IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 9, 2019, accepted June 30, 2019, date of publication July 3, 2019, date of current version July 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2926578

Physically Secure Lightweight Anonymous User Authentication Protocol for Internet of Things Using Physically Unclonable Functions

SOUMYA BANERJEE[1], VANGA ODELU[2], ASHOK KUMAR DAS[3], (Senior Member, IEEE), SAMIRAN CHATTOPADHYAY[1], (Senior Member, IEEE), JOEL J. P. C. RODRIGUES[4,5,6], (Senior Member, IEEE), AND YOUNGHO PARK[7], (Member, IEEE)

[1]Department of Information Technology, Jadavpur University, Salt Lake 700 098, India
[2]Department of Computer Science and Information Systems, Birla Institute of Technology & Science, Pilani Hyderabad Campus, Hyderabad 500 078, India
[3]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
[4]National Institute of Telecommunications, Santa Rita do Sapucaí 37540-000, Brazil
[5]Instituto de Telecomunicações, 1049-001 Lisbon, Portugal
[6]Federal University of Piauí, Teresina 64049-550, Brazil
[7]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

Corresponding author: Youngho Park (parkyh@knu.ac.kr)

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Science, ICT & Future Planning under Grant 2017R1A2B1002147, in part by the BK21 Plus project funded by the Ministry of Education, South Korea, under Grant 21A20131600011, in part by the *Fundação para a Ciência e a Tecnologia* through the UID/EEA/50008/2019 Project, in part by RNP, with resources from MCTIC, under the *Centro de Referência em Radiocomunicações*–CRR Project of the *Instituto Nacional de Telecomunicações* (Inatel), Brazil, under Grant 01250.075413/2018-04, and in part by the Brazilian National Council for Research and Development (CNPq) via under Grant 309335/2017-5.

ABSTRACT The Internet of Things (IoT) acts as an umbrella for the Internet-enabled devices for various applications, such as smart home, smart city, smart grid, and smart healthcare. The emergence of the immense economic potential necessitates a robust authentication mechanism that needs to be lightweight and suitable for real-time applications. Moreover, the physical integrity of these devices cannot be assumed as these are designed to be deployed in an unattended environment with minimum human supervision. A user authentication mechanism for the IoT, in addition to guaranteeing user anonymity and un-traceability functionality requirements, must also be resistant to device physical capture and related misuses. In this paper, we present a novel lightweight anonymous user authentication protocol for the IoT environment by utilizing ''cryptographic one-way hash function'', ''physically unclonable function (PUF)'' and ''bitwise exclusive-OR (XOR)'' operations. The broadly accepted Real-Or-Random (ROR) model-based formal security analysis, formal security verification using the automated software verification tool, namely ''automated validation of internet security protocols and applications (AVISPA)'' and also non-mathematical (informal) security analysis have been carried out on the proposed scheme. It is shown that the proposed scheme has the ability to resist various well-known attacks that are crucial for securing the IoT environment. Through a detailed comparative study, we show that the proposed scheme outperforms other existing related schemes in terms of computation and communication costs, and also security & functionality features. Finally, a practical demonstration of the proposed scheme using the NS3 simulation has been provided for measuring various network performance parameters.

INDEX TERMS Internet of Things (IoT), mutual authentication, key agreement, physically unclonable function, security, AVISPA.

I. INTRODUCTION

We are living in the age of information, and a significant portion of the information is derived from the innumerable Internet connected smart devices and sensors that make up the Internet of Things (IoT). It is projected that by the year 2020, the number of IoT devices will approach fifty billion [1]. This exponential growth in popularity of IoT devices, partly driven by the cultural shift of preference of smart (Internet enabled)

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

consumer appliances, exposes a huge attack surface for the adversaries to exploit the information. Without adequate addressable of the concern regarding the security and privacy of the vast amount of sensitive data that is expected to flow through these IoT networks, popular consumer deployment of these technologies will be untenable [2]. The economic potential alone provides the impetus to develop robust authentication mechanism for IoT architecture. Fig. 1 describes a generalized IoT architecture.

The authors in [3] defined the objectives of IoT that bridges between the physical world and the computer-based systems unlocking great economic welfare, accuracy and efficiency with minimal human action. Through this definition IoT subsumes the wireless sensor networks (WSNs) domain. The authentication problem in IoT architecture is quite similar to the problems addressed for WSNs. Thus, the lessons learned for developing anonymous authentication schemes for WSNs carry over to the IoT architecture. However, one difference between a typical IoT device and a typical WSN sensor is that generally the IoT device is more complex and expensive. Consequently, it is quite conceivable that an IoT device can have replaceable subsystems. The current standard threat model (defined in Section I-B) ensures that the stolen credentials from one system cannot be utilized to compromise the security of unrelated devices. But, in light of reusable modular IoT devices, a new attack must also be considered, such as impersonation of compromised devices. An adversary can extract the credentials from a physically captured smart device and using these credentials the adversary can impersonate on behalf of the captured smart devices. As the users and gateway nodes will use the almost same credentials to verify the identity of the device, this impersonating device cannot be also detected. In this scenario, even if the rest of the network is not compromised, the user who connects to the spurious devices will expose him/herself to the adversary. To get around a similar problem of stolen user credentials, a widely accepted approach is to incorporate user biometric into the authentication scheme. Analogously, we need to employ some sort of device biometric. Physically Unclonable Functions (PUFs) support such a functionality. In this paper, we present a novel physically secure lightweight anonymous authentication protocol for IoT using PUFs.

A. NETWORK MODEL

In this paper, we follow a similar network model to that presented in [4] and [5]. The IoT architecture is composed of disjoint sub-networks consisting of multiple IoT smart devices operating as sensors or actuators, that are connected over the public Internet. The smart devices are accessed through their respective gateway node (*GWN*) over a heterogeneous network. The authorized users, prior to enjoying services of a smart device (*SD*), must register with the corresponding *GWN*. The registered mobile users (*MU*s) can mutually authenticate with a smart device *SD* through the *GWN* in order to negotiate a session key for accessing the device real-time data. A standard security requirement for authentication is that it must support anonymity and intractability for both *MU* and *SD* [3].

B. THREAT MODEL

The authors in [3] defined the security requirements and also a threat model related to IoT ecosystems. In our work, we adhere to the broadly accepted Dolev-Yao (DY) threat model [6]. Under DY-threat model, an adversary $\mathcal{A}$ will have complete control over the communication media. Thus, $\mathcal{A}$ can eavesdrop upon, alter, delete and even forge messages that are transmitted through the communication media. Additionally, it is assumed that through power analysis attacks [7], $\mathcal{A}$ can extract the sensitive data stored in a lost or stolen smart card. Furthermore, it is within $\mathcal{A}$'s capacity to physically capture some IoT smart devices as the IoT devices can be deployed in some unattended environment, such as in some IoT applications including healthcare and surveillance, and $\mathcal{A}$ can extract the credentials stored in those captured devices. We work under the assumption that the *GWN*s are be physically secured under locking systems and thus, the *GWN*s are considered to be trusted entities in the IoT environment [8].

This proposed scheme is also based on the CK-adversary model [9]. The CK-adversary model is a more stronger threat model and it is considered as the current *de facto* standard in modeling key-exchange protocols [10]. Under the CK-adversary model, the adversary $\mathcal{A}$, in addition to all capabilities of the adversary under the DY model, can compromise secure information like session state, private and session keys. Thus, the key-exchange protocols need to guarantee that in the event of ephemeral (short-term) secret leakage, the effect on the security of session keys established among the communicating entities in an authenticated key-exchange protocol should be minimal [11].

C. RESEARCH CONTRIBUTIONS

The main contributions of the paper are listed below.

- A novel lightweight anonymous user authentication protocol has been designed for IoT environment, which relies on the lightweight operations like ''Physically Unclonable Functions (PUFs)'', ''fuzzy extractor functions'', ''one-way hash functions'' and ''bitwise XOR operations''.
- In the proposed protocol, the physical security of the user's device (smart card) and IoT smart devices deployed in the hostile environment is assured.
- The proposed protocol offers various functionality features, such as ''password and biometric update'', ''pseudo-identity renewal'' and ''challenge-response renewal''. In addition, the proposed protocol also supports ''device enrollment'' through which the IoT smart devices can be deployed any time (during initial deployment or after initial deployment).
- A detailed security analysis using the formal security using the broadly-accepted ROR model [12], formal security verification using the popular software-based

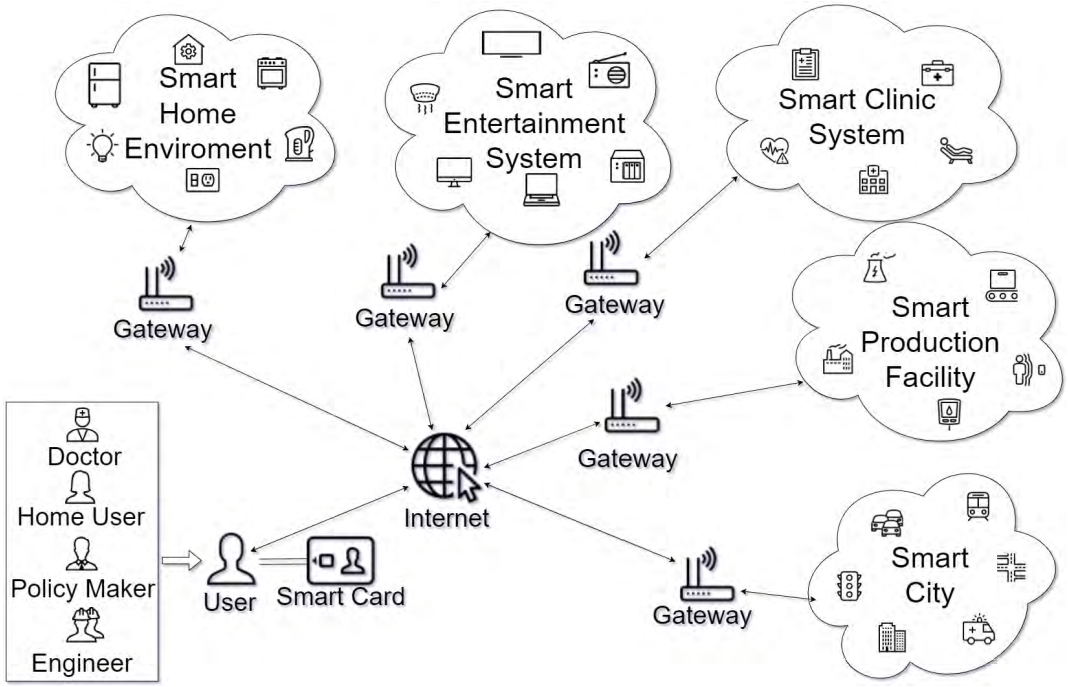

FIGURE 1. A generalized IoT architecture.

AVISPA tool [13] and informal security analysis has been carried out to show the proposed protocol provides high security.

- A rigorous comparative analysis shows that the proposed protocol achieves better security along with more functionality features, and provides comparable communication & computational overheads as compared to those for the related existing schemes.
- The NS3 simulation [14] has been carried out to measure several important network performance parameters on the proposed protocol.

D. PAPER ORGANIZATION

The organization of the paper is as follows. We present the theoretical background relevant to the work in Section II. A short review of the relevant authentication schemes from the existing literature in presented in Section III. The proposed scheme is presented in IV with the detailed description of all the phases. In Section V, we provide the rigorous security analysis of the proposed scheme through the formal security analysis and verification using ROR model and AVISPA verification) tool and also the informal analysis. We then present a comparative study showcasing the strength of the proposed scheme in Section VI with related existing schemes. A simulation study for the practical impact of the proposed scheme through NS3 simulation is presented in Section VII. Finally, we draw the conclusions in Section VIII.

II. THEORETICAL BACKGROUND

In this section, we provide a short description of the theoretical background that are essential in this paper.

A. ONE-WAY CRYPTOGRAPHIC HASH FUNCTION

One-way hash functions are extensively applied for data integrity. Cryptographic one-way hash functions are designed in such a way that they should be highly sensitive to even slight perturbations to the input. For example, even for two very similar inputs with little difference, the outputs are produced in such a way that they cannot be correlated to each other. Formally, a "collision-resistant one-way hash function" can be defined as follows [8].

Definition 1: Let h: $\{0,1\}^* \rightarrow \{0,1\}^n$ denote a one-way hash function. Upon receiving a variable length input, $h(\cdot)$ gives a fixed-size length output of n bits, called the message digest or hash output. If $Adv_{\mathcal{A}}^{Hash}(t)$ is defined as an adversary $\mathcal{A}$'s advantage in detecting hash collision in runtime t, $Adv_{\mathcal{A}}^{Hash}(t) = Pr[(x_1, x_2) \in_R \mathcal{A} : x_1 \neq x_2$ and $h(x_1) = h(x_2)]$, where $Pr[X]$ is the probability of a random event X, and x_1 & x_2 are strings that are randomly selected by $\mathcal{A}$. An (ϕ, t)-adversary $\mathcal{A}$ attacking a hash collision of $h(\cdot)$ means that with maximum execution time t, $Adv_{\mathcal{A}}^{Hash}(t) \leq \phi$.

B. PHYSICALLY UNCLONABLE FUNCTION

The Physically Unclonable Functions (PUFs) are designed to map an input uniquely to an output based on the physical micro structure of a device. An input-output pair together is known as a challenge-response pair and it is unique to each individual PUF circuit. A PUF circuit must exhibit the following properties [15]:

- The output of a PUF circuit must depend on the physical micro structure of the system.
- The output of a PUF must be unpredictable.

- The PUF circuit must be easy to evaluate as well as to implement.
- The PUF circuit must be unclonable.

As the output of PUF is dependent on the physical characteristics, any alteration to the system will change in the PUF output. It is further assumed that it is impossible to tamper the communication between PUF and its host device as in pointed out in [16].

Definition 2: A PUF, say PUF_1, is secure, if for two input challenges $C_1, C_2 \in \{0,1\}^k$ it produces output responses $R_1, R_2 \in \{0,1\}^k$ with at least d_1 variation, and for any two different PUFs (PUF_1, PUF_2) an input challenge C_1 should produce distinct output responses $R_1, R_2 \in \{0,1\}^k$ with at least d_2 variation. In other words,

$$Pr[HD(PUF_1(C_1), PUF_1(C_2)) > d_1] = 1 - \varepsilon,$$
$$Pr[HD(PUF_1(C_1), PUF_2(C_1)) > d_2] = 1 - \varepsilon,$$

where ε is a negligibly small value, C_1 and C_2 are challenges randomly selected by $\mathcal{A}$, HD defines the Hamming distance, and d_1 and d_2 are the error tolerance thresholds for PUF.

C. FUZZY EXTRACTOR

Even though now-a-days a PUF circuits can be developed with a high degree of reliability, noise in PUF remains an important issue. Zhang *et al.* [17] investigated dissipative filtering issue for ''a class of discrete-time switched fuzzy systems with missing measurements''. They formulated the occurrence of missing measurements by representing it as a random variable that follows the ''Bernoulli binary distribution''. They also pointed out that it characterizes the effect of data loss in information transmission among the fuzzy plant and the filter.

Gope *et al.* [18] recommended the fuzzy extractor method [19]. The fuzzy extractor is compromised of two methods, namely 1) probabilistic generation function $Gen(\cdot)$ and 2) deterministic re-production function $Rep(\cdot)$, that are defined below.

- *Gen:* For a challenge-response pair, say $PUF(C_i) = Res_i$, $Gen(\cdot)$ outputs a tuple comprising of a (secret) key R_i and helper data hd_i, that is, $Gen(Res_i) = (R_i, hd_i)$.
- *Rep:* Given a PUF output Res_i', $Rep(\cdot)$ can recover the original secret key R_i with the help of the helper data hd_i provided the the Hamming distance between the original PUF output Res_i and current PUF output Res_i' does not exceed a pre-defined error tolerance threshold value et. Thus, $Rep(Res_i', hd_i) = R_i$.

One of the estimations on error tolerance threshold values suggested by Cheon *et al.* [20] is provided as follows. If the Hamming distance between the original PUF output Res_i and current PUF output Res_i' is T and the number of bits in input string is in_b, then $et = \frac{T}{in_b}$.

III. LITERATURE SURVEY

Lamport [21] introduced a seminal on remote user authentication in 1981. Later, in the works by several other authors in [22]–[24] the concepts of mutual authentication, smart-card based authentication, user anonymity were introduced, which became the standard requirements for later authentication schemes. Wong *et al.* [25] proposed a hash-based lightweight user authentication scheme for the resource-constrained wireless sensor networks (WSNs). Das [26] presented an authentication scheme for the resource-constrained WSNs. However, the schemes [25], [26] were vulnerable to several attacks as identified and improved upon by the authors in [27]–[29].

Madhusudan and Mittal [30] identified that user anonymity is one of the ten desirable attributes for an ideal password authentication scheme. Turkanović *et al.* [31] discussed WSN as a component of IoT, and pointed out that user anonymity and un-traceability are the widely considered integral requirements for authentication schemes in WSN. Alqasen [32] concluded that owing to the diverse and heterogeneous nature of IoT, specific investigation into the security challenges for IoT architecture is also necessary.

Granjal *et al.* [33] identified ''privacy, anonymity, liability and trust'' as fundamental for the social acceptance of most of the future IoT applications. Mineraud *et al.* [34] analyzed malwares and highlighted inherent design flaws in the emerging IoT infrastructure and its associated security challenges. Makhdoom *et al.* [35], while discussing the threats to IoT, identified that user anonymity vis-a-vis id management as the key security and privacy challenges. Thus, user anonymity and un-traceability are necessary requirements for designing an authentication scheme for IoT environment.

Jeong *et al.* [36] proposed a ''One-Time Password (OTP)'' based approach for user authentication in smart home environment. Unfortunately, this scheme fails to assure mutual authentication, user anonymity and untracability. Hunumanathappa and Singh [37] also presented a pass-phrase based approach to ensure device attestation during user authentication for ubiquitous computing devices.

Santoso and Vun [38] proposed a user authentication scheme for smart homes using ''Elliptic Curve Cryptography (ECC)'' technique. However, this scheme fails in ensuring anonymity and untracability [8]. Porambage *et al.* [39] designed a scalable authentication protocol suitable for heterogeneous resource-constrained WSNs. Turkanović *et al.* [31] also presented a computationally efficient scheme for authentication in WSNs. Chang and Le [40] proposed two schemes for user authentication: 1) the first one is based on bitwise XOR and hash operations, and 2) the second scheme additionally uses ECC apart from bitwise XOR and hash operations to provide high security. Unfortunately, Das *et al.* [41] demonstrated that both the schemes were vulnerable to several known attacks, including man-in-the-middle, offline password guessing and replay attacks. Wazid *et al.* [5] also observed that the scheme [31] was vulnerable to known attacks like privileged insider, offline password guessing, user impersonation. They proposed a lightweight authenticated key management protocol for a generic IoT network.

Jie *et al.* [42] proposed an RFID based multi-layer architecture for smart homes. Song *et al.* [43] studied [42] and observed the certificate authority in smart devices were too computationally expensive for practical applications. As an alternative, they presented an authentication scheme based on hash functions and chaotic systems. Challa *et al.* [4] designed an authentication scheme intended for IoT deployment applying ECC signatures. Gope and Hwang [44] presented another lightweight scheme for user authentication in real-time WSN. However, their scheme does not support sensor node anonymity.

Shen *et al.* [45] investigated importance of reliability and applicability of using motion-sensor behavior in the domains of active and continuous smartphone authentication across different operational scenarios. They also presented a methodical assessment of ''distinctiveness'' and ''permanence'' properties of the behavior. Shen *et al.* [46] designed another authentication protocol using motion sensors (gyroscope and accelerometer) that are embedded in the smartphones. The main feature of their mechanism is that it accomplishes authentication process constantly and completely by monitoring the user daily tasks.

Amin *et al.* [47] presented a user authentication protocol for distributed cloud computing environment composed of IoT devices. However, Challa *et al.* [48] and Li *et al.* [49] demonstrated several security pitfalls in the scheme [47], such as privileged-insider and impersonation attacks. Apart from these, Amin *et al.*'s scheme [47] fails to guarantee some important requirements like user anonymity and forward secrecy properties.

Dhillon and Kalra [50] presented a multi-factor remote user authentication scheme for IoT environment. Chuang *et al.* [51] classified continuous authentication protocols for IoT into user-to-device model and device-to-device model, and presented a lightweight continuous authentication protocol for device-to-device authentication in IoT. Unfortunately, the schemes of Dhillon and Kalra [50] and Chuang *et al.* [51] fail to provide user and sensing device anonymity, respectively, and both the schemes also fail to satisfy untraceability property.

Zhou *et al.* [52] proposed an anonymous authentication scheme using only hash function and XOR operations. Unfortunately, their scheme is vulnerable to replay attack, and it also fails to preserve forward secrecy goal. Ferrag *et al.* [53] presented a detailed survey on various authentication schemes including user authentication for IoT. In addition to the individual vulnerabilities, all the discussed schemes fail to prevent impersonation of compromised smart devices (sensor nodes) using the extracted credentials.

Gope *et al.* [15] used physically unclonable function (PUF) to physically secure sensor nodes in industrial wireless sensor networks. Devadas *et al.* [16] proposed PUF-based RFID integrated circuits for anti-counterfeiting application. Since then PUFs have been widely used in securing RFID systems. Gope *et al.* [18] discussed the issue of noise in PUF output and its implication on authentication schemes. They utilized fuzzy extractor technique [19] to circumvent this issue. Additionally, their scheme has high communication overhead, and it is only secure under the DY threat model and cannot resist ephemeral secret leakage attack under the current CK-adversary model (discussed in the threat model in Section I-B).

TABLE 1. Important notations and their significance.

Symbol	Description
ID_u, SC_u	Identity and smart card of a user U, respectively
PW_u, BIO_u	Password & biometrics of U, respectively
ID_d, GWN	Identity of an IoT smart device SD and the gateway node, respectively
LTS	Long term secret of the GWN
$Gen(\cdot), Rep(\cdot)$	Fuzzy extractor probabilistic generation & reproduction functions, respectively
et	Error tolerance threshold applied in $Rep(\cdot)$
$PUF(\cdot)$	Physically unclonable function
(C_i, R_i)	i^{th} challenge response pair associated with $PUF(\cdot)$ rectified with fuzzy extractor
p	A sufficiently large prime number (160 bit number)
$\mathbb{Z}_p$	A finite (prime) field, $\mathbb{Z}_p = \{0, 1, \cdots, p-1\}$
$h(\cdot)$	Collision-resistant cryptographic one-way hash function
$\|\|, \oplus$	String concatenation and bitwise exclusive (XOR) operations, respectively

Most of the existing schemes proposed in the literature for the IoT and related environment are either insecure against various known attacks or they are inefficient in communication and computation. In this article, we aim to propose a novel secure lightweight anonymous authentication protocol for IoT environment using PUFs that can prevent impersonation of compromised smart devices in addition to resisting other well-known attacks needed for IoT security in order to eradicate the flaws in the existing user authentication mechanisms. The scheme proposed by Gope *et al.* [15] only provides user authentication mechanism in the existing literature that resists impersonation of compromised smart devices. However, the scheme proposed in this article outperforms the existing schemes including the recently proposed scheme [15] in terms of computational as well communication overheads. Furthermore, unlike the scheme proposed in [15], our proposed scheme resists ''Ephemeral Secret Leakage (ESL)'' attack (discussed in Section V-C.4) in the presence of an CK-adversary [9] (as discussed in the threat model in Section I-B). In Section VI, we also present a more comprehensive study showcasing the strength of the proposed scheme with other related existing state-of-art user authentication schemes.

IV. THE PROPOSED SCHEME

In this section, we present our proposed scheme that is a physically secure lightweight user authentication scheme in the IoT environment based on PUFs. The proposed scheme is divided into five distinct phases, namely 1) setup, 2) device enrollment, 3) user registration, 4) mutual authentication and session key agreement, and 5) maintenance. In Table 1, we define the important notations and their significance that are used in the proposed scheme.

Gateway (GWN)
Save each device SD's identity ID_d, and sets C_d and R_d along with $h(\cdot)$, $PUF(\cdot)$, $Gen(\cdot)$, $Rep(\cdot)$, et, and $\mathbb{Z}_p$, and long term secret key LTS
Smart device (SD)
Store ID_d, C_d and hd_d, along with $h(\cdot)$, $PUF(\cdot)$, $Gen(\cdot)$, $Rep(\cdot)$, et, and $\mathbb{Z}_p$

FIGURE 2. Summary of device enrollment.

The detailed description of all the phases related to the proposed scheme is provided in the following subsections.

A. SETUP PHASE

During the setup phase, the gateway node (GWN) defines the system parameters: a collision-resistant cryptographic one way hash function $h(\cdot)$, a physically unclonable function $PUF(\cdot)$, and the fuzzy extractor generator and reproduction functions $Gen(\cdot)$ and $Rep(\cdot)$. The GWN selects a prime field $\mathbb{Z}_p$ and also generates a long term secret key $LTS \in \mathbb{Z}_p$. After the setup, the system is ready for operations like device enrollment, user registration and other phases.

B. DEVICE ENROLLMENT PHASE

The IoT smart devices can be dynamically enrolled into the system in *offline mode* anytime after setup through the steps described below.

- *Step 1.* The GWN defines the identity ID_d of each smart device SD. The GWN then generates C_d, a set of n random challenges to be used during authentication for SD, where $C_d = \{C_{d_1}, \cdots, C_{d_n}\}$.[1]
- *Step 2.* The GWN computes the response set Res_d for the challenge set C_d as $Res_{d_i} = PUF(C_{d_i}), \forall i \in [1, n]$. The sets R_d and hd_d are then calculated by passing Res_d through the fuzzy generator function $Gen(\cdot)$, where $R_d = \{R_{d_i} | i \in [1,n]\}$, $hd_d = \{hd_{d_i} | i \in [1,n]\}$ and $\{R_{d_i}, hd_{d_i}\} = Gen(Res_{d_i}), \forall i \in [1, n]$.
- *Step 3.* The GWN stores the credentials $\{ID_d, C_d, hd_d\}$ along with the public system parameters $h(\cdot)$, $PUF(\cdot)$, $Gen(\cdot)$, $Rep(\cdot)$, et (an error tolerance threshold parameter used in $Rep(\cdot)$ function) and $\mathbb{Z}_p$ in the memory of SD prior to its deployment in the IoT environment. On the other hand, the GWN saves each device SD's identity ID_d and the challenge response sets C_d and R_d along with the public system parameters $h(\cdot)$, $PUF(\cdot)$, $Gen(\cdot)$, $Rep(\cdot)$, et, and $\mathbb{Z}_p$, and also its own long term secret key LTS in its database.

The device enrollment steps have been summarized in Figure 2.

[1]Additional random challenges are unnecessary in order to handle the issue of desynchronization or denial of service (DoS) attack as described in [15], because our proposed scheme does not require synchronization between the GWN and the smart devices.

User U	Gateway GWN
Enters ID_u	
$\xrightarrow[\text{secure channel}]{\langle ID_u \rangle}$	System parameters:
	$param = \{h(\cdot), PUF(\cdot), Gen(\cdot), Rep(\cdot), et, \mathbb{Z}_p\}$
	Compute $k_{u_{pre}} = h(ID_u \parallel LTS)$
	Generate DID_u,
	$PID_u = \{pid_0, \cdots, pid_s\} \in \mathbb{Z}_p$
	Save ID_u, DID_u and PID_u
	$\xleftarrow[\text{secure channel}]{SC_u = \langle DID_u, k_{u_{pre}}, PID_u, param \rangle}$
Input PW_u and imprint β_u	
Compute $\gamma_u = PUF(\beta_u)$,	
$(\alpha_u, hd_u) = Gen(\gamma_u)$,	
$IPB = h(ID_u \parallel \alpha_u \parallel PW_u)$,	
$hd_u^* = hd_u \oplus h(\alpha_u \parallel ID_u \parallel PW_u)$,	
$DID_u^* = DID_u \oplus h(ID_u \parallel PW_u \parallel \alpha_u)$,	
$k_{u_{pre}}^* = k_{u_{pre}} \oplus h(PW_u \parallel \alpha_u \parallel ID_u)$,	
$pid_i^* = pid_i \oplus h(\alpha_u \parallel PW_u \parallel ID_u \parallel i)$,	
$PID_u^* = \{pid_i^* \mid i \in [1, s]\}$	
Replace DID_u, $k_{u_{pre}}$ and PID_u with	
DID_u^*, $k_{u_{pre}}^*$ and PID_u^*, respectively	

FIGURE 3. Summary of user registration.

C. USER REGISTRATION PHASE

The users can register into the system anytime after the above setup phase in offline mode through secure channel with the following steps.

- *Step 1.* A user U picks his/her identity ID_u and sends it as the registration request message to the gateway node GWN through a secure channel.
- *Step 2.* On receiving the registration request, the GWN computes $k_{u_{pre}} = h(ID_u \parallel LTS)$ using the user U's identity ID_u and its long term secret key LTS, and also generates a dynamic identity DID_d for the U. Additionally, to handle the issue of desynchronization or DoS attack as described in [15], the GWN generates $PID_d = \{pid_0, \cdots, pid_s\}$ as a set of unlinkable pseudo-identities for the user U. Finally, the GWN issues a smart card SC_u containing the information DID_u, $k_{u_{pre}}$, PID_u and the system parameters $param = \{h(\cdot), PUF(\cdot), Gen(\cdot), Rep(\cdot), et, \mathbb{Z}_p\}$ for the user U through a secure channel.
- *Step 3.* On receiving the smart card SC_u, the user U selects his/her password PW_u and imprints the biometric β_u, and calculates $\gamma_u = PUF(\beta_u)$. Using the fuzzy generator function $Gen(\cdot)$, the smart card SC_u generates the biometric token α_u and the corresponding reproduction parameter hd_u. Next, SC_u calculates $IPB = h(ID_u \parallel \alpha_u \parallel PW_u)$ and saves it in its memory. SC_u also encrypts hd_u as $hd_u^* = hd_u \oplus h(\alpha_u \parallel ID_u \parallel PW_u)$, DID_u as $DID_u^* = DID_u \oplus h(ID_u \parallel PW_u \parallel \alpha_u)$ and PID_u as $PID_u^* = \{pid_i^* | i \in [1, s]\}$ where $pid_i^* = pid_i \oplus h(\alpha_u \parallel PW_u \parallel ID_u \parallel i)$. Finally, the values DID_u, $k_{u_{pre}}$ and PID_u in the smart card SC_u are replaced with DID_u^*, $k_{u_{pre}}^*$ and PID_u^*, respectively to complete the user registration process.

The summary of the user registration procedure has been presented in Figure 3.

D. MUTUAL AUTHENTICATION AND SESSION KEY AGREEMENT PHASE

A registered user U can access an enrolled smart device SD using the following steps described below. In this phase, both the user U and smart device SD can mutually authenticate in presence of the GWN and also negotiate a session key SK.

- *Step 1.* The user U provides his/he identity ID_u, password PW_u and imprints biometric β_u at the sensor of a specific terminal. The smart card SC_u then decrypts the biometric reproduction parameter hd_u from hd_u^* using ID_u and PW_u. By passing β_u and hd_u to the fuzzy reproduction function $Rep(\cdot)$, SC_u reconstructs the biometric token α_u. SC_u then calculates $IPB' = h(ID_u \parallel \alpha_u \parallel PW_u)$. If $IPB \neq IPB'$, the login attempt will fail. Otherwise, $DID_u = DID_u^* \oplus h(ID_u \parallel PW_u \parallel \alpha_u)$ and $k_{u_{pre}} = k_{u_{pre}}^* \oplus h(PW_u \parallel \alpha_u \parallel ID_u)$ are recovered. SC_u also selects two random nonces $k_{u1}, k_{u2} \in \mathbb{Z}_p$ from which the short term keys $k_{ud} = h(k_{u1} \parallel ID_u)$ and $k_{ug} = h(k_{u2} \parallel ID_u)$ are computed. Next, the values $Q_{ud} = k_{ud} \oplus h(ID_u \parallel k_{u_{pre}})$, $Q_{ug} = k_{ug} \oplus h(k_{u_{pre}} \parallel ID_u)$, $DID_d = ID_d \oplus h(k_{ug})$ and $Auth_u = h(k_{ug} \parallel k_{ud} \parallel k_{u_{pre}} \parallel DID_d)$ are calculated. Note that ID_d and DID_d are the identity and the single-use dynamic identity of the smart device SD. Finally SC_u composes the login request message $M_1 = \langle DID_u, Q_{ug}, Q_{ud}, DID_d, Auth_u \rangle$ and sends it to the gateway node GWN via open channel.
- *Step 2.* On receiving the login request message M_1, the GWN check for DID_u in its database. If DID_u is not found, the login request request is rejected. Otherwise, it looks up for the corresponding user identity ID_u and calculates $k_{u_{pre}} = h(ID_u \parallel LTS)$. The GWN then recovers $k'_{ud} = Q_{ud} \oplus h(ID_u \parallel k_{u_{pre}})$ and $k'_{ug} = Q_{ug} \oplus h(k_{u_{pre}} \parallel ID_u)$ from Q_{ud} and Q_{ug}, respectively. The GWN also calculates $Auth'_u = h(k'_{ug} \parallel k'_{ud} \parallel k_{u_{pre}} \parallel DID_d)$ and checks it against the received $Auth_u$. If the values match, the GWN updates DID_u with $DID'_u = h(DID_u \parallel k_{ug})$ in its database and recovers $ID_d = DID_d \oplus h(k'_{ug})$. The GWN looks up for the challenge response pair (C_{d_i}, R_{d_i}) using ID_d from the sets C_d and R_d, respectively. If it is so, the challenge-response pair (C_{d_i}, R_{d_i}) is purged from C_d and R_d. Now, the GWN computes $Q_g = k'_{ud} \oplus R_{d_i}$, $Auth_{R_d} = h(k'_{ug} \parallel R_{d_i})$ and $Auth_g = h(C_{d_i} \parallel R_{d_i} \parallel k'_{ud} \parallel Auth_{R_d})$. The GWN composes the authentication request message $M_2 = \langle C_{d_i}, Q_g, Auth_{R_d}, Auth_g \rangle$ and sends it to the accessed smart device SD for which the user U wants to access the real-time data, via an open channel.
- *Step 3.* On receiving the authentication request message M_2, the designated smart device SD looks up for hd_{d_i} corresponding to C_{d_i} from the sets C_d and hd_d. Using hd_d, the $PUF(\cdot)$ and the fuzzy reproduction function $Rep(\cdot)$, the smart device SD calculates $R'_{d_i} = rep(PUF(C_{d_i}), hd_{d_i})$, $k'^{'}_{ud} = Q_g \oplus R'_{d_i}$ and $Auth'_g = h(C_{d_i} \parallel R'_{d_i} \parallel k'^{'}_{ud} \parallel Auth_{R_d})$, and then checks $Auth'_g$ against the received $Auth_g$. If these match, the SD selects a random nonce $k_d \in \mathbb{Z}_p$ from which the short term key $k_{du} = h(k_d \parallel ID_d)$ is derived. SD then computes $Q_d = R'_{d_i} \oplus k_{du}$, $Q_{R'_d} = h(k''_{ud}) \oplus R'_{d_i}$, the session key shared with the user U as $SK = h(k_{du} \parallel k''_{ud} \parallel R'_{d_i})$, $Auth_d = h(SK \parallel R'_{d_i})$ and $HQ_R = h(R'_{d_i} \parallel Q_{ud}) \oplus Auth_{R_d}$. Finally, SD composes the authentication reply message $M_3 = \langle HQ_R, Q_d, Q_{R'_d}, Auth_d \rangle$ and sends it to U via an open channel.
- *Step 4.* On receiving the authentication reply message M_3, SC_u computes $R''_{d_i} = Q_{R'_d} \oplus h(k_{ud})$ and $Auth'_{R_d} = HQ_R \oplus h(R''_{d_i} \parallel Q_{ud})$, and checks if $Auth'_{R_d}$ matches against the value $h(k_{ug} \parallel R''_{d_i})$. If this is satisfied, SC_u computes $k'_{du} = Q_d \oplus R''_{d_i}$ and the session key shared with the accessed smart device SD as $SK' = h(k'_{du} \parallel k_{ud} \parallel R''_{d_i})$. SC_u then checks if the received $Auth_d$ is equal to $h(SK \parallel R''_{d_i})$. If it is so, SC_u sets $SK = SK'$ and $DID'_u = h(DID_u \parallel k_{ug})$, and updates DID_u^* in its memory with $DID'_u \oplus h(ID_u \parallel PW_u \parallel \alpha_u)$ for the subsequent authentication sessions in future.

The mutual authentication and session key agreement procedure has been summarized in Figure 4.

Remark 1: If the gateway node GWN fails to find DID_u in its database, it will reject the authentication request. This can occur in case of desynchronization between the GWN and a user U. In this case, the user U can reattempt with a pseudo-identity $pid_i \in PID_u$. Of course, once it is successfully authenticated with pid_i, the GWN and U will be resynchronized, and U can use DID_u as normal for subsequent authentication sessions. Additionally, if the check $Auth_d = h(SK \parallel R''_{d_i})$ fails, U should realize that the synchronization between the GWN and U has been lost, and he/she should use a pseudo-identity for the next authentication request. Note that that the pseudo-identity pid_i is valid for a single use and must be purged from PID_u after use.

E. MAINTENANCE PHASE

In this section, we describe the auxiliary procedures that are necessary for uninterrupted long-term operation of the scheme.

1) PASSWORD AND BIOMETRIC UPDATE PHASE

The procedure for updating the password and biometric information of a legal registered user U under the proposed scheme is discussed in this section.

The user U first logs into the system as described in Section IV-D using Step 1. After that U enters the new password PW_u^{new} and imprints new biometric information β_u^{new}, and calculates $\gamma_u^{new} = PUF(\beta_u^{new})$. Note that if the user U does not want to update his/her current biometrics with new biometrics, β_u^{new} will be treated as old β_u. However, it is necessary for the user U to update his/her current password with new password.

Using the fuzzy generator function $Gen(\cdot)$, the smart card SC_u generates a new biometric token α_u^{new} and the corresponding reproduction parameter hd_u^{new}. Then

User U	Gateway GWN	Smart Device SD
$\langle IPB, DID_u^*, k_{u_{pre}}^*, hd_u^* \rangle$	$\langle (C_{d_i}, R_{d_i}), DID_u, LTS \rangle$	$\langle ID_d, \{hd_{d_i}\} \rangle$
Enter ID_u & PW_u and imprint β_u		
Calculate $\gamma_u = PUF(\beta_u)$, $hd_u = hd_u^* \oplus h(ID_u \parallel PW_u)$, $\alpha_u = rep(\gamma_u, hd_u)$, $IPB' = h(ID_u \parallel \alpha_u \parallel PW_u)$		
If $IPB \neq IPB'$ terminate		
Calculate $DID_u = DID_u^* \oplus h(ID_u \parallel PW_u \parallel \alpha_u)$, $k_{u_{pre}} = k_{u_{pre}}^* \oplus h(PW_u \parallel \alpha_u \parallel ID_u)$		
Select $k_{u1}, k_{u2} \in \mathbb{Z}_p$		
Compute $k_{ud} = h(k_{u1} \parallel ID_u)$, $k_{ug} = h(k_{u2} \parallel ID_u)$, $Q_{ud} = k_{ud} \oplus h(ID_u \parallel k_{u_{pre}})$, $Q_{ug} = k_{ug} \oplus h(k_{u_{pre}} \parallel ID_u)$, $DID_d = ID_d \oplus h(k_{ug})$, $Auth_u = h(k_{ug} \parallel k_{ud} \parallel k_{u_{pre}} \parallel DID_d)$		
$M_1 = \langle DID_u, Q_{ug}, Q_{ud}, DID_d, Auth_u \rangle \rightarrow$		
	Check for DID_u	
	Lookup $ID_u \leftarrow DID_u$	
	Compute $k_{u_{pre}} = h(ID_u \parallel LTS)$, $k'_{ud} = Q_{ud} \oplus h(ID_u \parallel k_{u_{pre}})$, $k'_{ug} = Q_{ug} \oplus h(k_{u_{pre}} \parallel ID_u)$, $Auth'_u = h(k'_{ug} \parallel k'_{ud} \parallel k_{u_{pre}} \parallel DID_d)$,	
	If $Auth'_u \neq Auth_u$ terminate	
	Update $DID'_u = h(DID_u \parallel k_{ug})$	
	Compute $ID_d = DID_d \oplus h(k'_{ug})$	
	Lookup $C_{d_i}, R_{d_i} \leftarrow ID_d$	
	Compute $Q_g = k'_{ud} \oplus R_{d_i}$, $Auth_{R_d} = h(k'_{ug} \parallel R_{d_i})$. $Auth_g = h(C_{d_i} \parallel R_{d_i} \parallel k'_{ud} \parallel Auth_{R_d})$	
	$M_2 = \langle C_{d_i}, Q_g, Auth_{R_d}, Auth_g \rangle \rightarrow$	
		Compute $R'_{d_i} = rep(PUF(C_{d_i}), hd_{d_i})$, $k''_{ud} = Q_g \oplus R'_{d_i}$, $Auth'_g = h(C_{d_i} \parallel R'_{d_i} \parallel k''_{ud} \parallel Auth_{R_d})$
		If $Auth'_g \neq Auth_g$ terminate
		Select $k_d \in \mathbb{Z}_p$
		Calculate $k_{du} = h(k_d \parallel ID_d)$, $Q_d = R'_{d_i} \oplus k_{du}$, $Q_{R'_d} = h(k''_{ud}) \oplus R'_{d_i}$, $SK = h(k_{du} \parallel k''_{ud} \parallel R'_{d_i})$, $Auth_d = h(SK \parallel R'_{d_i})$, $HQ_R = h(R'_{d_i} \parallel Q_{ud}) \oplus Auth_{R_d}$
		$M_3 = \langle HQ_R, Q_d, Q_{R'_d}, Auth_d \rangle \leftarrow$
Compute $R''_{d_i} = Q_{R'_d} \oplus h(k_{ud})$, $Auth'_{R_d} = HQ_R \oplus h(R''_{d_i} \parallel Q_{ud})$		
If $Auth'_{R_d} \neq h(k_{ug} \parallel R''_{d_i})$ terminate		
Compute $k'_{du} = Q_d \oplus R''_{d_i}$, $SK' = h(k'_{du} \parallel k_{ud} \parallel R''_{d_i})$		
If $Auth_d = h(SK \parallel R''_{d_i})$ $SK = SK'$, $DID'_u = h(DID_u \parallel k_{ug})$, $DID_u^* = DID'_u \oplus h(ID_u \parallel PW_u \parallel \alpha_u)$		

FIGURE 4. Summary of mutual authentication and session key exchange.

SC_u recalculates $IPB^{new} = h(ID_u \parallel \alpha_u^{new} \parallel PW_u^{new})$, $hd_u^* = hd_u^{new} \oplus h(ID_u \parallel PW_u^{new})$, $DID_u^* = DID_u \oplus h(ID_u \parallel PW_u^{new} \parallel \alpha_u^{new})$, $k_{u_{pre}}^* = k_{u_{pre}} \oplus h(PW_u^{new} \parallel \alpha_u^{new} \parallel ID_u)$, $PID_u^* = PID_u \oplus h(\alpha_u^{new} \parallel PW_u^{new} \parallel ID_u)$ and commits the updated values in its memory. It is worth noticing that this phase is completely executed locally without further involving the GWN.

User U	Smart card SC_u
	$\langle DID_u^*, k_{u_{pre}}^*, hd_u^* \rangle$
Enter ID_u & PW_u and imprint β_u	
	Calculate $\gamma_u = PUF(\beta_u)$, $hd_u = hd_u^* \oplus h(ID_u \parallel PW_u)$, $\alpha_u = rep(\gamma_u, hd_u)$, $IPB' = h(ID_u \parallel \alpha_u \parallel PW_u)$
	If $IPB \neq IPB'$ terminate
	Compute $DID_u = DID_u^* \oplus h(ID_u \parallel PW_u \parallel \alpha_u)$, $k_{u_{pre}} = k_{u_{pre}}^* \oplus h(PW_u \parallel \alpha_u \parallel ID_u)$, $PID_u = PID_u^* \oplus h(\alpha_u \parallel PW_u \parallel ID_u)$
Enter new PW_u^{new} and imprint β_u^{new}	
	Calculate $(\alpha_u^{new}, hd_u^{new}) = Gen(\gamma_u^{new})$, $IPB^{new} = h(ID_u \parallel \alpha_u^{new} \parallel PW_u^{new})$, $hd_u^* = hd_u^{new} \oplus h(ID_u \parallel PW_u^{new})$, $DID_u^* = DID_u \oplus h(ID_u \parallel PW_u^{new} \parallel \alpha_u^{new})$, $k_{u_{pre}}^* = k_{u_{pre}} \oplus h(PW_u^{new} \parallel \alpha_u^{new} \parallel ID_u)$, $PID_u^* = PID_u \oplus h(\alpha_u^{new} \parallel PW_u^{new} \parallel ID_u)$
	Update values in SC_u

FIGURE 5. Summary of password and biometric update.

The password and biometric update procedure has been summarized in Figure 5.

2) PSEUDO IDENTITY RENEWAL PHASE

As noted in Remark 1, the user U utilizes $pid_i \in PID_d$ to authenticate in case of desyncronization with the GWN. The set PID_d is finite and will eventually get exhausted. Before this happens, the user U must acquire additional pseudo identities. The following steps are essential to achieve this goal.

- *Step 1.* The user U logs into the system as described in Section IV-D (see Step 1), and other steps that are very similar. U then composes the message $M_{pid_1} = \langle DID_u, Q_{ug}, Auth_u \rangle$ which is sent to the gateway node GWN via open channel.
- *Step 2.* On receiving M_{pid_1}, the GWN checks for DID_u in its database. If DID_u is not found, the authentication request is rejected. Otherwise, the GWN looks up for the corresponding user identity ID_u and calculates $k_{u_{pre}} = h(ID_u \parallel LTS)$, and also recovers $k'_{ug} = Q_{ug} \oplus h(k_{u_{pre}} \parallel ID_u)$ from Q_{ug}. The GWN then calculates $Auth'_u = h(k'_{ug} \parallel k_{u_{pre}})$ and checks it against the received $Auth_u$. If the values match, the GWN updates DID_u with $DID'_u = h(DID_u \parallel k_{ug})$ and generates $PID'_d = \{pid_0, \cdots, pid_s\}$ as a new set of unlinkable pseudo-identities for the user U. The GWN saves DID'_u as DID_u and appends PID'_d to PID_d in its memory. Now, the GWN computes $EPID = PID'_u \oplus h(k'_{ug} \parallel k_{u_{pre}} \parallel ID_u)$, $Auth_g = h(PID'_u \parallel k'_{ud} \parallel ID_u)$, and finally composes the message $M_{pid_2} = \langle EPID, Auth_g \rangle$ to sends it to the user U via open channel.
- *Step 3.* On receiving M_{pid_2}, U computes $PID'_u = EPID' \oplus h(k'_{ug} \parallel k_{u_{pre}} \parallel ID_u)$, $Auth'_g = h(PID'_u \parallel k'_{ud} \parallel ID_u)$ and

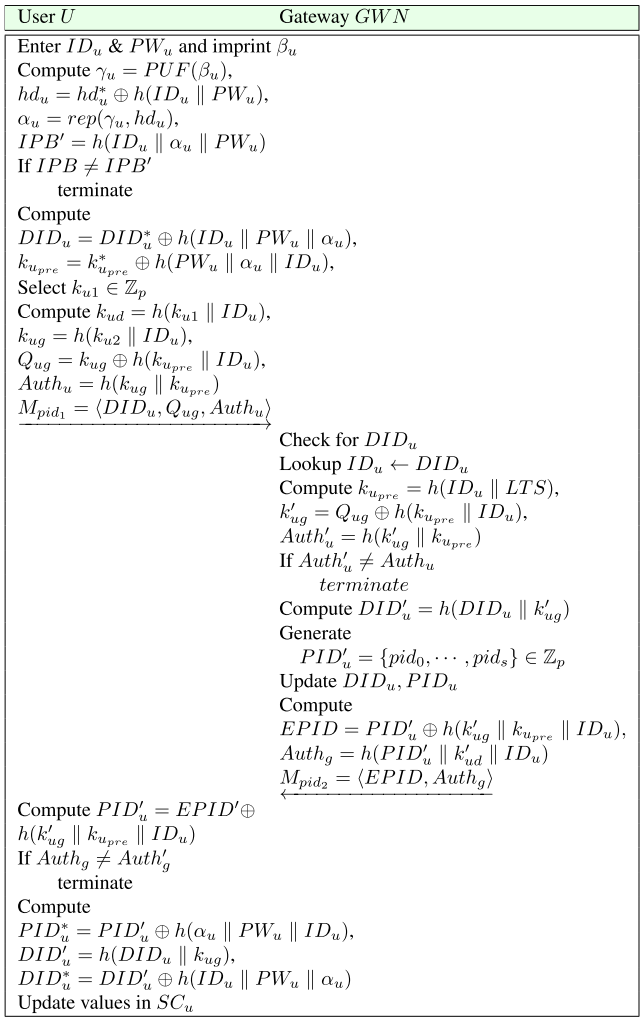

FIGURE 6. Summary of pseudo identity renewal.

checks it against the received $Auth_g$. If the values match, SC_u updates $DID'_u = h(DID_u \| k_{ug})$, prepends PID_u to PID'_u and calculates $PID_u^* = PID'_u \oplus h(\alpha_u \| PW_u \| ID_u)$ and $DID_u^* = DID'_u \oplus h(ID_u \| PW_u \| \alpha_u)$. Finally, SC_u commits the updated DID_u^* and PID_u^* into its memory.

The pseudo identity renewal procedure has been summarized in Figure 6.

3) CHALLENGE RESPONSE RENEWAL PHASE

The challenge response pairs ($C_{d_i} \in C_d, R_{d_i} \in R_d$) utilized for mutual authentication between a smart device *SD* and gateway node *GWN* are finite and will also eventually get exhausted. Before this situation occurs, the gateway node *GW* must acquire additional challenge response pairs for future operation. The steps involved in this process are described below.

- *Step 1.* The *GWN* looks up for a challenge response pair (C_{d_i}, R_{d_i}) using ID_d from the sets C_d and R_d. *GWN* then selects a nonce $k_g \in \mathbb{Z}_p$ from which the short term key $k_{gd} = h(k_g \| ID_d)$ is computed. The *GWN* also generates C_d^{new} as a set of another n random challenges

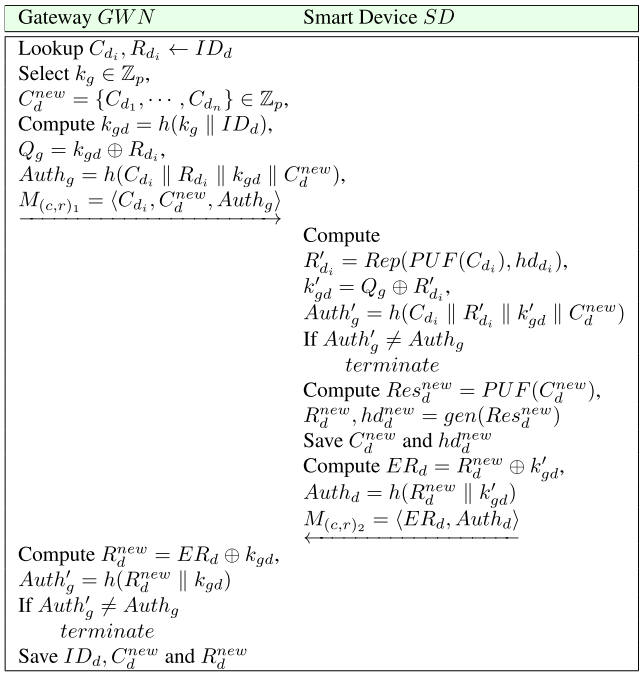

FIGURE 7. Summary of challenge response renewal.

to be used for future authentication, computes $Q_g = k_{gd} \oplus R_{d_i}$, $Auth_g = h(C_{d_i} \| R_{d_i} \| k_{gd} \| C_d^{new})$ and sends the message $M_{(c,r)_1} = \langle C_{d_i}, C_d^{new}, Auth_g \rangle$ to the smart device *SD* via open channel.

- *Step 2.* On receiving $M_{(c,r)_1}$, *SD* looks up for hd_{d_i} corresponding to C_{d_i} from the sets C_d and hd_d. Using hd_d, the $PUF(\cdot)$ and the fuzzy reproduction function $Rep(\cdot)$, *SD* calculates $R'_{d_i} = Rep(PUF(C_{d_i}), hd_{d_i})$, $k'^{'}_{gd} = Q_g \oplus R'_{d_i}$ and $Auth'_g = h(C_{d_i} \| R'_{d_i} \| k'_{gd} \| C_d^{new})$ and checks $Auth'_g$ against the received $Auth_g$. If these values match, *SD* computes the response set Res_d^{new} for the challenge set C_d^{new} as $Res_{d_i}^{new} = PUF(C_{d_i}^{new})$ $\forall i \in [1, n]$. The sets R_d^{new} and hd_d^{new} are then calculated by passing Res_d^{new} through the fuzzy generator function $Gen(\cdot)$ a $(R_{d_i}^{new}, hd_{d_i}^{new}) = Gen(Res_{d_i}^{new})$ $\forall i \in [1, n]$. *SD* appends the challenge C_d^{new}, the corresponding set of reconstruction data hd_d^{new} to C_d and hd_d, respectively. Finally, *SD* computes $ER_d = R_d^{new} \oplus k'_{gd}$, $Auth_d = h(R_d^{new} \| k'_{gd})$, composes another message $M_{(c,r)_2} = \langle ER_d, Auth_d \rangle$ and sends it to the gateway node *GWN* via open channel.
- *Step 3.* On receiving $M_{(c,r)_2}$, the *GWN* computes $R_d^{new} = ER_d \oplus k_{gd}$ and $Auth'_g = h(R_d^{new} \| k_{gd})$. If the calculated $Auth'_g$ is equal to $Auth_g$, the *GWN* appends C_d^{new} and R_d^{new} to C_d and R_d, respectively. The *GWN* commits the updated values its database.

The challenge response renewal procedure has been summarized in Figure 7.

V. SECURITY ANALYSIS

Wang *et al.* [54] made some important observations on security-related issues while analyzing several existing authentication protocols in the literature. They found that

attaining the soundness of authentication protocols is still an open problem. They noticed that the standard model-based formal security analysis can not capture some structural mistakes while proving the security of a protocol. Hence, it is extremely essential to design and analyze the authentication protocols which should provide high security. Due to this reason, other methods such as ''formal security analysis using the Real-Or-Random (RoR) model [12], formal security verification using AVISPA tool [13] and also informal security analysis'' are essential to assure that the design authentication protocol to be secure with high probability.

In Section V-A, we utilize the broadly-accepted ROR model [12] to formally analyze the security of the proposed scheme. In Section V-B, through the formal security verification using AVISPA simulation tool [13] we verify that the proposed scheme is free from man-in-the-middle and replay attacks. Additionally, in Section V-C, we also informally demonstrate that the proposed scheme is also secure against various other well-known attacks.

A. FORMAL SECURITY ANALYSIS THROUGH REAL-OR-RANDOM MODEL

In this section, we describe the Real-Or-Random (ROR) model proposed in [12], and then utilize it for formal security analysis.

1) PARTICIPANTS

Let π_U^u, π_{GWN}^g and π_{SD}^d denote the u^{th}, g^{th} and d^{th} instances corresponding to a user U, gateway node GWN and smart device SD, respectively. These are also called oracles [8], [40].

2) PARTNERING

Two instances π_U^u and π_{SD}^d are said to be partnered if and only if the following ''two conditions are fulfilled simultaneously: 1) the communication session id sid is common between them and 2) partial transcript of all message exchanged between them are unique''.

3) FRESHNESS

π_U^u and π_{SD}^d are fresh provided that the session key SK between U and SD has not been divulged to an adversary $\mathcal{A}$.

4) ADVERSARY

Under the ROR model, the adversary $\mathcal{A}$ is assumed have a complete control over the communication channel. Consequently, $\mathcal{A}$ can eavesdrop, alter, delete and even insert fabricated messages during communication. Additionally, the adversary $\mathcal{A}$ can execute the following queries.

- $Execute(\pi^u, \pi^d)$: By execution of this query, $\mathcal{A}$ can intercept all the transmitted messages among U, GWN and SD. Due to intercepting nature, an eavesdropping attack is modeled under this query.
- $Send(\pi^d, m)$: Execution of this query enables $\mathcal{A}$ to send a message, say msg to its participating instance π^d, and also to receive a response message in reply. This query is treated as an active attack.
- $CorruptSC(\pi^u)$: By executing this query, $\mathcal{A}$ can learn the credentials $\{IPB, DID_u^*, k_{u_{pre}}^*$, and $hd_u^*\}$ stored in a legal user U's stolen or lost smart card, SC_u.
- $CorruptSD(\pi^d)$: By executing this query, $\mathcal{A}$ can extract the credentials $\{ID_d, hd_{d_i}\}$ from a captured IoT sensing device SD. It is also assumed that the queries $CorruptSC$ and $CorruptSD$ provide the weak corruption model [40]. Consequently, a participant instance's short-term keys and the internal data are not corrupted.
- $Test(\pi^u, \pi^d)$: This query determines the semantic security of the established session key SK between U and SD following the indistinguishability in the ROR model [12]. At first $\mathcal{A}$ preforms an unbiased coin toss c. The outcome of this coin toss decides the result of the $Test$ query. If SK is fresh, π^u or π^d produces SK upon the satisfaction of the condition $c = 1$ or a random number for the fulfillment of the condition $c = 0$. In all other cases, it returns a null value.

5) SEMANTIC SECURITY OF SESSION KEY

According to the ROR model, $\mathcal{A}$ must distinguish between an instance's actual session key and a random key. $\mathcal{A}$ can perform the repeated number of $Test(\cdot)$ queries to π^u or π^d, and saves the result of $Test$ into bit b. $\mathcal{A}$ wins the game if $b = b'$, where b' is a randomly guessed bit. The advantage of $\mathcal{A}$ in breaking the semantic security of the proposed authenticated key agreement (AKE), say $\mathcal{P}$ in time t is defined as $Adv_{\mathcal{P},\mathcal{A}}^{AKE}(t) = |2.Pr[SUCCESS] - 1|$, where $SUCCESS$ represents an event such that $\mathcal{A}$ wins the game.

6) RANDOM ORACLE

All communicating entities in the proposed scheme including $\mathcal{A}$ will have access to the secure PUF, $PUF(\cdot)$ as well as a collision resistant hash function, $h(\cdot)$. Both are modeled as random oracles, say $\mathcal{HO}$.

7) SECURITY PROOF

By utilizing the definition of the secure PUF and the collision-resistant hash function from Section II, and acknowledging that passwords obey Zipf's law [55] and the above described ROR model, Theorem 1 provides the semantic security of the proposed scheme.

Theorem 1: Let $\mathcal{A}$ be a polynomial time adversary running against the proposed scheme $\mathcal{P}$ under the ROR model, in which user-chosen passwords follow the Zipf's law [55], and l_1 and l_2 denote the number of bits in the biometric secret key α_u and the secret user identity ID_u, respectively. If $Adv_{\mathcal{P},\mathcal{A}}^{AKE}$ denotes $\mathcal{A}$'s advantage in breaking $\mathcal{P}$'s semantic security in order to derive the session key between a legal registered user U and an accessed IoT sensing device SD, then

$$Adv_{\mathcal{P},\mathcal{A}}^{AKE}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_P^2}{|PUF|} + 2\max\{C'.q_s^{s'}, \frac{q_s}{2^{l_1}}, \frac{q_s}{2^{l_2}}\},$$

where q_h, q_P and q_s are the number of hash, PUF and *Send* queries, respectively, $|Hash|$ and $|PUF|$ define the range spaces of $h(\cdot)$ and $PUF(\cdot)$, respectively, and C' and s' are the Zipf's parameters [55].

Proof: We follow our proof analogous to the proof that presented in [15], [56], and [57]. G_0-G_4 are the five sequential games are defined. The event $SUCCESS_i$ denotes that the adversary $\mathcal{A}$ can successfully guess the bit c in the game G_j, $j \in [0, 4]$. The games are described in detailed as follows.

- **Game** G_0: This game corresponds to an actual (real) attack on the proposed scheme, $\mathcal{P}$ by $\mathcal{A}$. Since bit c is guessed at the beginning of G_0, it is follows that

$$Adv^{AKE}_{\mathcal{P},\mathcal{A}}(t) = |2.Pr[SUCCESS_0] - 1|. \quad (1)$$

- **Game** G_1: This game models as an eavesdropping attack, where $\mathcal{A}$ can query $Execute(\pi^u, \pi^d)$ oracle to intercept the messages $M_1 = \langle DID_u, Q_{ug}, Q_{ud}, DID_d, Auth_u\rangle$, $M_2 = \langle C_{d_i}, Q_g, Auth_{R_d}, Auth_g\rangle$ and $M_3 = \langle HQ_R, Q_d, Q_{R'_d}, Auth_d\rangle$ during login & authentication process. Afterwards $\mathcal{A}$ can also query *Test* oracle and determine if the result is the actual session key SK or a random number. Note that in the proposed scheme, $SK = h(k_{du} \parallel k''_{ud} \parallel R'_{d_i}) = h(k'_{du} \parallel k_{ud} \parallel R''_{d_i})$ is the established session key between a user U and a smart device SD. To compute SK, $\mathcal{A}$ requires the parallel knowledge of short term secrets (k_{u1} and k_d) as well as long term secrets (ID_u and ID_d). As these values are unknown to $\mathcal{A}$, only the intended user U and smart device SD can compute SK. Therefore, $\mathcal{A}$'s probability of wining the game G_1 is not increased through an eavesdropping attack. Consequently, we have the following result:

$$Pr[SUCCESS_1] = Pr[SUCCESS_0]. \quad (2)$$

- **Game** G_2: Under this game, the *Send* and hash queries are simulated. This game is modeled as an active attack, where $\mathcal{A}$ can attempt to fool a legitimate participant into accepting a modified message. $\mathcal{A}$ is permitted to make repeated queries to the random oracles to examine the presence of hash collisions. However, since all the messages M_1, M_2 and M_3 contain random nonces, no hash coalition occurs when $\mathcal{A}$ queries the *Send* oracle with the help of $h(\cdot)$. It is worth noticing that both the games G_1 and G_2 are ''indistinguishable'' except the *Send* and hash queries are simulated in G_2. Thus, by using the birthday paradox results, we have

$$|Pr[SUCCESS_2] - Pr[SUCCESS_1]| \leq \frac{q_h^2}{2|Hash|}. \quad (3)$$

- **Game** G_3: This game is as an extension to G_2 where the simulation of PUF queries are included in this game. Using analogous argument provided in G_2, the secure PUF(·) function property (discussed in Section II-B) gives the following result:

$$|Pr[SUCCESS_3] - Pr[SUCCESS_2]| \leq \frac{q_P^2}{2|PUF|}. \quad (4)$$

- **Game** G_4: This is the final game and it is considered as an extension of the previous game G_3, which incorporates the *CorruptSC* and *CorruptSD* queries simulation. Through the queries to these oracles, $\mathcal{A}$ can extract $\langle IPB, DID^*_u, k^*_{u_{pre}}, hd^*_u\rangle$ and $\langle ID_d, \{hd_{d_i}\}|\forall i \in [1, n]\rangle$ from the smart card of the user U and from the smart device SD, respectively. For non-compromised IoT smart device SD, both ID_d and the set $\{hd_{d_i}\}$ are also distinct. However, the probability of guessing the biometric secret key σ_i of l_1 bits, and secret identity of l_2 bits, are approximately $\frac{1}{2^{l_1}}$ and $\frac{1}{2^{l_2}}$, respectively [58]. In addition, $\mathcal{A}$ can leverage the Zipf's law on passwords [55] to guess the passwords. If we just consider trawling guessing attacks, the advantage of $\mathcal{A}$ will be over 0.5 when $q_s = 10^7$ or 10^8 [55]. Furthermore, if we account for targeted guessing attacks where $\mathcal{A}$ can utilize the target user's personal information, $\mathcal{A}$ will have an advantage over 0.5 when $q_s \leq 10^6$ [55]. In practice, arbitrarily many wrong password attempts are not permitted in the system. In the absence of guessing attacks, both the games G_3 and G_4 are identical. Thus, we have following result [56]:

$$|Pr[SUCCESS_4] - Pr[SUCCESS_3]| \leq \max\{C'.q_s^{s'}, \frac{q_s}{2^{l_1}}, \frac{q_s}{2^{l_2}}\}. \quad (5)$$

Finally, to win the game G_4, $\mathcal{A}$ needs to guess bit b' after querying the *Test* oracle. Thus, it is clear that

$$|Pr[SUCCESS_4] = \frac{1}{2}. \quad (6)$$

From Eqs. (1), (2) and (6), we have

$$\begin{aligned}\frac{1}{2}Adv^{AKE}_{\mathcal{P},\mathcal{A}}(t) &= |Pr[SUCCESS_0] - \frac{1}{2}| \\ &= |Pr[SUCCESS_1] - \frac{1}{2}| \\ &= |Pr[SUCCESS_1] - |Pr[SUCCESS_4]|. \quad (7)\end{aligned}$$

Applying the triangular inequality and using Eqs. (3), (4) and (5), we obtain

$$\begin{aligned}&|Pr[SUCCESS_1] - |Pr[SUCCESS_4]| \\ &\leq |Pr[SUCCESS_1] - |Pr[SUCCESS_3]| \\ &\quad + |Pr[SUCCESS_3] - |Pr[SUCCESS_4]| \\ &\leq |Pr[SUCCESS_1] - |Pr[SUCCESS_2]| \\ &\quad + |Pr[SUCCESS_2] - |Pr[SUCCESS_3]| \\ &\quad + |Pr[SUCCESS_3] - |Pr[SUCCESS_4]| \\ &\leq \frac{q_h^2}{2|Hash|} + \frac{q_P^2}{2|PUF|} \\ &\quad + \max\{C'.q_s^{s'}, \frac{q_s}{2^{l_1}}, \frac{q_s}{2^{l_2}}\}. \quad (8)\end{aligned}$$

Finally, by solving Eqs. (7) and (8), we obtain the required result:

$$Adv^{AKE}_{\mathcal{P},\mathcal{A}}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_P^2}{|PUF|} + 2\max\{C'.q_s^{s'}, \frac{q_s}{2^{l_1}}, \frac{q_s}{2^{l_2}}\}.$$

B. FORMAL SECURITY VERIFICATION THROUGH AVISPA SIMULATION

In this section, we perform the formal security verification on the proposed scheme using the broadly-accepted AVISPA tool [13].

AVISPA is a push button tool for the automated validation of security protocols. AVISPA implements the Dolev-Yao (DY) threat model [6] to test if a security protocol is safe or unsafe against replay & man-in-the-middle attacks. The security protocol to be analyzed in AVISPA requires to be implemented under the role-oriented language, known as ''High Level Protocol Specification Language (HLPSL)'' [59]. A built-in translator, called HLPSL2IF, converts HLPSL code to the ''Intermediate Format (IF)''. The IF is then passed into one of the four available backends for AVISPA to produce the ''Output Format (OF)''.

The four backends in AVISPA are as follows [13]:

- The first backend is ''On-the-fly Model-Checker (OFMC) that does several symbolic techniques to explore the state space in a demand-driven way''.
- The second backend is the ''CL-AtSe (Constraint-Logic-based Attack Searcher) that provides a translation from any security protocol specification written as transition relation in intermediate format into a set of constraints which are effectively used to find whether there are attacks on protocols''.
- The third backend is the ''SAT-based Model-Checker (SATMC) that builds a propositional formula which is then fed to a state-of-the-art SAT solver and any model found is translated back into an attack''.
- The fourth backend is the ''TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols) that approximates the intruder knowledge by using regular tree languages''.

The OF has various sections as described below [13].

- SUMMARY: It mentions ''whether the tested protocol is safe, unsafe, or whether the analysis is inconclusive''.
- DETAILS: It tells ''a detailed explanation of why the tested protocol is concluded as safe, or under what conditions the test application or protocol is exploitable using an attack, or why the analysis is inconclusive''.
- PROTOCOL: This defines the ''HLPSL specification of the target protocol in IF''.
- GOAL: It is ''the goal of the analysis which is being performed by AVISPA using HLPSL specification''.
- BACKEND: It provides ''the name of the back-end that is used for the analysis, that is, one of OFMC, CL-AtSe, SATMC and TA4SP''.
- Final section includes ''the trace of a possible vulnerability to the target protocol, if any, along with some useful statistics and relevant comments''.

More details regarding AVISPA and HLPSL can be found in [13].

The user registration, device enrollment, login & authentication phases for the proposed scheme are implemented in HLPSL. In our implementation, three basic roles for a user U, the GWN and a smart device SD are defined in HLPSL. The compulsory roles for the session and goal & environment are also defined in HLPSL.

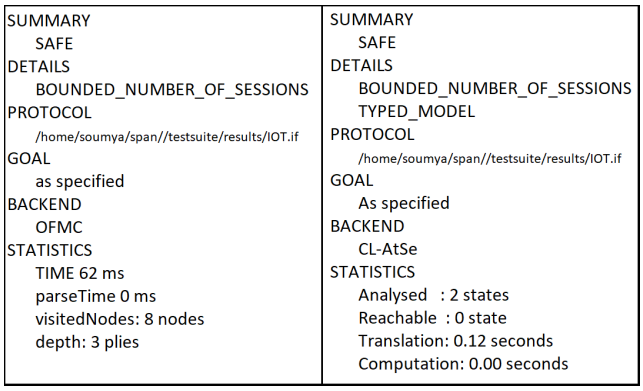

FIGURE 8. The simulation results under OFMC and CL-AtSe back-ends.

We then evaluate the proposed scheme against replay and man-in-the-middle attacks under the popular backends, OFMC and CL-AtSe using the SPAN, the Security Protocol ANimator for AVISPA tool [60]. There are three verifications associated with the testing of the proposed scheme [13]: 1) ''executability checking on non-trivial HLPSL specifications''; 2) ''replay attack checking''; and 3) ''Dolev-Yao (DY) model checking'' [6]. The first one is essential for assuring that the proposed protocol should reach to a state where a possible attack can be found while executing the protocol. Our HLPSL implentation assures that the proposed protocol was translated to HLPSL specification, which satisfied the design citeria (goals) for achieving the executability checking. The simulation was carried out for the execution tests with ''a bounded number of sessions''. For replay attack checking on the proposed protocol, both the considered backends (OFMC as well as CL-AtSe) check whether any the authorized agents can execute the specified protocol by searching a passive intruder. These back-ends have the ability to give the intruder (i) about the knowledge of some normal sessions between the legitimate agents. In addition, both OFMC & CL-AtSe backends can verify whether there is any man-in-the-middle attack mounted by i for the DY model checking. Fig. 8 presenting the simulation results show that the proposed scheme is secure against replay & man-in-the middle attacks.

C. INFORMAL SECURITY ANALYSIS

In this section, through informal security analysis, we demonstrate the security features of the proposed scheme as well as its resilience against well-known attacks.

1) ATTAINMENT OF MUTUAL AUTHENTICATION

In the proposed authentication scheme, during the authentication phase the GWN establishes trust in the authenticity of U if it can look up its identity ID_u from its memory using the received DID_u. The check on $Auth_u$ ensures the integrity of the received message. SD on receiving the

message $M_2 = \langle C_{d_i}, Q_g, Auth_{R_d}, Auth_g \rangle$ computes $Auth'_g$ and checks it against the received $Auth_g$. If the values match, SD can trust that the message is genuinely from the GWN. U on receiving the message $M_3 = \langle HQ_R, Q_d, Q_{R'_d}, Auth_d \rangle$, computes R''_{d_i} and $Auth'_{R_d}$ from the received values. If $Auth'_{R_d} \neq h(k_{ug} \parallel R''_{d_i})$, U authenticate SD. Thus, mutual authentication between the user U and the smart device SD is attained in the proposed scheme.

2) ATTAINMENT OF ANONYMITY AND UNTRACEABILITY

An eavesdropping adversary $\mathcal{A}$ can monitor the messages M_1, M_2 and M_3. However, none of these eavesdropped messages contain any identifying information for user or smart device in plaintext formats. Thus, the proposed scheme provides both user and smart device anonymity. Moreover, all of these messages are composed using the random nonces and long-term secrets, and thus, these are dynamic in nature across different authentication sessions. Therefore, it is infeasible for $\mathcal{A}$ to trace both the user and smart device across sessions. Thus, the proposed scheme preserves the ''untraceability property'' for user and smart device.

3) ATTAINMENT OF FORWARD AND BACKWARD SECRECY

Assuming that $\mathcal{A}$ can some how learn the session key SK along with all its contributing secret values k_{u_1}, ID_u, k_d, ID_d and R_{d_i} under the CK-adversary model (as discussed in the threat model in Section I-B). All other values are for single use, and therefore, compromise of a particular session will not compromise the session keys of any sessions previously established or to be established in future. Thus, the proposed scheme ensures ''forward and backward secrecy''.

4) RESILIENCE AGAINST EPHEMERAL SECRET LEAKAGE (ESL) ATTACK

In the proposed scheme, both a user U and a smart device SD establish a common session key $SK = h(k_{du} \parallel k_{ud} \parallel R_{d_i})$ during the execution of login & authentication phase, where k_{ud} is a secret comprising of a short term secret k_{u_1} and long term secret ID_u. Similarly, k_{du} is another secret comprising of a short term secret k_d and long term secret ID_d, and R_{d_i} is a long term single use secret.

The security of the session key SK is then based on the following two cases:

- *Case 1.* Assume that $\mathcal{A}$ has the short term secret credentials k_{u_1} and k_d. Then, it is computationally infeasible for $\mathcal{A}$ to calculate the session key SK without knowledge of the long term secret credentials.
- *Case 2.* If some or all of the long term secrets ID_u, ID_d and R_{d_i} are revealed to $\mathcal{A}$, it is also computationally infeasible for $\mathcal{A}$ to calculate SK without short term secrets k_{u_1} and k_d.

Thus, $\mathcal{A}$ can derive the valid session key SK only if both short and long term secrets are exposed at once. Hence, it is evident that the proposed scheme is resilient against ''ESL attack''.

5) RESILIENCE AGAINST IMPERSONATION ATTACKS

Assume that an adversary $\mathcal{A}$ attempts to impersonate a legitimate user U. As the pre-shared dynamic identity DID_U and the set pseudo-identities $\{PID_u\}$ are of single use, $\mathcal{A}$ cannot composite the message $M_1 = \langle DID_u, Q_{ug}, Q_{ud}, DID_d, Auth_u \rangle$. Similarly, if $\mathcal{A}$ attempts to impersonate the GWN by intercepting M_1, generating the message $M_2 = \langle C_{d_i}, Q_g, Auth_{R_d}, Auth_g \rangle$ is computationally infeasible as $\mathcal{A}$ does not have access to the challenge response pair (C_{d_i}, R_{d_i}). Hence, $\mathcal{A}$ will not succeed in composing $Auth_g = h(C_{d_i}||R_{d_i}||K_{ug}||Auth_{R_d})$ that is consistent with C_{d_i}. Finally, if $\mathcal{A}$ attempts to impersonate SD by generating $M_3 = \langle HQ_R, Q_d, Q_{R'_d}, Auth_d \rangle$, it will be computationally infeasible. As $\mathcal{A}$ is not able to recreate R_{d_i} and $HQ_R = h(R'_{d_i} \parallel Q_{ud}) \oplus Auth_{R_d}$, $Q_{R'_d} = h(k''_{ud}) \oplus R'_{d_i}$ and $Auth_d = h(SK \parallel R'_{d_i})$, he or she cannot compose a consistent M_3. Thus, the proposed scheme is resistant against ''impersonation attacks''.

6) RESILIENCE AGAINST STOLEN SMART CARD AND OFFLINE GUESSING ATTACKS

Assume that an adversary $\mathcal{A}$ extracts the secret credentials from a lost or stolen SC_i of a registered user U through power analysis attacks [7]. Then, $\mathcal{A}$ will have the credentials $IPB, DID^*_u, k^*_{u_{pre}}$ and hd^*_u. But, as all of these values are secured with the secret identity ID_u, password PW_u and the biometric key α_u, $\mathcal{A}$ needs simultaneous guessing of all three factors to compromise the security of the proposed scheme. Thus, it becomes a computationally infeasible problem for $\mathcal{A}$, and as a result, the proposed scheme is secure against ''offline guessing attacks in conjunction with the stolen smart card attack''.

7) RESILIENCE AGAINST PRIVILEGED-INSIDER ATTACK

An adversary $\mathcal{A}$, who acts as a privileged-insider user of the GWN, can intercept the initial registration request information ID_u. Also, none of the authentication messages contains any value dependent on the secrecy of ID_u. Additionally, assuming that the privileged adversary attempts the previously discussed offline guessing attack with a stolen smart card, he or she will still need to simultaneously guess password PW_u and biometric key α_u. It is then a computationally infeasible task for $\mathcal{A}$ too. Thus, the proposed scheme is secure against ''privileged-insider attack''.

8) RESILIENCE AGAINST PHYSICAL CAPTURE OF SMART DEVICE

Suppose $\mathcal{A}$ can physically capture some smart devices. Then, $\mathcal{A}$ can extract all the secret credentials from the memory of a physically captured smart device SD compromising of the information $\{ID_d, C_d, hd_d\}$ from SD's memory. However, as ID_d and $\{C_d\}$ are generated randomly, these are distinct and independent for all deployed smart devices. Hence, the compromised information do not help in computing the session keys among a user U and other non-compromised sensing devices SD'. Additionally, due to

TABLE 2. Computation costs comparison.

Scheme	User	Gateway node	Sensing device	Total cost
Our	$17T_h + T_f$	$8T_h$	$6T_h + T_f$	$31T_h + 2T_f$
	≈ 71.575 ms	≈ 4 ms	≈ 66.075 ms	≈ 141.65 ms
Gope *et al.* [15]	$6T_h + 3T_f$	$9T_h$	$4T_h + 2T_f$	$19T_h + 5T_f$
	≈ 192.225 ms	≈ 4.5 ms	≈ 128.15 ms	≈ 324.875 ms
Zhou *et al.* [52]	$10T_h$	$7T_h$	$19T_h$	$36T_h$
	≈ 5 ms	≈ 3.5 ms	≈ 9.5 ms	≈ 18 ms
Wazid *et al.*[5]	$13T_h + 2T_{E_s} + T_f$	$5T_h + 4T_{E_s}$	$4T_h + 2T_{E_s}$	$22T_h + 8T_{E_s} + T_f$
	≈ 86.975 ms	≈ 37.3 ms	≈ 19.4 ms	≈ 143.68 ms
Gope *et al.* [44]	$8T_h$	$9T_h$	$6T_h$	$23T_h$
	≈ 4 ms	≈ 4.5 ms	≈ 3 ms	≈ 11.5 ms
Chang-Le[40]	$7T_h + 2T_m$	$9T_h$	$5T_h + 2T_m$	$21T_h + 4T_m$
	≈ 129.65 ms	≈ 4.5 ms	≈ 128.65 ms	≈ 262.8 ms

the use of PUF(·) in this authentication scheme, $\mathcal{A}$ cannot even impersonate already compromised smart devices. This is because of the nature of PUF(·), $\mathcal{A}$ cannot compute $\{R_d\}$ from $\{C_d, hd_d\}$, which is essential for generating the valid message $M_3 = \langle HQ_R, Q_d, Q_{R'_d}, Auth_d\rangle$. Thus, the proposed scheme is ''unconditionally secure against physical capture of smart devices''.

VI. COMPARATIVE STUDY

In this section, we preform a detailed comparative study of the proposed scheme in terms of ''security & functionality features, communication and computational overheads'' with other existing related schemes, such as the schemes proposed by Gope *et al.* [15], Zhou *et al.* [52], Wazid *et al.* [5] and Chang and Le [40]. For the scheme [40], we consider its ECC-based version as it is more secure than its basic version.

A. COMPUTATION COSTS COMPARISON

We use the notations T_{E_s}, T_m, T_f and T_h to denote the time needed for computing symmetric encryption/decryption, elliptic curve point (scalar) multiplication, fuzzy extractor operation and hash operation, respectively. Based on experimental results reported in [61] and [62], we have $T_{E_s} \approx 8.7$, $T_m \approx 63.075$, $T_f \approx T_m = 63.075$ and $T_h \approx 0.5$ milliseconds, respectively.

In the proposed scheme, during the login and authentication process, the user U, the *GWN* and the smart device *SD* need to perform $17T_h + T_f$, $8T_h$ and $6\ T_h + T_f$ operations, respectively. Thus, the total computation cost is $31T_h + 2T_f$, that requires approximately 141.65 ms. Table 2 summarizes the computational cost for the compared schemes. It is clear that the proposed scheme has a much lower computational overhead as compared to that for other schemes[2] with the exception of the schemes [44], [52]. However, both the schemes [44], [52] are two-factor authentication schemes with poor security & functionality features (see Table 4) and higher communication overhead (see Table 3).

[2]It should be noted that the scheme in [15], as presented by Gope *et al.*, assumes ideal PUFs. But, all other schemes account for noisy PUF/biometric for the sake of fairness. We have assumed that all PUFs and biometric are processed through corresponding fuzzy extractor. The values reported in Table 2 are account for use of fuzzy extractor.

TABLE 3. Communication costs comparison.

Scheme	No. of bytes	No. of messages
Our	256	3
Gope *et al.* [15]	280	6
Zhou *et al.* [52]	732	3
Wazid *et al.* [5]	324	4
Gope *et al.* [44]	275	4
Chang-Le [40]	284	4

B. COMMUNICATION COSTS COMPARISON

In order to compute the communication overheads of the different schemes, we assume that the hash digest (assuming SHA-1 hash algorithm [63]) and identity to be 160 bits each, random nonce and PUF challenge response pair each to be 128 bits long. For other schemes, we additionally assume the timestamp to be 32 bits long, ECC point to be 320 bits and a ciphertext block (assuming Advanced Encryption Standard (AES-128) symmetric encryption) to be 128 bits.

In the proposed scheme, three exchanged messages $M_1 = \langle DID_u, Q_{ug}, Q_{ud}, DID_d, Auth_u\rangle$, $M_2 = \langle C_{d_i}, Q_g, Auth_{R_d}, Auth_g\rangle$ and $M_3 = \langle HQ_R, Q_d, Q_{R'_d}, Auth_d\rangle$ require $(160 + 160 + 160 + 160 + 160) = 800$ bits, $(128 + 160 + 160 + 160) = 608$ bits and $(160 + 160 + 160 + 160) = 640$ bits during the time of the login and authentication phase. The total communication overhead of the proposed scheme is then $(800 + 608 + 640) = 2048$ bits, that is, 256 bytes. In Table 3, we summarize the communication costs as well as the number of messages exchanged for the proposed schemes and compared schemes. We can observe that the proposed scheme commends the lowest communication overhead as compared to that for the other schemes.

C. SECURITY AND FUNCTIONALITY FEATURES COMPARISON

Table 4 tabulates the ''security & functionality features'' of the proposed scheme and other existing schemes. It is apparent that the proposed scheme offers superior ''security and more functionality features'' as compared to other compared schemes. The schemes proposed in [15] and [5], while these are closed in terms of functionally & security features, the scheme [15] achieves these at much higher computation and communication overheads. Additionally, the scheme [15]

TABLE 4. Security & functionality features comparison.

Feature	Our	Gope *et al.* [15]	Zhou *et al.* [52]	Wazid *et al.* [5]	Gope *et al.* [44]	Chang-Le [40]
$\mathcal{FR}_1$	☑	☑	☑	☑	☑	☑
$\mathcal{FR}_2$	☑	☑	NA	☑	☒	☒
$\mathcal{FR}_3$	☑	☑	☑	☑	☑	☒
$\mathcal{FR}_4$	☑	☑	☑	☑	☒	☒
$\mathcal{FR}_5$	☑	☑	☑	☑	☑	☒
$\mathcal{FR}_6$	☑	☑	☑	☑	☑	☑
$\mathcal{FR}_7$	☑	☑	☑	☑	☑	☑
$\mathcal{FR}_8$	☑	☑	☑	☑	☑	☑
$\mathcal{FR}_9$	☑	☑	☒	☑	☑	☑
$\mathcal{FR}_{10}$	☑	☑	NA	☒	☒	☒
$\mathcal{FR}_{11}$	☑	☑	☑	☑	☒	☒
$\mathcal{FR}_{12}$	☑	☑	☒	☑	☑	☑
$\mathcal{FR}_{13}$	☑	☑	☒	☑	☑	☑
$\mathcal{FR}_{14}$	☑	☑	☑	☑	☑	☑
$\mathcal{FR}_{15}$	☑	☒	☒	☑	☒	☒
$\mathcal{FR}_{16}$	☑	☑	☑	☑	☑	☒
$\mathcal{FR}_{17}$	3	3	2	3	2	2
$\mathcal{FR}_{18}$	☑	☑	☑	☑	☑	☒
$\mathcal{FR}_{19}$	☑	☑	☑	☒	☑	☒
$\mathcal{FR}_{20}$	☑	☑	NA	☑	☑	☒

Note: ☑: "a scheme supports a feature or it is resilient against an attack"; ☒: "a scheme does not support a feature or it is not secure against an attack". NA: not applicable for the scheme
$\mathcal{FR}_1$: user anonymity; $\mathcal{FR}_2$: smart device anonymity; $\mathcal{FR}_3$: untraceability; $\mathcal{FR}_4$: resilience against offline password guessing attack; $\mathcal{FR}_5$: fast detection of erroneous inputs; $\mathcal{FR}_6$: mutual authentication; $\mathcal{FR}_7$: session key agreement; $\mathcal{FR}_8$: resilience against impersonation attack; $\mathcal{FR}_9$: resilience against smart device physical capture attack; $\mathcal{FR}_{10}$: resilience against compromised device impersonation attack; $\mathcal{FR}_{11}$: resilience against privileged insider attack; $\mathcal{FR}_{12}$: resilience against forward secrecy; $\mathcal{FR}_{13}$: resilience against replay attack; $\mathcal{FR}_{14}$: resilience against man-in-the-middle attack; $\mathcal{FR}_{15}$: resistant to ESL attack; $\mathcal{FR}_{16}$: resilience against stolen smart card attack; $\mathcal{FR}_{17}$: two/three factor authentication; $\mathcal{FR}_{18}$: local password and biometric change; $\mathcal{FR}_{19}$: no clock synchronization; $\mathcal{FR}_{20}$: dynamic smart device addition

fails to resist ESL attack under the CK adversary model. On the other hand, the scheme [5] requires clock synchronization and it provides no resolution for device impersonation attack.

VII. PRACTICAL IMPACT STUDY

In this section, through a simulation study using the widely accepted NS3 (3.28) simulator [14], we measure the impact of the proposed scheme on various network performance parameters, such as "network throughput (in bytes per second)", "end-to-end delay (in seconds)" and "packet loss rate (in number of lost packets per seconds)".

We ran several simulations, with different number of users and smart devices for each. We simulated a single fixed access point which operated as the gateway node. The smart devices was radially scattered along a ring (inner radius 20 m and outer radius 100 m) centered on the gateway node *GWN*. The users were permitted to move freely (and randomly) across a square area of side 150 m and centered on the *GWN*. All the nodes communicate over 2.4 GHz IEEE 802.11 wi-fi standard. Additional details about the simulations are tabulated in Table 5. Any details that are not explicitly mentioned mean that those are assumed with the default values as specified by NS3 (3.28) simulator.

A. IMPACT ON NETWORK THROUGHPUT

In Figure 9, we plot the network throughput along the y-axis and different scenarios are along with the x-axis. The throughput is calculated by the expression $(\nu_r \times |\rho|)/T_\delta$, where T_δ, ν_r and $|\rho|$ represent the total time in seconds,

TABLE 5. Simulation parameters.

Parameter	Description	
Platform	NS3(3.28) / Ubuntu 16.04 LTS	
Network scenarios	No. of users	No. of devices
1	8	20
2	10	20
3	8	35
4	10	35
5	8	50
6	10	50
Mobility	random (0-3 m/s)	
Simulation time	1200 sec	

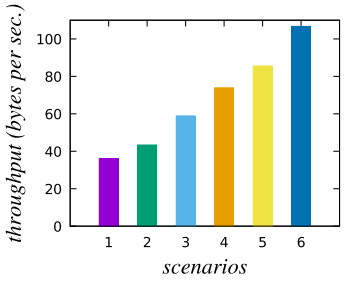

FIGURE 9. Throughput (bytes per second).

the number of received packets and its size, respectively. Form Figure 9, we observed that the network throughput increases with the number of messages exchanged.

B. IMPACT ON END-TO-END DELAY

In Figure 10, we plot the end-to-end delay (*eed*) along the y-axis and different scenarios along the x-axis. The *eed* is

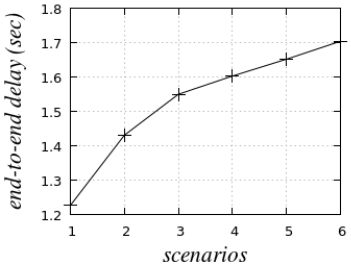

FIGURE 10. End-to-end delay in seconds.

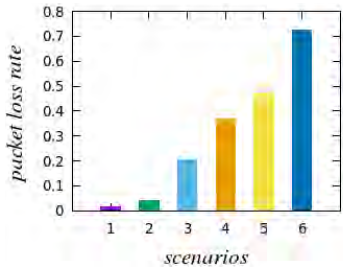

FIGURE 11. Packet loss rate.

formulated by the expression $\sum_{i=1}^{\nu_p}(T_{rcv_i} - T_{snd_i})/\nu_p$, where ν_p, T_{rcv_i} and T_{snd_i} represent the total number of packets, the time needed for receiving and sending a data packet i, respectively. We also observe that the end-to-end delay increases with the number of transmitted messages. This can be attributed to the increased number of messages contributing to the network congestion.

C. IMPACT ON PACKET LOSS RATE

In Figure 11, we plot the packet loss rate (plr) along the y-axis and different scenarios along the x-axis. The plr can be estimated by the expression $(\nu_t - \nu_r)/T_\delta$, where ν_t and ν_r represent the total number of packets transmitted and received, respectively, and T_δ represents the total time in seconds. As discussed previously this is the result of an increased number of messages contributing to the network congestion.

VIII. CONCLUSION

In this article, we discussed the necessity of designing a physically secure user authentication scheme for IoT environment. As a solution to the raised problem, we presented a novel physically secure lightweight anonymous user authentication protocol for IoT using physically unclonable functions. Through the rigorous analysis using the ROR model, formal security verification under AVISPA tool and informal security analysis, we demonstrated the security & functionality features of the proposed scheme. We also evaluated the practical impact of the proposed scheme using NS3 simulation and presented a comparative summary to demonstrate its potential to be deployed in a real-world environment.

ACKNOWLEDGMENTS

The authors thank the anonymous reviewers and the associate editor for their valuable feedback on the paper which helped us to improve its quality and presentation.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.
[2] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[3] 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.
[4] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.
[5] 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.
[6] 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.
[7] 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.
[8] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, "Secure remote user authenticated key establishment protocol for smart home environment," *IEEE Trans. Dependable Secure Comput.*, to be published. doi: 10.1109/TDSC.2017.2764083.
[9] 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, 2002, pp. 337–351.
[10] A. Dua, N. Kumar, A. K. Das, and W. Susilo, "Secure message communication protocol among vehicles in smart city," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 4359–4373, May 2018.
[11] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.
[12] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Public Key Cryptogr.*, Les Diablerets, Switzerland, vol. 3386, 2005, pp. 65–84.
[13] AVISPA. *Automated Validation of Internet Security Protocols and Applications*. Accessed: Mar. 2019. [Online]. Available: http://www.avispa-project.org/
[14] (2018). *NS-3.28*. Accessed: Mar. 2019. [Online]. Available: http://www.nsnam.org/ns-3-28/
[15] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, to be published. doi: 10.1109/TII.2019.2895030.
[16] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and implementation of PUF-based "Unclonable" RFID ICs for anti-counterfeiting and security applications," in *Proc. IEEE Int. Conf. RFID*, Las Vegas, NV, USA, Apr. 2008, pp. 58–64.
[17] M. Zhang, C. Shen, Z. Wu, and D. Zhang, "Dissipative filtering for switched fuzzy systems with missing measurements," *IEEE Trans. Cybern.*, to be published. doi: 10.1109/TCYB.2019.2908430.
[18] P. Gope, J. Lee, and T. Q. S. Quek, "Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 11, pp. 2831–2843, Nov. 2018.
[19] J.-P. Linnartz and P. Tuyls, "New shielding functions to enhance privacy and prevent misuse of biometric templates," in *Proc. Int. Conf. Audio-Video-Based Biometric Person Authentication*, Guildford, U.K., 2003, pp. 393–402.
[20] J. H. Cheon, J. Jeong, D. Kim, and J. Lee, "A reusable fuzzy extractor with practical storage size: Modifying canetti et al.'s construction," in *Proc. Australas. Conf. Inf. Secur. Privacy*, 2018, pp. 28–44.
[21] L. Lamport, "Password authentication with insecure communication," *Commun. ACM*, vol. 24, no. 11, pp. 770–772, Nov. 1981.
[22] Y. Sung-Ming and L. Kuo-Hong, "Shared authentication token secure against replay and weak key attacks," *Inf. Process. Lett.*, vol. 62, no. 2, pp. 77–80, Apr. 1997.
[23] J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," *IEEE Trans. Consum. Electron.*, vol. 50, no. 1, pp. 231–235, Feb. 2004.
[24] W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart cards," *Comput. Secur.*, vol. 18, no. 8, pp. 727–733, 1999.

[25] K. H. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput. (SUTC)*, Taichung, Taiwan, vol. 1, 2006, p. 8.

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

[27] H.-F. Huang, Y.-F. Chang, and C.-H. Liu, "Enhancement of two-factor user authentication in wireless sensor networks," in *Proc. 6th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.(IIH-MSP)*, Darmstadt, Germany, Oct. 2010, pp. 27–30.

[28] D. Nyang and M. K. Lee, "Improvement of das's two-factor authentication protocol in wireless sensor networks," *IACR Cryptol. ePrint Arch.*, vol. 2009, p. 631, 2009.

[29] P. Zhang, C. Lin, Y. Jiang, Y. Fan, and X. Shen, "A lightweight encryption scheme for network-coded mobile ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 9, pp. 2211–2221, Sep. 2014.

[30] R. Madhusudhan and R. C. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review," *Intell. Algorithms Data-Centric Sensor Netw.*, vol. 35, no. 4, pp. 1235–1248, Jul. 2012.

[31] 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.

[32] I. Alqassem, "Privacy and security requirements framework for the Internet of Things (IoT)," in *Proc. 36th Int. Conf. Softw. Eng.*, Hyderabad, India, May 2014, pp. 739–741.

[33] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, Aug. 2015.

[34] J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, "A gap analysis of Internet-of-Things platforms," *Comput. Commun.*, vol. 89, pp. 5–16, Sep. 2016.

[35] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to The Internet of Things," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1636–1675, 2nd Quart., 2018. doi: 10.1109/COMST.2018.2874978.

[36] J. Jeong, M. Y. Chung, and H. Choo, "Integrated OTP-based user authentication scheme using smart cards in home networks," in *Proc. 41st Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Waikoloa, HI, USA, Jan. 2008, p. 294.

[37] P. Hanumanthappa and S. Singh, "Privacy preserving and ownership authentication in ubiquitous computing devices using secure three way authentication," in *Proc. Int. Conf. Innov. Inf. Technol. (IIT)*, Abu Dhabi, United Arab Emirates, Mar. 2012, pp. 107–112.

[38] F. K. Santoso and N. C. H. Vun, "Securing IoT for smart home system," in *Proc. Int. Symp. Consum. Electron. (ISCE)*, Madrid, Spain, Jun. 2015, pp. 1–2.

[39] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Two-phase authentication protocol for wireless sensor networks in distributed IoT applications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 2728–2733.

[40] 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.

[41] A. K. Das, S. Kumari, V. Odelu, X. Li, F. Wu, and X. Huang, "Provably secure user authentication and key agreement scheme for wireless sensor networks," *Secur. Commun. Netw.*, vol. 9, no. 16, pp. 3670–3687, Nov. 2016.

[42] Y. Jie, J. Y. Pei, L. Jun, G. Yun, and X. Wei, "Smart home system based on IoT technologies," in *Proc. Int. Conf. Comput. Inf. Sci.*, Shiyang, China, Jun. 2013, pp. 1789–1791.

[43] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017.

[44] P. Gope and T. Hwang, "A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7124–7132, Nov. 2016.

[45] C. Shen, Y. Li, Y. Chen, X. Guan, and R. Maxion, "Performance analysis of multi-motion sensor behavior for active smartphone authentication," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 48–62, Jan. 2018.

[46] C. Shen, Y. Chen, and X. Guan, "Performance evaluation of implicit smartphones authentication via sensor-behavior analysis," *Inf. Sci.*, vols. 430–431, pp. 538–553, Mar. 2018.

[47] R. Amin, N. Kumar, G. Biswas, R. Iqbal, and V. Chang, "A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment," *Future Gener. Comput. Syst.*, vol. 78, pp. 1005–1019, Jan. 2018.

[48] S. Challa, A. K. Das, P. Gope, N. Kumar, F. Wu, and A. V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems," *Future Gener. Comput. Syst.*, to be published.

[49] W. Li, B. Li, Y. Zhao, P. Wang, and F. Wei, "Cryptanalysis and security enhancement of three authentication schemes in wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2018, 2018, Art. no. 8539674. doi: 10.1155/2018/8539674.

[50] P. K. Dhillon and S. Kalra, "Secure multi-factor remote user authentication scheme for Internet of Things environments," *Int. J. Commun. Syst.*, vol. 30, no. 16, p. e3323, Nov. 2017.

[51] Y.-H. Chuang, N.-W. Lo, C.-Y. Yang, and S.-W. Tang, "A lightweight continuous authentication protocol for the Internet of Things," *Sensors*, vol. 18, no. 4, p. 1104, Apr. 2018.

[52] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," *Future Gener. Comput. Syst.*, vol. 91, pp. 244–251, Feb. 2019.

[53] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication Protocols for Internet of Things: A Comprehensive Survey," *Secur. Commun. Netw.*, vol. 2017, Sep. 2017, Art. no. 6562953. doi: 10.1155/2017/6562953.

[54] D. Wang, D. He, P. Wang, and C.-H. Chu, "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 4, pp. 428–442, Jul./Aug. 2015.

[55] D. Wang, H. Cheng, P. Wang, X. Huang, and G. Jian, "Zipf's law in passwords," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2776–2791, Nov. 2017.

[56] S. Roy, A. K. Das, S. Chatterjee, N. Kumar, S. Chattopadhyay, and J. J. Rodrigues, "Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 457–468, Jan. 2019.

[57] 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.

[58] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1953–1966, Sep. 2015.

[59] D. von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project avispa," in *Proc. 3rd APPSEM Workshop (APPSEM)*, Frauenchiemsee, Germany, Sep. 2005, pp. 1–17.

[60] AVISPA. (2019). *SPAN, the Security Protocol ANimator for AVISPA*. Accessed: Mar. 2019. [Online]. Available: http://www.avispa-project.org/

[61] D. He, N. Kumar, M. Khan, and J.-H. Lee, "Anonymous two-factor authentication for consumer roaming service in global mobility networks," *IEEE Trans. Consum. Electron.*, vol. 59, no. 4, pp. 811–817, Nov. 2013.

[62] Q. Jiang, J. Ma, G. Li, and L. Yang, "An efficient ticket based authentication protocol with unlinkability for wireless access networks," *Wireless Pers. Commun.*, vol. 77, no. 2, pp. 1489–1506, 2014.

[63] (Apr. 1995). *Secure Hash Standard*. Accessed: Mar. 2019. [Online]. Available: http://www.umich.edu/~x509/ssleay/fip180/fip180-1.htm

SOUMYA BANERJEE received the M.Tech. degree in software engineering from Jadavpur University, Kolkata, India, where he is currently pursuing the Ph.D. degree in computer science and engineering. His current research interests include cryptography and network security. He has authored five papers in international journals and conferences in the above areas.

VANGA ODELU received the M.Tech. degree from IIT Kharagpur, and the Ph.D. degree in network security and cryptography from IIT Kharagpur, Kharagpur, in 2016. He is currently an Assistant Professor with the Birla Institute of Technology & Science Pilani, Pilani Hyderabad Campus, Hyderabad. He received Outstanding Potential for Excellence in Research and Academics (OPERA) by BITS Pilani. He was selected as an Outstanding Young Foreign Scholar Korean Research Fellowship (KRF-2017) by the Korean Government (Global competition among 15 positions). He has authored more than 45 papers in international journals and conferences. His research interests include cryptography, network security, hierarchical access control, attribute-based encryption, remote user authentication, security in cloud computing, and the Internet of Things. He is a Track Chair for the Intelligent Security Systems of Fifth International Conference on Mining Intelligence and Knowledge Exploration (MIKE 2017 & 2018). He is an Active Reviewer for several SCI-indexed journals including IEEE Transactions, Elsevier, Springer, and Technical Program Committee member for several reputed International Conferences.

ASHOK KUMAR DAS (M'17–SM'18) 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 an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His current research interests include cryptography, wireless sensor network security, hierarchical access control, security in vehicular ad hoc networks, smart grid, Internet of Things (IoT), Cyber-Physical Systems (CPS) and cloud computing, and remote user authentication. He has authored more than 190 papers in international journals and conferences in the above areas, including over 165 reputed journal papers. Some of his research findings are published in top cited journals, such as the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, the IEEE TRANSACTIONS ON SMART GRID, the IEEE INTERNET OF THINGS JOURNAL, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, the IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS (formerly the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE), the *IEEE Consumer Electronics Magazine*, IEEE ACCESS, the *IEEE Communications Magazine*, *Future Generation Computer Systems*, *Computers & Electrical Engineering*, *Computer Methods and Programs in Biomedicine*, *Computer Standards & Interfaces*, *Computer Networks*, *Expert Systems with Applications*, and the *Journal of Network and Computer Applications*. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He is on the Editorial Board of *KSII Transactions on Internet and Information Systems*, the *International Journal of Internet Technology*, and *Secured Transactions* (Inderscience), and *IET Communications*, is a Guest Editor of *Computers & Electrical Engineering* (Elsevier) for the special issue on Big data and IoT in e-healthcare and for *ICT Express* (Elsevier) for the special issue on Blockchain Technologies and Applications for 5G Enabled IoT, and has served as a Program Committee Member in many international conferences.

SAMIRAN CHATTOPADHYAY received the bachelor's and master's degrees in computer science and engineering from IIT Kharagpur, India, and the Ph.D. degree from Jadavpur University, Kolkata, India, where he is currently a Professor with the Department of Information Technology. He is having more than 25 years of teaching experience at Jadavpur University, four years of industry experience, and 12 years of technical consultancy in the reputed industry houses. He has authored more than 110 papers in international journals and conferences.

JOEL J. P. C. RODRIGUES (S'01–M'06–SM'06) is currently a Professor with the National Institute of Telecommunications (Inatel), Brazil; a Senior Researcher with the Instituto de Telecomunicações, Portugal; and a Visiting Professor with the Federal University of Piauí, Brazil. He is also the Leader of the Internet of Things Research Group (CNPq), the Director for Conference Development—IEEE ComSoc Board of Governors, the IEEE Distinguished Lecturer, Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the President of the scientific council at ParkUrbis Covilh Science and Technology Park, the Past Chair of the IEEE ComSoc Technical Committee on eHealth, the Past Chair of the IEEE ComSoc Technical Committee on Communications Software, Steering Committee Member of the IEEE Life Sciences Technical Community and Publications Co-Chair, and a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He has authored or coauthored more than 700 papers in refereed international journals and conferences, three books, and two patents. He is a member of the Internet Society, and a Senior Member of ACM. He received several Outstanding Leadership and Outstanding Service Awards by the IEEE Communications Society and several best papers awards. He is the Editor-in-Chief of the *International Journal of E-Health and Medical Communications* and an Editorial Board Member of several top journals.

YOUNGHO PARK (M'17) received the B.S., M.S., and Ph.D. degrees in electronic engineering from Kyungpook National University, Daegu, South Korea, in 1989, 1991, and 1995, respectively. From 1996 to 2008, he was a Professor with the School of Electronics and Electrical Engineering, Sangju National University, South Korea. From 2003 to 2004, he was a Visiting Scholar with the School of Electrical Engineering and Computer Science, Oregon State University, USA. He is currently a Professor with the School of Electronics Engineering, Kyungpook National University. His research interests include computer networks, multimedia, and information security.