

C. Login and Authentication Phase

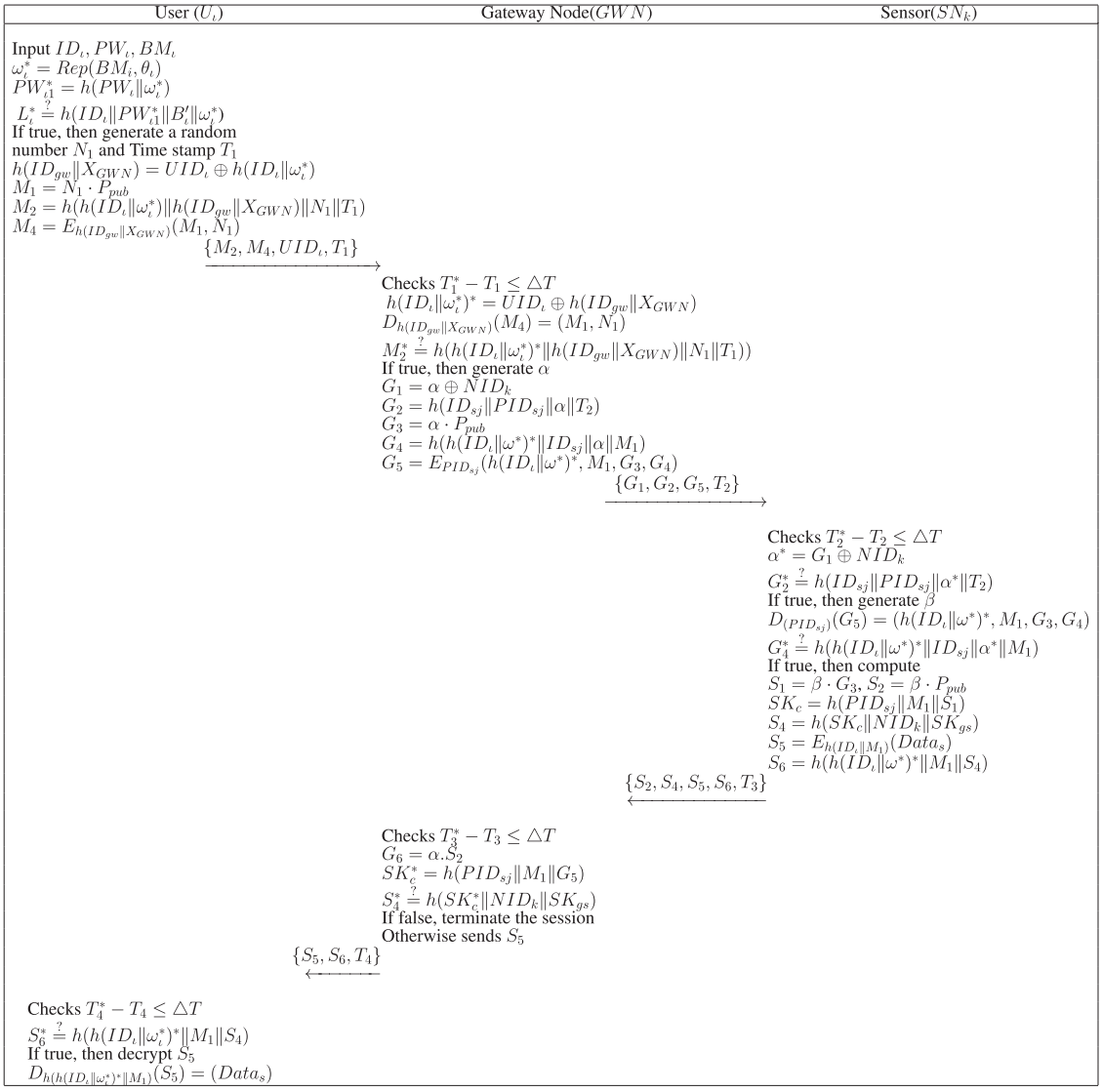
In this phase, a user enter his login details, which is authenticated by servers. U_ι performs the following steps to execute the phase.

S1: U_ι inserts the provided SC into card reader and inputs his ID_ι, PW_ι, and imprints his biometric BM_ι at the sensor of the terminal. *SC* recovers biometric key $\omega^*_\iota = Rep(BM_i, \theta_\iota)$ and computes $PW^*_{\iota 1} = h(PW_\iota \| \omega^*_\iota)$, $L^*_\iota \stackrel{?}{=} h(ID_\iota \| PW^*_{\iota 1} \| B'_\iota \| \omega_\iota)$. Then, the *SC* selects a random number N_1 and computes $h(ID_{gw} \| X_{GWN}) = UID_\iota \oplus h(ID_\iota \| \omega^*_\iota)$, $M_1 = N_1 \cdot P_{pub}$, $M_2 = h(h(ID_\iota \| \omega^*_\iota) \| h(ID_{gw} \| X_{GWN}) \| N_1 \| T_1)$, $M_4 = E_{h(ID_{gw} \| X_{GWN})}(M_1, N_1)$ if the condition is satisfied. Now, U_ι sends the login message $\{M_2, M_4, UID_\iota, T_1\}$ to *GWN* through public channel, where T_1 is the current time stamp.

S2: When *GWN* received the login message, first checks the timeliness of the received time stamp with the condition $T^*_1 - T_1 \leq \triangle T$, where T^*_1 is the received time stamp and $\triangle T$ is the maximum transmission delay. If the condition is true, *GWN* computes $h(ID_\iota \| \omega^*_\iota) = UID_\iota \oplus h(ID_{gw} \| X_{GWN})$, $D_{h(ID_{gw} \| X_{GWN})}(M_4) = (M_1, N_1)$, and verifies $M^*_2 \stackrel{?}{=} h(h(ID_\iota \| \omega^*_\iota) \| h(ID_{gw} \| X_{GWN}) \| N_1 \| T_1)$. If the condition fails, *GWN* rejects the session. Otherwise, generate a random number α and computes $G_1 = \alpha \oplus NID_k$, $G_2 = h(ID_{sj} \| PID_{sj} \| \alpha \| T_2)$, $G_3 = \alpha \cdot P_{pub}$, $G_4 = h(h(ID_\iota \| \omega^*)^* \| ID_{sj} \| \alpha \| M_1)$, and $G_5 = E_{(PID_{sj})}(h(ID_\iota \| \omega^*_\iota), M_1, G_3)$. Now, *GWN* sends the message $\{G_1, G_2, G_4, T_2\}$ to the SN_k through public channel.

S3: Upon receiving the message at time T^*_2, SN_k checks the validity of T_2 with condition $T^*_2 - T_2 \leq \triangle T$. If the condition fails, the session is rejected. Otherwise, SN_k computes $\alpha^* = G_1 \oplus NID_k$ and verifies $G^*_2 \stackrel{?}{=} h(ID_{sj} \| PID_{sj} \| \alpha^* \| T_2)$. If it is satisfactory, SN_k computes $D_{(PID_{sj})}(G_5) = (ID_\iota, M_1, G_3)$, $S_1 = \beta \cdot G_3$, $S_2 = \beta \cdot P_{pub}$, $SK_c = h(PID_{sj} \| M_1 \| S_1)$, $S_4 = h(SK_c \| NID_k \| SK_{gs})$, $S_5 = E_{h(ID_\iota \| M_1)}(Data_s)$, $S_6 = h(ID_\iota \| M_1 \| S_4)$ where β is the random number and sends $\{S_2, S_4, S_5, S_6, T_3\}$ to the U_ι through the public channel.

TABLE IV
GRAPHICAL REPRESENTATION OF LOGIN AND AUTHENTICATION PHASE



S4: Upon obtaining the message on time T_3^*, *GWN* checks whether $T_3^* - T_3 \leq \triangle T$ holds. If true, then U_ι verifies $S_4^* \stackrel{?}{=} h(SK_c^* \| NID_k \| SK_{gs})$ where $SK_c^* = h(PID_{sj} \| M_1 \| G_6)$, $G_6 = \alpha \cdot S_2$. If the conditions fails, *GWN* terminate the session. Otherwise, send $\{S_4, S_5, S_6, T_4\}$ to the U_ι.

S5: On receiving the message, U_ι checks $T_4^* - T_4 \leq \triangle T$. If it is fail, the session is aborted, otherwise it authenticates the sensor by computing $S_6^* \stackrel{?}{=} h(h(ID_\iota \| \omega_\iota^*)^* \| M_1 \| S_4)$. If it satisfies, then U_ι decrypt the data as $D_{h(h(ID_\iota \| \omega_\iota^*)^* \| M_1)}(S_5) = (Data_s)$. Table IV summarized the graphical representation of the login and authentication phase of our scheme.

D. Password Change Phase

This phase is needed to change the old password with a new password of a valid user. The details are illustrated below.

S1: The U_ι first insert his *SC* and enters his ID_ι, PW_ι and BM_ι. *SC* computes $\omega_\iota^* = Rep(BM_i, \theta_\iota)$, $PW_{\iota 1}^* = h(PW_\iota \| \omega_\iota^*)$ and verifies $L_\iota^* \stackrel{?}{=} h(ID_\iota \| PW_{\iota 1}^* \| B_\iota' \| \omega_\iota^*)$. If the condition fails, it abort the session. Otherwise, asks for the new password PW_{new} to enter.

S2: Upon getting the new password, *SC* computes $PW_{\iota 1}^{new} = h(PW_\iota^{new} \| \omega_\iota)$, $L_\iota^{new} = h(ID_\iota \| PW_{\iota 1}^{new} \| B_\iota' \| \omega_\iota)$ and replace L_ι with L_ι^{new} into the SC's memory. The *SC* can change the password without involvement of *GWN*.

E. Sensor Node Addition Phase

To deploy a new sensor node SN_k^{new} in the existing network, *GWN* completes the following steps.

S1: The *GWN* chooses a unique identity ID_{sj}^{new} for the new sensor and computes $PID_{sj}^{new} = h(ID_{sj}^{new} \| k)$, $NID_k^{new} = ID_{sj}^{new} \oplus h(ID_{gw} \| k)$, where ID_{gw} is the identity and k is the master key of *GWN*.

S2: The *GWN* now stores PID_{sj}^{new} and NID_k^{new} into the SN_k^{new}'s memory.

F. Smart Card Revocation Phase

This phase is important to revoke the SC if it is lost or stolen. The phase is depicted in detail below.

S1: When the *SC* is lost or stolen, U_ι creates a registration message with same user identity ID_ι and a new random number b^{nw}. Then, sends $\{ID_\iota, (ID_{i1}^{nw}), PW_{\iota 1}\}$ to the *GWN* for a new *SC*.

S2: Upon receiving the message, *GWN* search for the ID_ι. If it is exit, then computes $A_\iota^{nw} = h(ID_\iota \| ID_{gw} \| X_{GWN})$, $B_\iota^{nw} = ID_{i1}^{nw} \oplus PW_{\iota 1} \oplus h(A_\iota)$, $UID_\iota^{nw} = ID_{i1}^{nw} \oplus h(ID_{gw} \| X_{GWN})$ and embedded $\{B_\iota^{nw}, UID_\iota^{nw}, h(.)\}$ into the *SC*. Now, issues the SC to the valid user.

S3: After receiving the *SC*, U_ι computes $B_\iota^{nw'} = B_\iota^{nw} \oplus h(ID_\iota \| b^{nw}) \oplus h(ID_\iota \| \omega_\iota)$, $L_\iota^{nw} = h(ID_\iota \| PW_{\iota 1} \| B_\iota^{nw'} \| \omega_\iota)$ and replace B_ι^{nw} with $B_\iota^{nw'}$ and delete B_ι^{nw}. Now, SC contains $\{B_\iota^{nw'}, L_\iota^{nw}, \omega_\iota\}$ in its memory.

V. Security Analysis of the Proposed Scheme

This section includes formal and informal security analysis, demonstrating that the proposed scheme can withstand several well-known attacks.

A. Formal Security Analysis Using RoR Model

We apply a widely accepted RoR standard model, which is used to prove the session key security of the scheme [60]. For the formal proof, there are three participants that are user U_ι, gateway node *GWN*, and sensor SN_k involved in the proposed scheme TDTAS. The definitions are described as follows.

Participants: We denote three instances $\vartheta_{u_\iota}^s$, ϑ_{gwn}^u, and $\vartheta_{sn_k}^v$ of participants U_ι, *GWN*, and SN_k, respectively. ϑ^t is the union of all participants and any participant instance t of ϑ^t is an oracle. Each oracle has three states: accept, reject, and $\perp$. If the oracle receives the correct message, then it reaches an accept state. When the oracle receives an erroneous message, it enters the reject state. If no decision or result is obtained, the oracle enters the *perp* state.

Partnering: Any two instances, ϑ^{t1} and ϑ^{t2} are partnered if both the instances mutually authenticated to each other, share the same session key sk_u or sk_s, and both are in accepted states. Each participant may run the protocol several times and may obtain a session key.

Adversary($\mathcal{A}_v$)*:* An adversary used the DY model, which helps him to eavesdrop, modify, insert, or delete the transmitted message during the communication [55]. $\mathcal{A}_v$ can perform many oracles queries defined in the following.

1) *Execute*(ϑ^s, ϑ^v)*:* This query model the passive attacks and eavesdrops any messages transmitted between U_ι, *GWN*, and SN_k. The query returns the copy of the transmitted message as output.
2) *Send*(ϑ^t, m)*:* This query model the active attack, such as replay attacks, modification attack, and impersonation attacks. $\mathcal{A}_v$ may intercept, modify, or tamper the message and send it to the ϑ^t. To response the message, ϑ^t computes and replies the honest message to $\mathcal{A}_v$.
3) *Corrupt(SC):* This query models SC lost attack. $\mathcal{A}_v$ may extract all the information stored on the SC after executing this query. With the help of message eavesdropping and SC information, $\mathcal{A}_v$ may try to do off-line password guessing attack.
4) *Test*(ϑ^t)*:* This query simulates the session key by flipping an unbiased coin b. If $b = 1$, correct session key is returned and if $b = 0$, random binary string is returned. If ($\vartheta_{u_\iota}^s$/ $\vartheta_{sn_k}^v$) has not generated their session key, then $\perp$ is returned.

Semantic Security: $\mathcal{A}_v$ may interact with the instances by determining the value of a bit b. If $\mathcal{A}_v$ guesses the queries correctly, then the scheme fails to provide semantic security. Otherwise, he wins the game. Let $\mathcal{S}$ denotes the event in which $\mathcal{A}_v$ wins. In breaking the semantic security of the scheme, $\mathcal{A}_v$ has an advantage $Adv_p^{TDTAS} = |2.P[\mathcal{S}] - 1|$.

Theorem 1: Let E_p, D_1, D_2, and D_3 be an elliptic curve group and uniformly distributed dictionaries of ID_ι, PW_ι, and BM_ι, respectively. $|D_1|, |D_2|$, and $|D_3|$ denote the size of the D_1, D_2, and D_3, respectively. Thus, we obtain

$$Adv_p^{TDTAS} \leq \frac{(q_s + q_e)^2}{(q-1)} + \frac{(q_h)^2 + (q_s + q_e)^2}{2^l} + \max\left\{2.q_s\left(\frac{1}{|D_2|}, \frac{1}{|D_3|}\right)\right\} + 2Adv_{v,\mathcal{A}}^{IND-CPA}(k)$$

where q_h, q_s, and q_e represent the *hash*, *Send*, and *Execute* queries, respectively. 2^l is the string length of the hash results and $t' = t + (3q_e + q_s)T_e$ where T_e represents the time required to compute one modular exponentiation.

Proof: There are four games.

Game 0: This game corresponds to the real attacks in the oracle model. According to the definition, we have

$$Adv_p^{TDTAS} = 2P[\mathcal{S}_0] - 1. \quad (1)$$

Game 1: In this game, all the oracles are used. An adversary $\mathcal{A}_v$ launches a passive attack by *Send*(ϑ^t, m) and *Execute*(ϑ^s, ϑ^v) oracle. $\mathcal{A}_v$ has to decide the value of b in *Test*(ϑ^t) oracle. The session key is computed by using $N_1, \beta, ID_\iota, PW_\iota, X_{GWN}$. Adversary tries to extract these values from $\{msg1, msg2, msg3\}$. $\mathcal{A}_v$ cannot compute session key without corrupting SC and *GWN*'s database. The user identity, biometric, and *GWN*'s master key remain unknown to the adversary. So, the eavesdropping attack does not provide any advantage compared to Game 0. Thus, we have

$$P[\mathcal{S}_0] = P[\mathcal{S}_1]. \quad (2)$$

Game 2: In this game, we simulate the active attack by adding *Send* queries to Game 1. According to birthday paradox there are three types of collision.

1) The upper bound probability of collisions for random numbers N_1, N_1^{new} is $([(q_s + q_e)^2]/[2^{l+1}])$.
2) The upper bound probability of random numbers N_1 and β is $([(q_s + q_e)^2]/[2(q-1)])$.
3) The upper bound probability of collision of hash oracles is $([(q_h)^2]/[2^{l+1}])$. Game G_2 and Game G_1 are hard to differentiate unless the previous collisions occur.

So, we have

$$|P[\mathcal{S}_2] - P[\mathcal{S}_1]| \leq \frac{(q_s + q_e)^2}{2(q-1)} + \frac{(q_h)^2}{2^{l+1}} + \frac{(q_s + q_e)^2}{2^{l+1}}. \quad (3)$$

Game 3: In this game, the simulation of *Corrupt*(*SC*) query has been added. $\mathcal{A}_v$ receives SC information by querying *Corrupt*(*SC*). Then, A_k attempts for dictionary attack with possible password and biometric information in D_2 and D_3. Now, $\mathcal{A}_v$ fakes the login message and sends the corresponding query to the server. The password guessing probability for $\mathcal{A}_v$ is $(q_s/|D_2|)$, while biometric template is $(q_s/|D_3|)$. Then, we have

$$|P[\mathcal{S}_3] - P[\mathcal{S}_2]| \leq \max\left\{q_s\left(\frac{1}{|D_2|}, \frac{1}{|D_3|}\right)\right\}. \tag{4}$$

Game 4: Game 3 is transformed into Game 4 by adding *Corrupt*(*SC*) query. Suppose, $\mathcal{A}v$ can eavesdropped all the login and authentication messages $\{M_2, M_4, UID_i, T_1\}$, $\{G_1, G_2, G_4, T_2\}$, $\{S_4, S_5, T_3\}$, and $\{S_5, T_4\}$ of the proposed scheme. Besides, $\mathcal{A}v$ can obtain the SC information $\{B'_\iota, L_\iota, UID_\iota, \theta_\iota\}$. Now, $\mathcal{A}v$ tries to runs encryption algorithm on the input $\{M_4\}$. Using (Definition 2) indistinguishability of encryption under chosen plaintext (IND-CPA) secure symmetric cipher used in the proposed scheme, $\mathcal{A}v$ will choose the random bit b' for cipher text of input $\{M_4\}$. If both the ciphertext will same, then $\mathcal{A}v$ will win the game. Thus, we have

$$|P[\mathcal{S}_4] - P[\mathcal{S}_3]| \leq Adv_{v,\mathcal{A}}^{IND-CPA}(k). \tag{5}$$

Considering all above the games, $\mathcal{A}_v$ is only left to guess the bit b to win the game. Thus, we have

$$P[\mathcal{S}_4] = \frac{1}{2}. \tag{6}$$

From (1) and (2), we obtain

$$Adv_p^{TDTAS} = 2P[\mathcal{S}_1] - 1. \tag{7}$$

By dividing 2 in both side, we get

$$\frac{1}{2}Adv_p^{TDTAS} = P[\mathcal{S}_1] - \frac{1}{2}.$$

Putting the value of $(1/2)$, we have

$$\frac{1}{2}Adv_p^{TDTAS} = P[\mathcal{S}_1] - P[\mathcal{S}_4]. \tag{8}$$

Using (3), (4), and triangle inequality we can get the following equation:

$$\begin{aligned}
|P[\mathcal{S}_1] - P[\mathcal{S}_2]| + |P[\mathcal{S}_2] - P[\mathcal{S}_3]| &\leq \frac{(q_s+q_e)^2}{2(q-1)} \\
&+ \frac{(q_h)^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2^{l+1}} + \max\left\{q_s\left(\frac{1}{|D_2|}, \frac{1}{|D_3|}\right)\right\} \\
|P[\mathcal{S}_3] - P[\mathcal{S}_1]| &\leq \frac{(q_s+q_e)^2}{2(q-1)} + \frac{(q_h)^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2^{l+1}} \\
&+ \max\left\{q_s\left(\frac{1}{|D_2|}, \frac{1}{|D_3|}\right)\right\}.
\end{aligned} \tag{9}$$

From (5) and (9)

$$\begin{aligned}
|P[\mathcal{S}_1] - P[\mathcal{S}_4]| \leq \frac{(q_s+q_e)^2}{2(q-1)} &+ \frac{(q_h)^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2^{l+1}} + \\
&+ \max\left\{q_s\left(\frac{1}{|D_2|}, \frac{1}{|D_3|}\right)\right\} \\
&+ Adv_{v,\mathcal{A}}^{IND-CPA}(k)
\end{aligned}$$

$$\begin{aligned}
\frac{1}{2}Adv_p^{TDTAS} \leq \frac{(q_s+q_e)^2}{2(q-1)} &+ \frac{(q_h)^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2^{l+1}} \\
&+ \max\left\{q_s\left(\frac{1}{|D_2|}, \frac{1}{|D_3|}\right)\right\} \\
&+ Adv_{v,\mathcal{A}}^{IND-CPA}(k).
\end{aligned}$$

Multiplying 2 both side

$$\begin{aligned}
Adv_p^{TDTAS} \leq \frac{(q_s+q_e)^2}{(q-1)} &+ \frac{(q_h)^2 + (q_s+q_e)^2}{2^l} \\
&+ \max\left\{2.q_s\left(\frac{1}{|D_2|}, \frac{1}{|D_3|}\right)\right\} + 2Adv_{v,\mathcal{A}}^{IND-CPA}(k).
\end{aligned}$$

■

B. Informal Security Analysis

The informal security analysis of TDTAS is discussed as follows.

1) User Anonymity: A valid user never sent ID_ι in plain text to *GWN* or SN_k during the login and authentication phase. If an adversary eavesdrops the message, then also he is unable to extract as ID_ι is either encrypted or protected by one way hash function. Thus, the TDTAS achieves user anonymity.

2) Sensor Node Anonymity: In the TDTAS, the identity of the sensor node ID_{sj} does not reveal during communication. Thus, an adversary could not get ID_{sj} directly from the transmitted message. Furthermore, *GWN* encrypted the G_3 with PID_{sj}, where $PID_{sj} = h(ID_{sj}\|k)$ protected with one way hash function and k is the master key of the *GWN*. Thus, the TDTAS achieves sensor node anonymity.

3) Stolen Smart Card Attack: Let an adversary retrieve the sensitive information $\{B'_\iota, L_\iota, UID_\iota, \theta_\iota, h(.)\}$ from the *SC* using power analysis attack and tries to get ID_ι and PW_ι from the $\{B'_\iota, L_\iota\}$. However, it is computationally hard for an $\mathcal{A}_v$ as $L_\iota = h(ID_\iota\|PW_{\iota 1}\|B'_\iota\|\omega_\iota)$ and $B'_\iota = B_\iota \oplus h(ID_\iota\|b) \oplus h(ID_\iota\|\omega_\iota)$, where ID_ι and PW_ι are protected with one way hash function. Thus, the TDTAS is resilient against stolen SC attack.

4) Replay Attack: Assume that an adversary captures all login and authentication messages transmitted through an open channel and tries to replay the same message after some time. However, it is difficult to send the same message as *GWN*, SN_k, and U_ι checks the validity of the time stamp. Further, the assumption is A_v generates a new timestamp, however, he can be found by checking the correctness of $M_2^* \stackrel{?}{=} h(ID_\iota^*\|h(ID_{gw}\|X_{GWN})\|N_1\|T_1)$ and $G_2^* \stackrel{?}{=} h(ID_{sj}\|PID_{sj}\|\alpha^*\|T_2)$. The proposed scheme hence resist replay attack.

5) Insider Attack: In an insider attack, a privileged insider such as a system administrator may get the user's information and tries to log in to the accounts of a valid user. However, in TDTAS, the valid user transmits the password as $PW_{\iota 1} = h(PW_\iota\|\omega_\iota)$ instead of an original password. The generated password is also secured with a one-way hash function that is computationally hard to recover. Thus, neither an insider nor the registration center knows about the original password.

6) Man-in-the-Middle Attack: Let, the login message $\{M_2, M_4, UID_\iota, T_1\}$ is obtained by an adversary. However,

A_v could not change the login message, as *GWN* verifies the U_ι as $M_2^* \stackrel{?}{=} h(ID_\iota^* \| h(ID_{gw} \| X_{GWN}) \| N_1 \| T_1)$, where $ID_\iota, h(ID_{gw} \| X_{GWN})$ are only known to valid user and gateway node. Similarly, ID_{sj} and PID_{sj} only known to sensor node and gateway node. SN_k could find any modified message from *GWN* to *Sj*. Thus, the TDTAS is secured from man-in-the-middle (MIM) attacks.

7) Known Session-Specific Temporary Information Attack: The session key is computed as $SK_c = h(PID_{sj} \| M_1 \| S_1)$, where $S_1 = \beta \cdot G_3$, $G_3 = \alpha \cdot P_{pub}$. Let, the random number α and β two numbers are revealed. However, it is impossible to compute the session key as he need PID_{sj} and M_1 where $M_1 = N_1.P_{pub}$. To compute session key, $\mathcal{A}_v$ has to obtain PID_{sj}, N_1 simultaneously, which is an infeasible task. As a result, if two random numbers are compromised, no prior session key will be revealed.

8) User Impersonation Attack: In the TDTAS, to generate a valid login message $\{M_2, M_4, UID_\iota, T_1\}$, $\mathcal{A}_v$ needs to know $ID_\iota, ID_{gw}, N_1, X_{GWN}$ where N_1 and X_{GWN} are the random number and master key generated by the *GWN* and U_ι, respectively. To guess both ID_ι and PW_ι simultaneously is an infeasible work for him. Again, to compute $PW_{\iota 1}$ adversary needs user's biometric which is impossible for $\mathcal{A}_v$. Thus, user impersonation attack is not possible in our scheme.

9) Ephemeral Secret Leakage Attack: In an ephemeral secret leakage attack, if an adversary can reveal the private keys, then the session key would turn out to be known from the eavesdropped messages. In the proposed scheme let the private key is revealed, however session key cannot reveal as M1 and S1 and used for computation. As N1 and beta are used to compute the session key which are random in nature, for each session the session key will be different. Thus, the proposed scheme can resist ephemeral secret leakage attack.

10) Session Key Security: The session key security includes perfect forward secrecy and known key secrecy.

Perfect Forward Secrecy: Let the session key is compromised, and an adversary obtained the random number α and β, which are used to compute the session key. However, the compromise of one session key will not reveal any other previous session key as $\mathcal{A}_v$ needs $ID_\iota, PW_{\iota 1}, ID_{gw}, X_{GWN}$ to compute the session key. Thus, the TDTAS achieves perfect forward secrecy.

Known Key Secrecy: For known key secrecy, if the master key is revealed, then also the session key will not be computed. Although S_2 and *Pub* is obtained by an adversary, however, find β is computationally hard (Definition 3). Besides, due to two random numbers, the session key will be different in each session. Thus, the TDTAS provides known key secrecy.

11) Mutual Authentication: *GWN* is treated as trusted party which act as a bridge of communication between U_ι and SN_k. In login phase, *GWN* authenticate the U_ι by checking the condition $M_2^* \stackrel{?}{=} h(h(ID_\iota \| \omega^*)^* \| h(ID_{gw} \| X_{GWN}) \| N_1 \| T_1)$. If it is false, *GWN* reject the session. Similarly, *GWN* and SN_k authenticates to each other by verifying $G_2^* \stackrel{?}{=} h(ID_{sj} \| PID_{sj} \| \alpha^* \| T_2)$ and $S_4^* \stackrel{?}{=} h(SK_c^* \| NID_k \| SK_{gs})$, respectively. If any one of the condition is not satisfied, then the session is aborted. Thus, TDTAS provides mutual authentication.

12) Three-Factor Security: Three-factor security includes password, SC, and biometric information.

Case 1: The assumption is a $\mathcal{A}v$ has the *SC* information and password of a valid user. However, he is unable to obtain the user's identity using this information as biometric information is used.

Case 2: The assumption is A_v has SC information, biometric, and the login message $\{M_2, M_4, UID_\iota, T_1\}$. Also, he could retrieve $\omega_\iota^* = Rep(BM_i, \theta_\iota)$ using biometric and *Rep* function. Now, he could derive ID_ι and PW_ι by verifying $L_\iota^* \stackrel{?}{=} h(ID_\iota \| PW_{\iota 1}^* \| B_\iota' \| \omega_\iota)$. To guess both ID_ι and PW_ι in polynomial time is an infeasible work for him.

Case 3: Assume that an adversary has a password and biometric and attempt to derive ID_ι. However, he could not derive without knowledge of B_ι'. Again, it is an infeasible work, as ID_ι is protected with a hash function. Thus, TDTAS provides three-factor security.

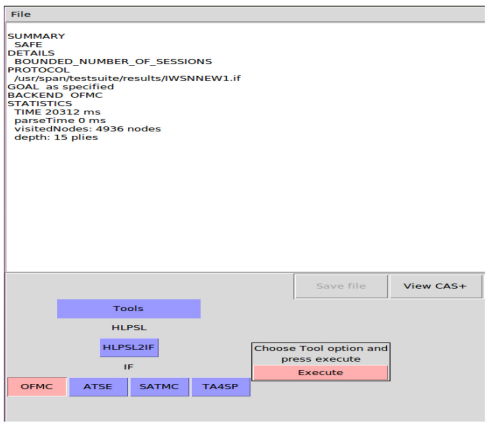
13) Efficient Login Phase: In an authentication scheme, an efficient login phase is achieved when the SC can identify incorrect input, thereby no need to contact the server for identifying the incorrect input. In the TDTAS, for the efficient login *SC* verifies the condition $L_\iota^* \stackrel{?}{=} h(ID_\iota \| PW_{\iota 1}^* \| B_\iota' \| \omega_\iota^*)$, where $PW_{\iota 1}^* = h(PW_\iota \| \omega_\iota^*)$, $\omega_\iota^* = Rep(BM_i, \theta_\iota)$. Thus, an adversary needs to know identity, password, and biometric simultaneously to satisfies the condition, which is an infeasible work for him. Hence, the TDTAS achieves efficient login phase.

14) Efficient Password Change Phase: In the TDTAS, the user can change his biometrics and password without contacting *GWN*. Since the SC could verify correctness of identity, password, and biometrics and replaces $PW_{\iota 1}$, L_ι with $PW_{\iota 1}^{new}$, L_ι^{new} into the SC's memory without involvement of *GWN*. Hence, the TDTAS provides an efficient password and biometry change phase.

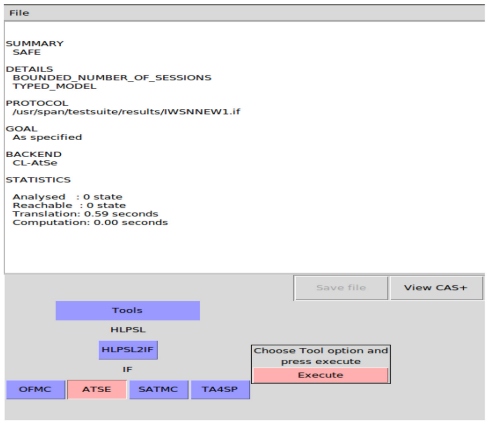
VI. Formal Security Verification Using AVISPA Tool

This section presents the simulation of the proposed scheme using the AVISPA tool [61], [62], [63]. It is a GUI-based tool for automated validation of the security protocols, which ensures the formal verification against several attacks. AVISPA tool needs the scheme to be specified in a role-oriented language called high-level protocol specification (HLPSL). It has two major roles, namely, basic role and composition role. The basic role demonstrates each participant involved in the scheme and composition role represent the scenario of participants. The protocol specification is given as input to the HLPSL2IF translator. HLPSL2IF translator takes HLPSL specification as input and produces intermediate form (IF) as output. IF is a lower-level specification than HLPSL. IF can be read directly by AVISPA backend tools. After the protocol has been properly accomplished, one of the four AVISPA backend tools generates output format (OF). Depending on the OF result is produced as SAFE or UNSAFE.

OFMC, CL-Atse, SATMC, and TA4sp are the four backends included. The suggested approach has been tested using two different backends: 1) OFMC and 2) CL-Atse, with the results



(a)



(b)

Fig. 2. Result using AVISPA tool. (a) Result using OFMC backend. (b) Result using ATSE backend.

reported in Fig. 2(a) and (b). The results confirm that TDTAS is secure under the DY model.

VII. Performance Comparison of the Proposed Scheme

This section presents the performance evaluation of our scheme with the other relevant scheme in terms of computation, communication, and storage cost as well as the security features of the scheme.

Fig. 3 provides a comparative analysis of the suggested scheme's computing cost with other relevant schemes. We denote T_{HS}, T_{EP}, and T_{EN} as the computational time required for a cryptographic one-way hash function, elliptic curve point multiplication, and symmetric encryption/decryption functions with values 0.0000464, 0.02314, and 0.00258 s, respectively. The computational cost of the proposed scheme of user is $5T_{HS} + 1T_{EP}$, the gateway node $6T_{HS} + 2T_{EP}$, and the sensor node $5T_{HS} + 2T_{EP}$, respectively. Thus, the total cost of TDTAS is $16T_{HS} + 5T_{EP} \approx 0.1157$ s. Similarly, Jiang et al. and Li et al. have the total computational cost are $23T_{HS} + 3T_{EP} \approx 0.07035$ s and $21T_{HS} + 3T_{EP} \approx 0.0701$ s, respectively. Where as the Sharif et al. needs $35T_{HS} \approx 0.0016$ s. Again Yu and Li [64] and Wang et al. [65] have more computational cost compared to proposed scheme. Though TDTAS needs a little more time, it is justified that the proposed scheme provides more functionality

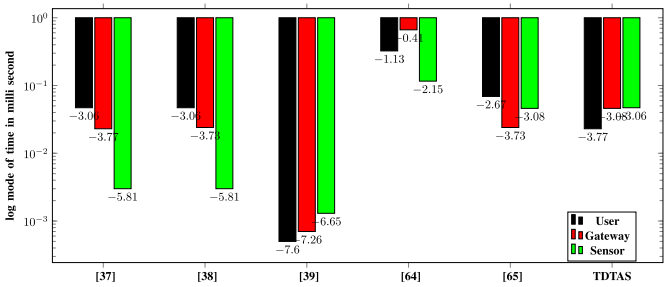


Fig. 3. Comparison of computational cost.

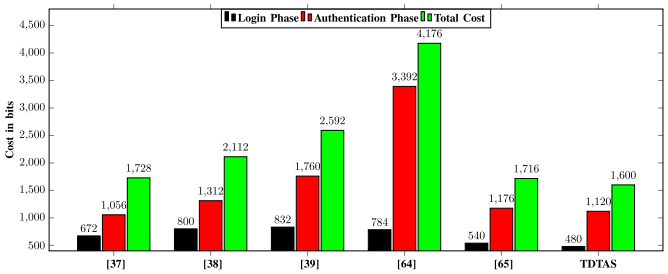


Fig. 4. Comparison of communication cost.

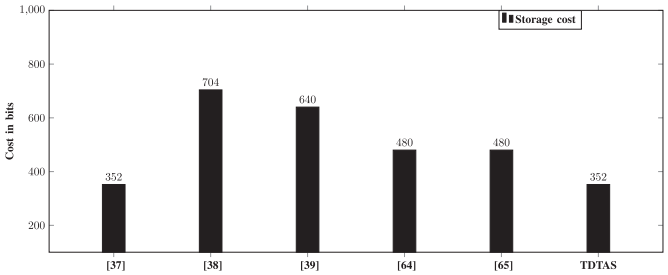


Fig. 5. Comparison of storage cost.

features, better security, less communicational, and storage cost as compared to other related schemes.

The efficiency of the TDTAS is also analyzed in terms of the communication costs associated with sending messages throughout the login and authentication phases. We consider the length of the identity/password/nonce/time stamp is 32 bits, encryption/decryption is 128 bits and hash function/ECC is 160 bits. In the proposed scheme, four message are exchanged among U_i, GWN_i, and SN_k. The login message require $Msg1 = \{M_2, M_4, UID_\iota, T_1\}$ $(160 + 128 + 160 + 32) = 480$ bits, $Msg2 = \{G_1, G_2, G_5, T_2\} = (160 + 160 + 128 + 32) + 480$ bits, $Msg3 = \{S_2, S_4, S_5, S_6, T_3\} = 160 + 160 + 128 + 160 + 32 = 640$ bits, and $Msg4 = \{S_4, S_5, S_6, T_4\} = 160 + 128 + 160 + 32 = 480$ bits, respectively. Thus, the total communicational cost is $480 + 480 + 640 + 480 = 2080$ bits. Similarly, the schemes of Jiang et al., Li et al., and Sharif et al. are 1728, 2112, and 2592 bits, respectively. The graphical comparison of the proposed scheme with other related schemes are presented in Fig. 4.

Fig. 5 shows the comparative study on storage costs for the proposed TDTAS and other existing schemes. The storage cost is calculated as $\{B'_\iota, L_\iota, UID_\iota, \theta_\iota\} = 352$ bits.

TABLE V
COMPARISON OF FUNCTIONALITY AND SECURITY FEATURES

Security Properties → Scheme↓	Σ_1	Σ_2	Σ_3	Σ_4	Σ_5	Σ_6	Σ_7	Σ_8	Σ_9	Σ_{10}	Σ_{11}	Σ_{12}	Σ_{13}	Σ_{14}	Σ_{15}
Jiang *et al.* [37]	✓	×	✓	✓	✓	×	×	✓	✓	✓	×	×	×	✓	×
Li *et al.* [38]	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	×	×
Sharif *et al.* [39]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	×	×	×	×
Yu *et al.* [64]	✓	×	×	✓	✓	×	×	✓	×	✓	×	✓	×	✓	×
Wang *et al.* [65]	✓	×	✓	✓	✓	✓	×	✓	✓	✓	✓	×	✓	✓	×
Proposed scheme	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Σ_1-User anonymity, Σ_2-Sensor anonymity , Σ_3-Stolen smart card attack, Σ_4-Replay attack, Σ_5-Insider attack, Σ_6-Man-in-the middle attack, Σ_7-Known session specific temporary information attack, Σ_8-User impersonation attack, Σ_9-Session key security, Σ_{10}-Mutual authentication, Σ_{11}-Three factor security, Σ_{12}-Efficient login phase, Σ_{13}-Efficient password change phase, Σ_{14}-Inefficient computation of session key, Σ_{15}-Security proof using RoR model.
✓- Prevent Attack, ×- Attack not prevented

The functionality and security features of the proposed scheme are compared with other existing schemes in Table V. It is observed that Jiang et al. and Li et al.'s scheme are vulnerable to MIM attack and could not achieve three-factor security. Further, Jiang et al. and Sharif et al.'s scheme lacks the detection of unauthorized login and does not support the password change phase freely. Besides, the scheme in Li et al. and Sharif et al. are incapable of computing the session key. Thus, compared with other related schemes, the proposed scheme achieves more security features and resists several attacks. In addition, none of the schemes are proved under the RoR model.

VIII. CONCLUSION

This article represents the security weakness of Sharif et al.'s scheme. We pointed out that the scheme lacks the functions of password change, inefficient login, and could not achieve user anonymity. Besides, the scheme could not guarantee session key security, which is vulnerable to several passive and active attacks. We proposed a three-party-based authentication scheme for 5G-enabled IoT environments along with a fuzzy extractor. The security analysis results show TDTAS can resist most of the known attacks and security features. Unlike existing schemes, the formal security analysis of the proposed scheme has been proved under the RoR model. Moreover, the informal security analysis indicates that the scheme is secure and robust. The formal verification of our scheme has been done using a widely accepted AVISPA tool. In future work, we plan to simulate our scheme using the NS-2 tool to evaluate its efficiency. In addition, the computational cost associated with the proposed scheme may be reduced further. Moreover, research needs to enhance the capability of the proposed scheme for secure communication among IoT devices to achieve desired performance metrics, such as transmission delay, throughput, QoS, etc.

REFERENCES

[1] R. Zhang, S. Cui, and C. Zhao, "Design of a data acquisition and transmission system for smart factory based on NB-IoT," in *Proc. Int. Conf. Commun. Signal Process. Syst.*, 2018, pp. 875–880.

[2] Y. Shi, Y. Zhao, R. Xie, and G. Han, "Designing a structural health monitoring system for the large-scale crane with narrow band IoT," in *Proc. IEEE 23rd Int. Conf. Comput. Supported Cooper. Work Design (CSCWD)*, 2019, pp. 239–242.

[3] Y. Zhu, G. Jia, G. Han, Z. Zhou, and M. Guizani, "An NB-IoT-based smart trash can system for improved health in smart cities," in *Proc. IEEE 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, 2019, pp. 763–768.

[4] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015.

[5] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, "PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks," *IEEE Trans. Depend. Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar./Apr. 2021.

[6] P. Wang, C.-M. Chen, S. Kumari, M. Shojafar, R. Tafazolli, and Y.-N. Liu, "HDMA: Hybrid D2D message authentication scheme for 5G-enabled VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5071–5080, Aug. 2021.

[7] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[8] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, L. Leng, and N. Kumar, "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks," *Comput. Netw.*, vol. 101, pp. 42–62, Jun. 2016.

[9] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

[10] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based Industrial Internet of Things deployment," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4900–4913, Dec. 2018.

[11] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 964–975, Jan. 2018.

[12] C. Otto, A. Milenkovic, C. Sanders, and E. Jovanov, "System architecture of a wireless body area sensor network for ubiquitous health monitoring," *J. Mobile Multimedia*, vol. 1, no. 4, pp. 307–326, 2006.

[13] 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.

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

[15] C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 59, pp. 250–261, Apr. 2017.

[16] R. Ali, A. K. Pal, S. Kumari, M. Karuppiah, and M. Conti, "A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring," *Future Gener. Comput. Syst.*, vol. 84, pp. 200–215, Jul. 2018.

[17] M. Chen, T.-F. Lee, and J.-I. Pan, "An enhanced lightweight dynamic pseudonym identity based authentication and key agreement scheme using wireless sensor networks for agriculture monitoring," *Sensors*, vol. 19, no. 5, p. 1146, 2019.

[18] F. Wu, L. Xu, X. Li, S. Kumari, M. Karuppiah, and M. S. Obaidat, "A lightweight and provably secure key agreement system for a smart grid with elliptic curve cryptography," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2830–2838, Sep. 2019.

[19] J. Chen, C. Touati, and Q. Zhu, "A dynamic game approach to designing secure interdependent IoT-enabled infrastructure network," *IEEE Trans. Netw. Sci. Eng.*, vol. 8, no. 3, pp. 2601–2612, Jul./Sep. 2021.

[20] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[21] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 10, no. 4, pp. 361–371, 2010.

[22] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks,'" *Sensors*, vol. 10, no. 3, pp. 2450–2459, 2010.

[23] H.-L. Yeh, T.-H. Chen, P.-C. Liu, T.-H. Kim, and H.-W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[24] S. Challa et al., "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 69, pp. 534–554, Jul. 2018.
[25] 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.
[26] A. K. Sutrala, A. K. Das, N. Kumar, G. R. Alavalapati, A. V. Vasilakos, and J. J. P. C. Rodrigues, "On the design of secure user authenticated key management scheme for multigateway-based wireless sensor networks using ECC," *Int. J. Commun. Syst.*, vol. 31, no. 8, 2018, Art. no. e3514.
[27] W. Han, "Weakness of a secured authentication protocol for wireless sensor networks using elliptic curves cryptography," in *Proc. IACR Cryptol. ePrint Arch*, 2011, p. 293.
[28] W. Shi and P. Gong, "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 4, 2013, Art. no. 730831.
[29] Y. Choi, D. Lee, J. Kim, J. Jung, J. Nam, and D. Won, "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 14, no. 6, pp. 10081–10106, 2014.
[30] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 316–323, 2013.
[31] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 35, no. 5, pp. 1646–1656, 2012.
[32] M. Turkanovic and M. Holbl, "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks," *Elektronika ir Elektrotechnika*, vol. 19, no. 6, pp. 109–116, 2013.
[33] C.-T. Li, C.-Y. Weng, and C.-C. Lee, "An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks," *Sensors*, vol. 13, no. 8, pp. 9589–9603, 2013.
[34] M. Turkanović, B. Brumen, and M. Hölbl, "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.*, vol. 20, pp. 96–112, Sep. 2014.
[35] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.
[36] D. He, N. Kumar, and N. Chilamkurti, "A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks," *Inf. Sci.*, vol. 321, pp. 263–277, Nov. 2015.
[37] Q. Jiang, J. Ma, F. Wei, Y. Tian, J. Shen, and Y. Yang, "An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 76, pp. 37–48, Dec. 2016.
[38] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K.-K. R. Choo, "A three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things environments," *J. Netw. Comput. Appl.*, vol. 103, pp. 194–204, Feb. 2018.
[39] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Future Gener. Comput. Syst.*, vol. 100, pp. 882–892, Nov. 2019.
[40] C.-T. Chen, C.-C. Lee, and I.-C. Lin, "Efficient and secure three-party mutual authentication key agreement protocol for WSNs in IoT environments," *PLoS ONE*, vol. 15, no. 4, 2020, Art. no. e0232277.
[41] D. Kumar, H. K. Singh, and C. Ahlawat, "A secure three-factor authentication scheme for wireless sensor networks using ECC," *J. Discr. Math. Sci. Cryptography*, vol. 23, no. 4, pp. 879–900, 2020.
[42] R. Vinoth, L. J. Deborah, P. Vijayakumar, and N. Kumar, "Secure multifactor authenticated key agreement scheme for industrial IoT," *IEEE Internet Things J.*, vol. 8, no. 5, pp. 3801–3811, Mar. 2021.
[43] F. Wu, X. Li, L. Xu, P. Vijayakumar, and N. Kumar, "A novel three-factor authentication protocol for wireless sensor networks with IoT notion," *IEEE Syst. J.*, vol. 15, no. 1, pp. 1120–1129, Mar. 2021.
[44] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.
[45] S. Shin and T. Kwon, "Two-factor authenticated key agreement supporting unlinkability in 5G-integrated wireless sensor networks," *IEEE Access*, vol. 6, pp. 11229–11241, 2018.
[46] K. Chatterjee, "An improved authentication protocol for wireless body sensor networks applied in healthcare applications," *Wireless Pers. Commun.*, vol. 111, no. 4, pp. 2605–2623, 2020.
[47] D. Kumar, S. Chand, and B. Kumar, "Cryptanalysis and improvement of an authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 2, pp. 641–660, 2019.
[48] M. Nikravan and A. Reza, "A multi-factor user authentication and key agreement protocol based on bilinear pairing for the Internet of Things," *Wireless Pers. Commun.*, vol. 111, no. 1, pp. 463–494, 2020.
[49] H. Mirvaziri and R. Hosseini, "A novel method for key establishment based on symmetric cryptography in hierarchical wireless sensor networks," *Wireless Pers. Commun.*, vol. 112, no. 4, pp. 2373–2391, 2020.
[50] Q. Xie, Z. Ding, and B. Hu, "A secure and privacy-preserving three-factor anonymous authentication scheme for wireless sensor networks in Internet of Things," *Security Commun. Netw.*, vol. 2021, Sep. 2021, Art. no. 4799223.
[51] B. Hu, W. Tang, and Q. Xie, "A two-factor security authentication scheme for wireless sensor networks in IoT environments," *Neurocomputing*, vol. 500, pp. 741–749, Aug. 2022.
[52] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, 1984.
[53] K.-K. R. Choo, "Key establishment: Proofs and refutations," Ph.D. dissertation, Dept. Comput. Sci., Queensland Univ. Technol., Brisbane, QUT, Australia, 2006.
[54] 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.*, 2004, pp. 523–540.
[55] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.
[56] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.
[57] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Adv. Cryptol. CRYPTO*, 1999, p. 789.
[58] J. Haapola, Z. Shelby, C. A. Pomalaza-Raez, and P. Mähönen, "Cross-layer energy analysis of multihop wireless sensor networks," in *Proc. EWSN*, vol. 5, 2005, pp. 33–44.
[59] A. Dementyev, S. Hodges, S. Taylor, and J. Smith, "Power consumption analysis of Bluetooth low energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario," in *Proc. IEEE Int. Wireless Symp. (IWS)*, 2013, pp. 1–4.
[60] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Public Key Cryptography*, 2005, pp. 65–84.
[61] A. Armando et al., "The AVISPA tool for the automated validation of Internet security protocols and applications," in *Proc. Int. Conf. Comput.-Aided Verification*, 2005, pp. 281–285.
[62] AVISPA. "AVISPA Automated Validation of Internet Security Protocols and Applications." 2015. [Online]. Available: http://www.avispa-project.org/
[63] S. S. Sahoo, S. Mohanty, and B. Majhi, "An improved and secure two-factor dynamic ID based authenticated key agreement scheme for multiserver environment," *Wireless Pers. Commun.*, vol. 101, no. 3, pp. 1307–1333, 2018.
[64] B. Yu and H. Li, "Anonymous authentication key agreement scheme with pairing-based cryptography for home-based multi-sensor Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 9, p. 19, 2019.
[65] X. Wang, Y. Teng, Y. Chi, and H. Hu, "A robust and anonymous three-factor authentication scheme based ECC for smart home environments," *Symmetry*, vol. 14, no. 11, p. 2394, 2022.

Shreeya Swagatika Sahoo (Member, IEEE) received the Ph.D. degree in computer science and engineering from the National Institute of Technology Rourkela, Rourkela, India, in 2021.

She is currently working as an Assistant Professor with the Department of Computer Science and Engineering, SoA University, Bhubaneswar, India. She has more than two years of teaching experience and four years of research experience. Her current research interests include cryptography, security protocol, and network security.

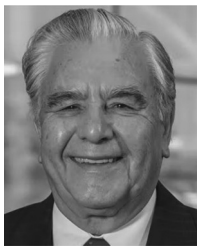
Sujata Mohanty received the Ph.D. degree in computer science and engineering from the National Institute of Technology (NIT) Rourkela, Rourkela, India, in 2013.

She is currently working as an Assistant Professor with the Department of Computer Science and Engineering, NIT Rourkela. Her research interests include information security, cryptography, and network security.

Kshira Sagar Sahoo (Senior Member, IEEE) received the master's degree in information and communication technology from the Indian Institute of Technology Kharagpur, Kharagpur, India, in 2014, and the Ph.D. degree in computer science and engineering from the National Institute of Technology Rourkela, Rourkela, India, in 2019.

He is a Kempe Fellow with the Autonomous Distributed Systems Laboratory, Department of Computing Science, Umeå University, Umeå, Sweden. He has more than five years teaching experience, two-year industry experience, and four years of research experience. He has published more than 90 research papers in various top international journals and conferences, including the IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, IEEE SYSTEMS JOURNAL, IEEE INTERNET OF THINGS JOURNAL, ACM TOMM, and Elsevier FGCS. His research interests include future-generation network infrastructure, such as SDN, edge computing, IoT, urban anomaly detection, and Industrial IoT.

Dr. Sahoo is a Senior Member of the IEEE Computer Society and an Associate Member of the Institute of Engineers India.



Mahmoud Daneshmand (Life Senior Member, IEEE) received the B.S. and first M.S. degrees in mathematics from the University of Tehran, Tehran, Iran, in 1964 and 1966, respectively, and the second M.S. and Ph.D. degrees in statistics from the University of California at Berkeley, Berkeley, CA, USA, in 1973 and 1976, respectively.

He is the Co-Founder and a Professor with the Department of Business Intelligence and Analytics as well as the Data Science Ph.D. Program, and a Professor with the Department of Computer Science, Stevens Institute of Technology, Hoboken, NJ, USA. He has more than 40 years of industry and university experience as the Executive Director of Bell Laboratories, Murray Hill, NJ, USA; the Assistant Chief Scientist with AT&T Shannon Labs-Research, Florham Park, NJ, USA; a Professor with the University of California at Berkeley; a Researcher with the University of Texas at Austin, Austin, TX, USA; a Distinguished Member of Technical Staff with New York University, New York, NY, USA; a Technology Leader with Sharif University of Technology, Tehran; the Founding Chair of Department with the University of Tehran; and the Dean of School with the Stevens Institute of Technology. He is a Data Scientist, expert in big data analytics, artificial intelligence, and machine learning with extensive industry experience, including with the Bell Laboratories as well as the Info Lab, AT&T Shannon Labs-Research. He has published more than 250 journal and conference papers; authored/coauthored three books, and has graduated more than 2500 Ph.D. and M.S. students. He holds key leadership roles in IEEE Journal Publications, IEEE Major Conferences, Industry–IEEE Partnership, and IEEE Future Direction Initiatives.

Dr. Daneshmand has served as the general chair, the keynote chair, the panel chair, the executive program chair, and the technical program chair of many IEEE major conferences. He has given many keynote speeches in major IEEE as well as international conferences.

Amir H. Gandomi (Senior Member, IEEE) received the Ph.D. degree in engineering from The University of Akron, Akron, OH, USA, in 2015.

He is a Professor of Data Science and an ARC DECRA Fellow with the Faculty of Engineering and Information Technology, University of Technology Sydney (UTS), Ultimo, NSW, Australia. He is also affiliated with Obuda University, Budapest, Hungary, as a Distinguished Professor. Prior to joining UTS, he was an Assistant Professor with the Stevens Institute of Technology, Hoboken, NJ, USA; and a Distinguished Research Fellow with BEACON Center, Michigan State University, East Lansing, MI, USA. He is active in delivering keynotes and invited talks. He has published over 350 journal papers and 14 books which collectively have been cited more than 40 000 times (H-index = 88). His research interests are global optimization and (big) data analytics using machine learning and evolutionary computations in particular.

Dr. Gandomi has received multiple prestigious awards for his research excellence and impact, such as the 2022 Walter L. Huber Prize and the Highest-Level Mid-Career Research Award in all areas of civil engineering. He has been named as one of the most influential scientific minds and received the Highly Cited Researcher award (top 1% publications and 0.1% researchers) from Web of Science for six consecutive years, from 2017 to 2022. In the recent most impactful researcher list, done by Stanford University and released by Elsevier, he is ranked as the top 1000 researchers (top 0.01%) and top 50 researchers in AI and Image Processing subfield in 2021! He also ranked 17th in GP bibliography among more than 15 000 researchers. He has served as an Associate Editor, an Editor, and the Guest Editor in several prestigious journals, such as AE of IEEE NETWORKS and IEEE INTERNET OF THINGS JOURNAL.