PFLUA-DIoT: A Pairing Free Lightweight and Unlinkable User Access Control Scheme for Distributed IoT Environments

Shehzad Ashraf Chaudhry, Mohammad Sabzinejad Farash, Neeraj Kumar, *Senior Member, IEEE*, and Mohammed H. Alsharif

***Abstract*—The Internet of Things (IoT) connects enormous objects through various sensors to facilitate daily life by interconnecting the information space with the decision-makers. Security and privacy are, however, the main concerns in IoT due to the openness of communication channels and the unattended nature of common sensors. To provide security and privacy for sensors and users in IoT-based systems; in 2019, Zhou *et al.* proposed an unlinkable authentication scheme using bilinear pairings. However, the vulnerability of their scheme against sensor node impersonation attack as proved in this article renders the scheme of their work impractical and insecure. A pairing free lightweight and unlinkable authentication scheme for distributed IoT devices (PFLUA-DIoT) is then proposed in this article. The security of PFLUA-DIoT is proved using the formal method along with a discussion on its provision of security features. The performance and security comparisons show that PFLUA-DIoT provides known security features and provides better performance. Due to the avoidance of bilinear pairing-based expensive operations, PFLUA-DIoT completes authentication in less than half running time as compared with their and related schemes. Therefore, the PFLUA-DIoT can address the security and privacy issues of IoT, practically and efficiently.**

***Index Terms*—Device access control, device impersonation, forged message, IoT access.**

I. Introduction

THE Internet of Things (IoT) encompasses very large networks of homogenous and heterogeneous devices termed as things. The real-world entities can be managed through sensing devices deployed remotely and controlled centrally [1]. A large number of applications including eHealth, smart vehicular systems, smart grids, and smart cities, etc. are enhancing the quality of life through sensing devices. The sensing technologies can be deployed centrally, where users are connected with some intermediate device for gaining live sensing information; as well as distributively, where users are directly connected to the sensors and access the information on edge of a network [2]. In distributed networks, the communication between users and sensors is carried out through the open channel. The sensing information is typically used for decision making after evaluation and analysis. Forging of such information can have grave consequences as decisions are made on this information. Like traditional networks, the sensor networks are subject to traditional attacks and unlike many traditional networks, the battery operation and that too on low-powered sensors renders the security of these devices a more tedious task [3]–[5]. In past, some efforts were exerted to secure IoT-based systems [6]–[9]. However, all these were proved to suffer from one or other weaknesses. Turkanovic *et al.* [10] presented a hash-functions-based sensor access scheme without the mediation of the gateway. Nevertheless, Farash *et al.* [11] proved the weaknesses of the scheme [10] against impersonation and related attacks. The scheme of Farash *et al.* [11] was proved as insecure against some critical attacks including an impersonation by Amin *et al.* [12] in 2016. Amin *et al.* also presented an update scheme using only symmetric-key primitives. Another scheme proposed by Amin–Biswas [13] was proved as insecure against forgery and related attacks by Wu *et al.* [14]. Liu–Chang [15] also proposed a scheme to access medical sensors directly without the intervention of a gateway. In 2020, Ali *et al.* [16] showed that the scheme [15] can become prey to user secret key reveal and impersonation attacks. Li *et al.* [17] also exposed some weaknesses of the scheme of Liu–Chang. Another scheme using only symmetric key primitives was proposed by Dhillio–Kalra [18]. In 2018, Karati *et al.* [19] and Luo *et al.* [20] also presented two different scheme using bilinear pairings. Likewise, In 2019, Jia *et al.* [21] presented another pairing-based authentication scheme for IoT. Some other schemes were also presented by different researchers [22]–[28], some of these [22]–[26] were lacking one or the other security feature, and others [27], [28] were lacking the efficiency mainly due to heavy computation costs.

Manuscript received June 13, 2020; revised September 3, 2020; accepted October 26, 2020. Date of publication December 10, 2020; date of current version March 24, 2022. *(Corresponding author: Neeraj Kumar.)*

Shehzad Ashraf Chaudhry is with the Department of Computer Engineering, Faculty of Engineering, and Architecture, Istanbul Gelisim University, Istanbul 34310, Turkey (e-mail: ashraf.shehzad.ch@gmail.com).

Mohammad Sabzinejad Farash is with the Faculty of Mathematical Sciences and Computer, Kharazmi University, Tehran 15719-14911, Iran (e-mail: m.sabzinejad@gmail.com).

Neeraj Kumar is with the Department of CSED, Thapar Institute of Engineering and Technology, Punjab 147004, India and also with the School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, Uttarakhand and also with the Department of Computer Science and Information Engineering, Asia University, Taiwan and King Abdul Aziz University, Jeddah, Saudi Arabia (e-mail: neeraj.kumar@thapar.edu).

Mohammed H. Alsharif is with the Department of Electrical Engineering, College of Electronics and Information Engineering, Sejong University, Seoul 05006, Korea (e-mail: malsharif@sejong.ac.kr).

Digital Object Identifier 10.1109/JSYST.2020.3036425

A. Motivations

In 2019, Zhou *et al.* [29] proposed a user access to sensor scheme using ECC and bilinear pairing. They argued the efficiency and security of the scheme along with unlinkability. However, in this article, it is to show that the scheme of Zhou *et al.* [29] is impractical due to its weakness against sensor node impersonation attack. A pairing free lightweight and unlinkable user access to sensor scheme for distributed IoT devices (PFLUA-DIoT) is then proposed in this article. The structure of the remaining sections/subsections is as follows: Section I-B describes the adopted attack model. In Section II, we describe the working of the scheme of Zhou *et al.* [29], and the weakness of their scheme against sensor node impersonation attack is proved in Section III. The proposed PFLUA-DIoT is presented in Section IV. The security of the PFLUA-DIoT is analyzed formally in Section V-A, whereas discussion on important security feature provision is solicited in Section V-D. The security and performance comparisons are conducted in Section VI. The article is finally, concluded in Section VII.

B. Attack Model

Based on both Dolev–Yao (DY) [30] and Canetti–Krawczyk (CK) [31], the active attack model is considered in this article. The adopted attack model is very common and is used to analyze many protocols [32]–[40]. Following attacker ($\mathcal{A}$) capabilities are assumed in the adopted attack model.

1) $\mathcal{A}$ controls the public channel and as per his capabilities, $\mathcal{A}$ can listen, replay, jam, or send a modify message to any of the communicating parties (i.e., user U_i and/or sensor SN_j).
2) $\mathcal{A}$ has the capabilities to launch power analysis to expose parameters stored in stolen smart card or in the memory of the captured sensor.
3) The system users and sensors are not trusted, which means any communicating entity can try to impersonate on behalf of others.
4) The public parameters including identities and public keys of all the entities including the Trusted third party (TTP) are accessible to all other system and nonsystem entities.
5) Private keys of the participants including the TTP are safe and no adversary $\mathcal{A}$ is powerful enough to reveal the private key of any of the system entities.

II. Revisiting the Scheme of Zhou et al.

In this section, we revisit the scheme of Zhou *et al.* [29] designed to provide security through ECC and pairing-based authentication and session key establishment, specifically for distributed IoT applications.

A. Initialization

For initialization, the TTP selects an elliptic curve (EC) $E_p(\alpha, \beta)$ and a point P along with additive group G_1 over $E_p(\alpha, \beta)$, generated by P. Considering G_2 as a multiplicative group, the TTP selects $h, H, H_1 : \{0,1\}^* \rightarrow Z_q^*$ the three hash function, along with MAC as a message authentication code function. Moreover, TTP selects bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$. TTP then selects/computes the key pair $\{s_T \in z_q^*, Q_T = s_T P$ and announces $\{G_1, G_2, P, q, h, H, H_1, MAC, e, Q_T\}$ publicly and keeps s_T secret. During this phase, all the sensor nodes $SN_j : \{j = 1, 2, \ldots, m\}$ are also initialized each by selecting it's private key say s_j and computing and publicizing it's public key $Q_j = s_j P$.

B. Registration

This phase initiates independently by each user say $U_i : \{i = 1, 2, \ldots, n\}$ by selecting his identity, password pair $\{ID_i, PW_i\}$. U_i computes $RPW_i = h(PW_i, ID_i)$ and sends the pair $\{ID_i, RPW_i\}$ to TTP on a secure channel. TTP on receiving the $\{ID_i, RPW_i\}$ message, selects $k \in z_q^*$ and computes $Q_{i1} = kP,\ S_{i1} = s_T Q_{i1},\ pid_i = ID_i \oplus h(RPW_i, k)$, $f_i = s_T h(pid_i) + k$ and sends back $\{Q_{i1}, S_{i1}, f_i, pid_i\}$ to U_i. Once received, U_i computes $h(RPW_i, k) - ID_i \oplus pid_i$, $e_i = h(h(RPW_i, k), ID_i, PW_i)$ and embeds $\{f_i, pid_i, e_i\}$ in his smart card memory. U_i then selects his partial private key $s_{i2} \in z_q^*$ and computes $Q_{i2} = s_{i2} P$. Finally, U_i publicizes the pair $\{Q_{i1}, Q_{i2}\}$; whereas, partial private key pair $\{S_{i1}, s_{i2}\}$ is kept confidential.

C. Zhou et al.'s User Login and Authentication

For the execution of this phase, the user U_i initiates a login and authentication request. Following steps are executed in-sequence between the user U_i and sensor node SN_j:

ZLK 1: $\boldsymbol{U}_i \rightarrow\ SN_j :\ R_1 = \{E_i\}$

Initially, U_i enters $\{ID_i, PW_i\}$ pair and the smart device computes $h(RPW_i, k) = ID_i \oplus pid_i$, $e_i^{'} = h(h(RPW_i, k), ID_i, PW_i)$ and checks validity of $e_i^{'}$ by performing equality checking with the stored e_i, in case equality does not hold, the process stops. Otherwise, U_i selects $r_i \in Z_q^*$, computes $E_i = r_i Q_j$ and sends the request $R_1 = \{E_i\}$ to the node SN_j.

ZLK 2: $\boldsymbol{S}N_j \rightarrow\ U_i :\ R_2 = \{t_j, E_j, MAC_y(t_j)\}$

SN_j upon receiving R_1, selects $r_j \in Z_q^*$, computes $E_j = r_j P, F_j = r_j s_j^{-1} E_i = (x, y)$, generates t_j and further computes $MAC_y(t_j)$. SN_j further sends $R_2 = \{t_j, E_j, MAC_y(t_j)$ to U_i.

ZLK 3: $\boldsymbol{U}_i \rightarrow\ SN_j :\ R_3 = \{aid_i, rpid_i, \delta, t_i\}$

U_i, after receiving R_2 check freshness t_j's and on proven freshness, computes $F_i = r_i E_j = (x^{'}, y^{'})$. As next step, U_i checks $MAC_y(t_j) \stackrel{?}{=} MAC_{y^{'}}(t_j)$. On successful verification of $MAC_y(t_j)$, U_i computes $rpid_i = pid_i \oplus x^{'}$, $aid_i = h(ID_i, r_i) \oplus pid_i,\ W_i = e(S_{i1}, yQ_j)$ and then selects current t_i. U_i further computes $\delta = s_{i2} + f_i H(t_i, w_i, F_i)$, $sk = H_1(F_i, h(ID_i, r_i), t_i, t_j)$ and sends $R_3 = \{aid_i, rpid_i, \delta, t_i\}$ to SN_j.

SN_j after successful verification of t_i, computes $pid_i = rpid_i \oplus x, w_i^{'} = e(Q_{i1}, ys_j Q_T), h(ID_i, r_i) = aid_i \oplus pid_i$ and checks $\delta.P \stackrel{?}{=} Q_{i2} + H(t_i, w_i^{'}, F_j).(h(pid_i)Q_T + Q_{i1}$. SN_j in case of successful verification computes the session key $sk = H_1(F_i, h(ID_i, r_i), t_i, t_j)$.

III. Sensor Node Impersonation Attack on the Scheme of Zhou et al.

In this section, we explore the weakness of the scheme of Zhou *et al.* [29] to sensor node (SN) impersonation attack. For the simulation of the SN impersonation attack, we consider an adversary $\mathcal{A}$ with ordinary capabilities of just listening to the channel and have access to the public parameters as mentioned in the adopted attack model (Section I-B). Following is the simulation of the steps executed among the legal user U_i and the attacker $\mathcal{A}$ (pretending itself to be a legal SN say SN_j):

SNIA 1: $\boldsymbol{U}_i \rightarrow \; SN_j: \; R_1 = \{E_i\}$

Initially, U_i enters $\{ID_i, PW_i\}$ pair and the smart device computes $h(RPW_i, k) = ID_i \oplus pid_i$, $e_i^{'} = h(h(RPW_i, k), ID_i, PW_i)$ and checks validity of $e_i^{'}$ by performing equality checking with the stored e_i, in case equality does not hold, the process stops. Otherwise, U_i selects $r_i \in Z_q^*$ and computes

$$E_i = r_i Q_j. \quad (1)$$

U_i sends the request $R_1 = \{E_i\}$ to the node SN_j.

SNIA 2: $\boldsymbol{\mathcal{A} \rightarrow \; U_i: \; R_2 = t_j, E_j, MAC_y(t_j)}$

$\mathcal{A}$ intercepts the message, selects $r_j \in Z_q^*, t_j$ and then computes

$$E_j = Q_j \quad (2)$$

$$F_j = E_i = (x, y) \quad (3)$$

$$MAC_y(t_j). \quad (4)$$

$\mathcal{A}$ sends the reply $R_2 = \{t_j, E_j, MAC_y(t_j)\}$ to U_i

SNIA 3: $\boldsymbol{U}_i \rightarrow \; SN_j: \; R_3 = \{aid_i, rpid_i, \delta, t_i\}$

U_i, after receiving R_2 check freshness t_j's and on proven freshness, computes

$$F_i = r_i E_j = (x^{'}, y^{'}). \quad (5)$$

As next step, U_i checks

$$MAC_y(t_j) \stackrel{?}{=} MAC_{y'}(t_j). \quad (6)$$

On successful verification of $MAC_y(t_j)$, U_i selects t_i and computes

$$rpid_i = pid_i \oplus x^{'} \quad (7)$$

$$aid_i = h(ID_i, r_i) \oplus pid_i \quad (8)$$

$$w_i = e(S_{i1}, yQ_j) \quad (9)$$

$$\delta = s_{i2} + f_i H(t_i, w_i, F_i) \quad (10)$$

$$sk = H_1(F_i, h(ID_i, r_i), t_i, t_j). \quad (11)$$

SNIA 4: U_i further sends $R_3 = \{aid_i, rpid_i, \delta, t_i\}$ to SN_j.

$\mathcal{A}$ intercepts and computes

$$pid_i = rpid_i \oplus x \quad (12)$$

$$h(ID_i, r_i) = aid_i \oplus pid_i \quad (13)$$

$$sk = H_1(F_i, h(ID_i, r_i), t_i, t_j). \quad (14)$$

Proposition 1: The senor node SN_j in Zhou *et al.* [29] authentication scheme for distributed IoT devices can be impersonated by an adversary $\mathcal{A}$ using only the public parameters and with the capabilities to intercept the communication message sent by a legal user U_i. $\mathcal{A}$ is not only able to get it authenticated on behalf of SN_j but also can share a session key sk with U_i

Proof: U_i initiates the login request by computing and sending $R_1 = \{E_i\}$ to SN_j. $\mathcal{A}$ intercepts and computes $\{E_j, F_j, MAC_y(t_j)\}$ as per (2)–(4) and sends $R_2 = \{t_j, E_j, MAC_y(t_j)\}$ to U_i and after receiving R_2, U_i verifies freshness of t_j and computes F_i in (5). U_i further verifies $MAC_y(t_j) \stackrel{?}{=} MAC_{y'}(t_j)$ in (6). U_i finally, computes $rpid_i, aid_i, w_i, \delta$, and session key sk as per (7)–(11), respectively. U_i then sends $R_3 = \{aid_i, rpid_i, \delta, t_i\}$ to SN_j. The adversary $\mathcal{A}$ intercepts and computes $pid_i, h(ID_i, r_i), sk$ as given in (12)–(14). For a successful SN impersonation attack, $\mathcal{A}$ has to pass: 1) timestamp t_j freshness, as $\mathcal{A}$ generated fresh time stamp t_j, therefore this test is passed; 2) the test $(MAC_y(t_j) \stackrel{?}{=} MAC_{y'}(t_j))$ given in (6), where t_j is genuine and fresh, while $y^{'}$ is *y*-axis of the EC point F_i computed in (5). Therefore, the ability of the attacker to compute the same F_j in (3) determines the success and/or failure of impersonation attack. As attacker computes $E_j = Q_j$ in (2), $F_j = E_i = r_i Q_j$ in (3) and the same E_j is used to compute $F_i = r_i E_j = r_i Q_j$ in (5). Hence F_j computes by $\mathcal{A}$ and F_i computes by U_i are exactly the same. Therefore, $\mathcal{A}$ can pass this test on the fly and can get itself authenticated from U_i. The session key computed on both sides is also the same as: U_i computes $sk = H_1(F_i, h(ID_i, r_i), t_i, t_j)$ in (11), now $\mathcal{A}$ has computed true F_i and knows both timestamps $\{t_i, t_j\}$. Moreover, using x (x-coordinate of F_i) $\mathcal{A}$, computes $pid_i = rpid_i \oplus x$ through (12) and using pid_i computes $h(ID_i, r_i) = aid_i \oplus pid_i$ in (9). Therefore, the session key is computed by $\mathcal{A}$ in (14) is same as computed by U_i in (11). Hence, the adversary using just public parameters has successfully impersonated as a legal sensor node SN_j.

IV. PFLUA-DIoT: Proposed Scheme

The proposed pairing free lightweight unlinkable authentication scheme for distributed IoT (PFLUA-DIoT) is presented in this section. Following subsections provide a brief explanation of each of the corresponding phase of the PFLUA-DIoT which is also illustrated in Fig. 1.

A. PFLUA-DIoT: Initialization

For initialization, the TTP selects an EC $E_p(\alpha, \beta)$ and a point P and $h, H: \{0, 1\}^* \rightarrow Z_q^*$ the two hash functions, along with MAC as a message authentication code function. TTP then selects/computes the key pair $\{s_T \in z_q^*, Q_T = s_T P$ and announces $\{P, q, h, H, MAC, Q_T\}$ publicly and keeps s_T secret. During this phase, all the sensor nodes $SN_j: \{j = 1, 2 \ldots m\}$ are also initialized each by selecting it's private key say s_j and computing and publicizing it's public key $Q_j = s_j P$.

B. PFLUA-DIoT: Registration

This phase is initiated independently by each user say $U_i: \{i = 1, 2 \ldots n\}$ by selecting his identity, password

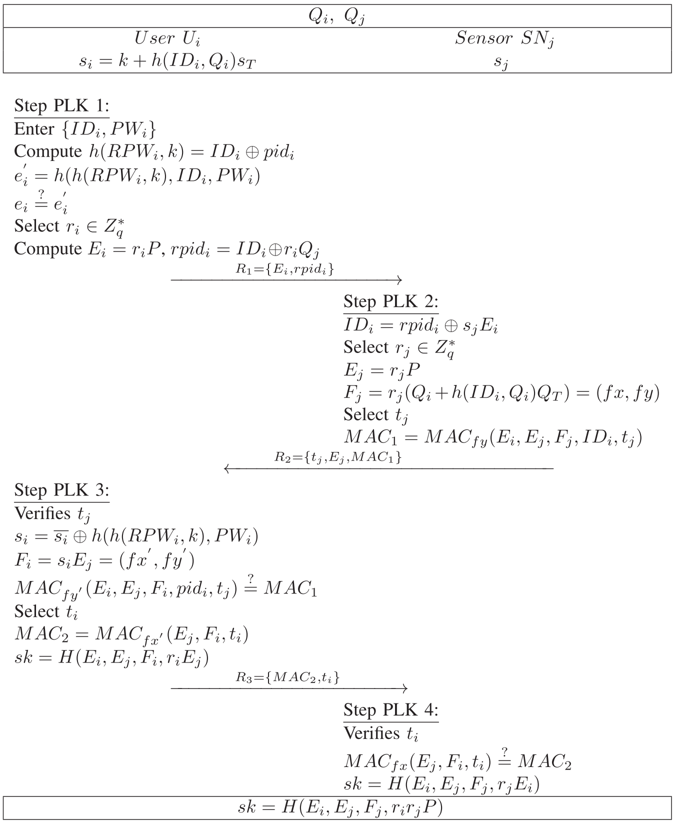
$Q_i,\ Q_j$
$User\ U_i$
$s_i = k + h(ID_i, Q_i)s_T$
$Sensor\ SN_j$
s_j
Step PLK 1:
Enter $\{ID_i, PW_i\}$
Compute $h(RPW_i, k) = ID_i \oplus pid_i$
$e_i^{'} = h(h(RPW_i, k), ID_i, PW_i)$
$e_i \overset{?}{=} e_i^{'}$
Select $r_i \in Z_q^*$
Compute $E_i = r_iP$, $rpid_i = ID_i \oplus r_iQ_j$
$R_1=\{E_i, rpid_i\}$
Step PLK 2:
$ID_i = rpid_i \oplus s_jE_i$
Select $r_j \in Z_q^*$
$E_j = r_jP$
$F_j = r_j(Q_i + h(ID_i, Q_i)Q_T) = (fx, fy)$
Select t_j
$MAC_1 = MAC_{fy}(E_i, E_j, F_j, ID_i, t_j)$
$R_2=\{t_j, E_j, MAC_1\}$
Step PLK 3:
Verifies t_j
$s_i = \overline{s_i} \oplus h(h(RPW_i, k), PW_i)$
$F_i = s_iE_j = (fx^{'}, fy^{'})$
$MAC_{fy'}(E_i, E_j, F_i, pid_i, t_j) \overset{?}{=} MAC_1$
Select t_i
$MAC_2 = MAC_{fx'}(E_j, F_i, t_i)$
$sk = H(E_i, E_j, F_i, r_iE_j)$
$R_3=\{MAC_2, t_i\}$
Step PLK 4:
Verifies t_i
$MAC_{fx}(E_j, F_i, t_i) \overset{?}{=} MAC_2$
$sk = H(E_i, E_j, F_j, r_jE_i)$
$sk = H(E_i, E_j, F_j, r_ir_jP)$

Fig. 1. Proposed PFLUA-DIoT.

pair $\{ID_i, PW_i\}$. U_i computes $RPW_i = h(PW_i, ID_i)$ and sends the pair $\{ID_i, RPW_i\}$ to TTP on a secure channel. TTP on receiving the $\{ID_i, RPW_i\}$ message, selects $k \in z_q^*$ and computes $Q_i = kP$, $pid_i = ID_i \oplus h(RPW_i, k)$, $s_i = h(ID_i)s_T + k$ and sends back $\{Q_i, s_i, pid_i\}$ to U_i. Once received, U_i computes $h(RPW_i, k) = ID_i \oplus pid_i$, $e_i = h(h(RPW_i, k), ID_i, PW_i)$, $\overline{s_i} = s_i \oplus h(h(RPW_i, k), PW_i)$ and embeds $\{e_i, \overline{s_i}\}$ in his smart card memory and removes s_i. Finally, U_i publicizes the Q_i; and the smart card contains $\{Q_i, \overline{s_i}, pid_i, e_i\}$.

C. PFLUA-DIoT: Login and Authentication

For the execution of this phase, the user U_i initiates a login and authentication request. Following steps as illustrated in Fig. 1 are executed in-sequence between the user U_i and sensor node SN_j:

PLK 1: $\boldsymbol{U}_i \rightarrow\ SN_j :\ R_1 = \{E_i, rpid_i\}$

Initially, U_i enters $\{ID_i, PW_i\}$ pair and the smart device computes $h(RPW_i, k) = ID_i \oplus pid_i$, $e_i^{'} = h(h(RPW_i, k), ID_i, PW_i)$ and checks validity of $e_i^{'}$ by performing equality checking with the stored e_i, in case equality does not hold, the process stops. Otherwise, U_i selects $r_i \in Z_q^*$, computes $E_i = r_iP$, $rpid_i = ID_i \oplus r_iQ_j$ and sends the request $R_1 = \{E_i, rpid_i\}$ to the node SN_j

PLK 2: $\boldsymbol{SN}_j \rightarrow\ U_i :\ R_2 = \{t_j, E_j, MAC_1\}$

SN_j upon receiving R_1, selects $r_j \in Z_q^*$, computes $ID_i = rpid_i \oplus s_jE_i$, $E_j = r_jP$, $F_j = r_j(Q_i + h(ID_i, Q_i)Q_T) = (fx, fy)$ generates t_j and further computes $MAC_1 = MAC_{fy}(E_i, E_j, F_j, ID_i, t_j)$. SN_j further sends $R_2 = \{t_j, E_j, MAC_1\}$ to U_i.

TABLE I
Notations Guide

Symbols	Representations
TTP, D_k	Trusted third party, k^{th} Device
x_{CA}, x_k	Private keys of CA and D_k
$E_p(\alpha, \beta), P$	Elliptic cure and a point on $E_p(\alpha, \beta)$
$Q_T = x_TP$	Private key of CA
$Q_k = x_k.P$	Private key of D_k
c_k, z_k	Certificate and signatures of D_k
$A_k, \mathcal{A}$	Certificate related parameter, Adversary
$\|\|, H(..)$	Concatenation and Hash functions

PLK 3: $\boldsymbol{U}_i \rightarrow\ SN_j :\ R_3 = \{MAC_2, t_i\}$

U_i, after receiving R_2 check freshness of t_j and on proven freshness, computes $s_i = \overline{s_i} \oplus h(h(RPW_i, k), PW_i)$ and $F_i = s_iE_j = (fx^{'}, fy^{'})$. As next step, U_i checks $MAC_{fy'}(E_i, E_j, F_i, ID_i, t_j) \overset{?}{=} MAC_1$. On successful verification of $MAC_y(t_j)$, U_i selects t_i, computes $MAC_2 = MAC_{fx'}(E_j, F_i, t_i)$ and $sk = H(E_i, E_j, F_i, r_iE_j)$ and sends $R_3 = \{MAC_2, t_i\}$ to SN_j.

PLK 4: SN_j after successful verification of t_i, checks $MAC_{fx}(E_j, F_i, t_i) \overset{?}{=} MAC_2$. SN_j in case of successful verification computes the session key $sk = H(E_i, E_j, F_j, r_jE_i)$.

V. Security Analysis

This section presents the security proof of the proposed PFLUA-DIoT formally under ROR model [41] as well as describes attack resilience of PFLUA-DIoT through a brief discussion on security feature provision.

A. Formal Security Analysis

The formal provable security analysis is solicited here. Following sections provide evidence of the robustness of the proposed scheme while combating several attacks:

B. Security Model

The formal security model and its proof are accomplished by customizing the [42]–[44] works in our proposed protocol environment. The PFULA-DIoT's formal security model [41] consists of two entities the attacker $\mathcal{A}$ and a responder $\mathcal{R}$. $\mathcal{A}$ contacts any instance of user or sensor, we denote both by a single instance E^{α}, where α represents αth instance of any of the user or sensor. Table II represents the queries by $\mathcal{A}$ and the corresponding response by $\mathcal{R}$.

We denote E_{UiSn} as the event that $\mathcal{A}$ impersonate U_i to SN_j by forging R_3; whereas, E_{SnUi} denotes the event where $\mathcal{A}$ can forge R_2 to impersonate as SN_j. We also consider an event E_{sc} as the event where $\mathcal{A}$ can overcome the semantic security of the proposed scheme.

TABLE II
QUERIES AND THEIR ANSWERS

$\boldsymbol{Setup}$: The Challenger $\mathcal{C}$ answers this query by returning the system parameters to $\mathcal{A}$.
$\boldsymbol{h(m_k)}$: The $\mathcal{C}$ stores a list L_{hs} and on querying $h(m_k)$, generates random $r_k \in Z_p^*$ and stores $\{m_k, r_k\}$ in L_{hs}, if m_k is a not found in L_{hs}. Otherwise, $\mathcal{C}$ picks the record $\{m_k, r_k\}$ from L_{hs} and in either cases returns r_k to $\mathcal{A}$.
$\boldsymbol{MAC(k, m_K)}$: The $\mathcal{C}$ stores a list L_{Mc} containing tuples of the form $MAC(k, m_K, M)$ and on querying $MAC(k, m_K)$, generates random $M \in Z_p^*$ and stores $\{k, m_k, M\}$ in L_{Mc}, if $\{k, m_K, M\}$ is a not found in L_{Mc}. Otherwise, $\mathcal{C}$ picks the record $\{k, m_K, M\}$ from L_{Mc} and in either cases returns M to $\mathcal{A}$.
$\boldsymbol{Send(E^\alpha, M_\alpha)}$ **:** Send represents an active attack and the $\mathcal{C}$ acts as per the original PFULA-DIoT, on this query and send the corresponding message to $\mathcal{A}$.
$\boldsymbol{Execute(U_i^x, SN_j^y)}$: This query represents the passive attack and the PFLUA-DIoT works as per the protocol specification and returns R_1, R_2 and R_3.
$\boldsymbol{Reveal(E^\alpha)}$ The $\mathcal{C}$ returns current session key SK shared among $\mathcal{A}$ and an entity E^α.
$\boldsymbol{Test(E^\alpha)}$ **:** $\mathcal{A}$ requests E^α for the key SK and E^α replies probabilistic-ally an outcome of a flipped unbiased coin c.

C. Provable Security

For proof purposes following theorem are argued as below:

Theorem 1: PFLUA-DIoT protocol achieves mutual authentication, if $Pr[E_{UiSn}]$ and $Pr[E_{SiUn}]$ both are negligible.

Proof: $\mathcal{A}$ is allowed to perform $Send(U_i, R_3)$. The forging may be successful if and only if the responder $\mathcal{R}$ gets $MAC_{fx}(E_j, F_i, t_i) \overset{?}{=} MAC_2$ verified. $\mathcal{R}$ can get a record from the maintained list L_{mc} with probability $1/q_{mc}$. Therefore, the probability for forging R_3 by $\mathcal{A}$ is $Pr[E_{UiSn}] = 1/q_{mc}$. Likewise, $\mathcal{A}$ is also allowed to perform $Send(SN_j, R_2)$. The forging may be successful if and only if the responder $\mathcal{R}$ gets $MAC_{fy'}(E_i, E_j, F_i, ID_i, t_j) \overset{?}{=} MAC_1$ is verified. In this way, $\mathcal{A}$ can generate two messages $\{t_j, E_j, MAC_1\}$ and $\{t_j^{'}, E_j^{'}, MAC_1^{'}\}$ and the $\mathcal{R}$ can compute $r_j - r_j^{'}P$ with probability $1/p$ and $\mathcal{R}$ extracts a record from the maintained list L_{mc} and the probability is $1/q_{mc}$. Therefore, the probability of this event is $Pr[E_{SnUi}] = 1/p.q_{mc}$. Hence, $\mathcal{A}$ cannot forge $U_i \rightarrow SN_j$ and $SN_j \rightarrow U_i$ security with nonnegligible probability.

Theorem 2: The PFLUA-DIoT is semantically secure.

Proof: On querying $Test$, $\mathcal{R}$ can get nonnegligible advantage ϵ to get the right session key (sk), this event is denoted by E_{key}. The probability for $\mathcal{A}$ to guess c in the $Test$ session is $\geq 1/2$, so it leads to $Pr[E_{key}] \geq \epsilon/2$. Now, let $E_{Test}^{U_i}$ and $E_{Test}^{SN_j}$ represents the events that U_i and SN_j are queried through $Test$. We have the following:

$$\begin{aligned}\epsilon/2 &\leq Pr[E_{key}] \\ &= Pr[E_{key} \wedge E_{Test}^{U_i}] + Pr[E_{key} \wedge E_{Test}^{SN_j} \wedge E_{UiSn}] \\ &\quad + Pr[E_{key} \wedge E_{Test}^{SN_j} \wedge \neg E_{UiSn}] \\ &\leq Pr[E_{key} \wedge E_{Test}^{U_i}] + Pr[E_{key} \wedge E_{Test}^{SN_j} \wedge \neg E_{UiSn}] \leq \\ &\geq \epsilon/2 - Pr[E_{UiSn}].\end{aligned}$$

Since $Pr[E_{Test}^{SN_j} \wedge \neg E_{UiSn} = E_{Test}^{U_i}$, therefore

$$Pr[sk = H(E_i, E_j, F_j, r_j E_i)] \geq \epsilon/4 - Pr[E_{UiSn}]/2. \quad (15)$$

Using Theorem 1, $Pr[E_{UiSn}]$ can be ignored. Therefore, the proposed PFLUA-DIoT is semantically secure.

D. Security Features Discussion

In this section we conduct an informal discussion of the security features of the proposed PFLUA-DIoT.

1) Anonymity and Unlinkability: In proposed PFLUA-DIoT, not only user identity $(rpid_i = ID_i \oplus r_i Q_j)$ is hidden in dynamic parameters based on freshly generated (session-specific) random variable r_i to provide dynamic pseudo-identity but all other parameters communicated through public channels are either built upon random nonces (r_i, r_j) or on current time stamps (t_i, t_j). Therefore, none of the parameters can expose any related information between two separate sessions of the access control process. Hence, neither U_i nor SN_j can be linked/tracked and PFLUA-DIoT provides anonymity and unlinkability.

2) Impersonation Attack: An attacker $\mathcal{A}$ may try to impersonate either the initiating user U_i or the responding sensor node SN_j and in order to be successful in his forgery attack, $\mathcal{A}$ has to create legal and valid initiating user messages $R_1 = \{E_i, rpid_i\}$ and $R_3 = \{MAC_2, t_i\}$ or it has to create valid and legal response message $R_2 = \{t_j, E_j, MAC_1\}$ on behalf of sensor node. $\mathcal{A}$ is considered to have all public parameters $\{Q_i, Q_j, ID_i, ID_j, P, q, h, H, MAC, Q_T\}$ including public identities of U_i and SN_j. As per the attackers capabilities mentioned in the attack model (Section I-B), $\mathcal{A}$ already have access to the parameters previously exchanged among the entities $R_1^{Pre} = \{E_i^{Pre}, rpid_i^{Pre}\}$, $R_2^{Pre} = \{t_j^{Pre}, E_j^{Pre}, MAC_1^{Pre}\}$ and $R_3^{Pre} = \{MAC_2^{Pre}, t_i^{Pre}\}$. As described in Section V-D1, all the messages exchanged on public channel are unlinked, so the attacker has no benefit of capturing exchanged data related to more than one sessions. Due to the involvement of two legal entities in access control phase of the PFLUA-DIoT, the attack simulation and resilience can be described in two separate ways.

1) $\mathcal{A}$ may try to impersonate on behalf of the initiating user say U_i, $\mathcal{A}$ can form an initial request by selecting some random r_a and by computing and sending $E_a = r_a P, rpid_a = ID_i \oplus r_a Q_j$ to the sensor node SN_j. However, $\mathcal{A}$ may never be able to compute $F_i = s_i E_j$ on reception of reply message $R_2 = \{t_j, E_j, MAC_1\}$ as it requires private key s_i of U_i and ultimately, $\mathcal{A}$ is unable to compute $MAC_2 = MAC_{fx'}(E_j, F_i, t_i)$ and $sk = H(E_i, E_j, F_i, r_i E_j)$ as both require the knowledge of F_i. The inability of computing F_i, MAC_2 and sk is translated into it's inability to create valid and legal response message $R_3 = \{MAC_2, t_i\}$. Hence, no attacker has any benefit of the public parameters for computation of valid request messages $\{R_1, R_3\}$ and the session key.
2) $\mathcal{A}$ may try to impersonate on behalf of a sensor node and for that, $\mathcal{A}$ may wait for access control request $R_1 = \{E_i, rpid_i\}$ from some user say U_i. $\mathcal{A}$ now needs to extract user identity ID_i and for exposing $\{ID_i = rpid_i \oplus s_j E_i\}$, the attacker needs s_j, the private key of the sensor. Therefore, $\mathcal{A}$ may not be able to compute $F_j = r_j(Q_i + h(ID_i, Q_i)Q_T) =$

(f_x, f_y), $MAC_1 = MAC_{fy}(E_i, E_j, F_j, ID_i, t_j)$ and as a result $\mathcal{A}$ is unable to compute session key $sk = H(E_i, E_j, F_j, r_jE_i)$.

Hence, our PFLUA-DIoT resists both user and sensor impersonation attacks.

3) Forward Secrecy: In the proposed PFLUA-DIoT, every session has it's own random variable (r_i and r_j) and timestamps (t_i and t_j). It is also argued in Section V-D1 that all sessions are unlinkable. Therefore, the compromise of any session key cannot effect previous or next session-specific shared keys.

4) Replay Attack: $\mathcal{A}$ may try to replay some message but can not be successful because of the session specific random nonces (r_i or r_j) and timestamps (t_i or t_j) are part of both messages $R_2 = \{t_j, E_j, MAC_1\}$ and $R_3 = \{MAC_2, t_i\}$; therefore, the replay will be detected at an early stage, and the attacker may never be able to generate any session key using the replay.

5) Stolen Smart Card: In the proposed PFLUA-DIoT, even the smart card is lost and $\mathcal{A}$ gets information $\{Q_i, \overline{s_i}, pid_i, e_i\}$ stored on smart card, $\mathcal{A}$ still needs user identity ID_i and password PW_i to computes $h(RPW_i, k)$. Moreover, the private key si of U_i can be extracted only by using $h(RPW_i, k)$ and PW_i, i.e., $s_i = \overline{s_i} \oplus h(h(RPW_i, k), PW_i)$ and this private key is used to compute $F_i = s_iE_j = (fx^{'}, fy^{'})$, which is used in formation of session key $sk = H(E_i, E_j, F_i, r_iE_j)$ as well as to prove authenticity through $MAC_2 = MAC_{fx'}(E_j, F_i, t_i)$ in-front of sensor node. Therefore, stolen smart card parameters are having no significance until $\mathcal{A}$ gets the private key of the user, which is accessible only when the attacker has access to user password PW_i and identity ID_i. Hence, the proposed PFLUA-DIoT resists stolen smart card attack.

6) Man in the Middle Attack: The proposed PFLUA-DIoT provides resistance against U_i impersonation as well as SN_j impersonation and as argued in Section V-D2, no adversary is capable enough to generate valid and legal access control messages exchanged over an insecure channel. Therefore, $\mathcal{A}$ cannot generate initiating or responding message. Moreover, it is also described in Section V-D4 that replay is detected immediately. Hence, the proposed PFLUA-DIoT resists man in the middle attack.

7) Sensor Capture Attack: In the proposed PFLUA-DIoT, each sensor node stores only it's own private key s_j. The private key s_j of a sensor node SN_j has no relationship with the private key say s_k of any other sensor node say SN_k, as all private keys are generated randomly. Therefore, the physical capturing of SN_j bears no weaknesses on part of other noncompromised sensor nodes, and the proposed PFLUA-DIoT resists physical sensor capture attack.

VI. Comparisons

This section presents the performance and security comparisons of the proposed PFLUA-DIoT with existing schemes proposed in [20]–[29]. The comparisons are made keeping in consideration the performance with respect to computation and running times along with the bits communicated to complete the authentication procedure, and the security features provided by the schemes. The comparisons are explained in the following sections.

TABLE III
Operations and the Corresponding Costs

Operation	Notation	Time (ms)
Bilinear-pair mapping	T_{Bpair}	≈ 5.811
Point multiplication	T_{Pmul}	≈ 2.226
Point addition	T_{Padd}	≈ 0.0288
Symmetric enc/dec-ryption	T_{Scrp}	≈ 0.0046
One-way hash function	T_{Ohsh}	≈ 0.0023
Fuzzy Extractor	T_{Fext}	≈ 2.226

A. Performance Comparisons

This section provides comparisons with respect to computation and running times (RT) in milliseconds (ms) along with the bits exchanged (communication cost) between the entities for completion of an authentication cycle. Table III presents the notations introduced along with their meanings and running time of each as per the experiment conducted [45] on a dual E2200 PC with Ubuntu OS along with PBC library, the RAM size, and processor speeds are 2 GB, 2.20 GHz, respectively.

To complete the authentication process, the user U_i in our PFLUA-DIoT scheme executes $3T_{Pmul}$ and $4T_{Ohsh}$; whereas, the sensor node SN_j executes $3T_{Pmul}$, $1T_{Padd}$, and $9T_{Ohsh}$ operations. Therefore, the total computation required for completion of the procedure is $6T_{Pmul} + 1T_{Padd} + 8T_{Ohsh}$, as per the experiment [45], the total running time for completion of 1 cycle of the authentication procedure in proposed PFLUA-DIoT is ≈ 13.4055 ms. The scheme of Zhou *et al.* [29] completes the process in ≈ 29.4772 ms, the other scheme [20]–[28] completes the same in ≈ 29.9312 ms, ≈ 33.0472 ms, ≈ 31.3644 ms, ≈ 22.775 ms, ≈ 33.4176 ms, ≈ 50.4595 ms, ≈ 41.6062 ms, ≈ 29.5106 ms, and ≈ 67.9155 ms, respectively. The communication cost of each of the scheme [20]–[29] is calculated using the bits exchanged between system entities and for this purpose, we keep $SHA - 1$ as oneway hash function with bit size 160, the standard sizes as recommended by NIST for modular exponentiation-based parameters and ECC-based parameters are considered as 1024 and 320 b, respectively. The size of identity and random numbers are assumed to be 160 b and the size of timestamp is fixed at 32 b. The user U_i and sensor node SN_J exchanges three messages for completion of the procedure in our PFLUA-DIoT scheme. The initial message $R_1 = \{E_i, rpid_i\}$ is sent from U_i to SN_j and total bits sent are $\{320 + 160\} = 480$; while the reply message $R_2 = \{t_j, E_j, MAC_1\}$ is sent from SN_j to U_i and total bits sent during transmission of R_2 are $\{32 + 320 + 160\} = 512$; the final response message $R_3 = \{MAC_2, t_i\}$ is sent from U_i to SN_j and it takes $\{160 + 32\} = 192$ b. Hence, total bits exchanged for PFLUA-DIoT scheme are $\{480 + 512 + 192\} = 1184$. The communication cost of the scheme of Zhou *et al.* [29] is 1344 b. The communication cost of the proposed PFLUA-DIoT is less than all the scheme presented in [20]–[22], [24]–[29], while it's slightly higher than the scheme put forward in [23].

The computation cost along with running time and communication costs of each of the compared scheme [20]–[29] is also given in Table IV, and it is very clear that the proposed scheme has the least computation cost, approximately less than half as

TABLE IV
PERFORMANCE COMPARISONS

	Computation Cost	RT (ms)	Bits
Our	$6T_{Pmul} + 1T_{Padd} + 9T_{Ohsh}$	≈ 13.4055	1184
[29]	$2T_{Bpair} + 8T_{Pmul} + 1T_{Padd} + 8T_{Ohsh}$	≈ 29.4772	1344
[22]	$18T_{Pmul} + 6T_{Padd} + 12T_{Ohsh}$	≈ 31.3644	3296
[21]	$3T_{Bpair} + 7T_{Pmul} + 14T_{Ohsh}$	≈ 33.0472	2560
[20]	$4T_{Bpair} + 3T_{Pmul} + 2T_{Padd} + 2T_{Ohsh}$	≈ 29.9312	3040
[27]	$2T_{Bpair} + 8T_{Pmul} + 2T_{Padd} + 10T_{Ohsh}$	≈ 29.5106	1312
[24]	$14T_{Pmul} + T_{fext} + 12T_{Ohsh}$	≈ 33.4176	2528
[25]	$6T_{Bpair} + 7T_{Pmul} + 5T_{Ohsh}$	≈ 50.4595	1632
[26]	$6T_{Bpair} + 3T_{Pmul} + 1T_{Scry} + 2T_{Ohsh}$	≈ 41.6062	3488
[23]	$2T_{Bpair} + 5T_{Pmul} + 10T_{Ohsh}$	≈ 22.775	1024
[28]	$9T_{Bpair} + 7T_{Pmul} + 15T_{Ohsh}$	≈ 67.9155	1600

TABLE V
SECURITY FEATURES

	$\mathcal{F}_{n1}$	$\mathcal{F}_{n2}$	$\mathcal{F}_{n3}$	$\mathcal{F}_{n4}$	$\mathcal{F}_{n5}$	$\mathcal{F}_{n6}$	$\mathcal{F}_{n7}$	$\mathcal{F}_{n8}$	$\mathcal{F}_{n9}$	$\mathcal{F}_{n10}$
Our	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[29]	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
[22]	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓
[21]	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
[20]	✓	✓	✓	✗	✗	✓	✗	✓	✓	✓
[27]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
[24]	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
[25]	✓	✓	✗	✓	✓	✗	✓	✓	✓	✓
[26]	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓
[23]	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
[28]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

compared with most of the schemes, which is due to avoidance of pairing-based operations for the completion of authentication.

B. Security Features

This section provides comparisons with respect to attack resistance and security features provided by proposed PFLUA-DIoT and the schemes proposed in [20]–[29]. The summary of the comparisons is given in Table V. According to Table V, the scheme of Zhou *et al.* [29] lacks resistance against SN_j impersonation attack as proved in Section III. The scheme of Das *et al.* [22] is weak against impersonation and man in middle attacks; the scheme of Jia *et al.* [21] and Luo *et al.* [20] do not provide direct authentication between two communicating entities rather both require an intermediate agent or trusted third party for completion of the process, in addition, the scheme of Luo *et al.*[20] does not provide mutual authentication and is weak against the leakage of ephemeral secrets attack. The scheme of Challa *et al.* [24] entails incorrectness and cannot provide authentication among two entities in case there is more than one user exist in the system. The scheme presented by Bakhtiari *et al.* [25] does not provide resistance against impersonation and man in middle attacks. The scheme of Li *et al.* [26] does not provide mutual authentication and the scheme of Wang–Zhang [23] lacks resistance against impersonation attack. Only the proposed PFLUA-DIoT and the schemes proposed by He *et al.* [27] and Xiong-Qin [28] provide all required security features and resistance against the known attacks. The proposed PFLUA-DIoT due to its low computation and communication costs is more suitable than both the schemes [27], [28].

VII. CONCLUSION

In this article, we proved that a very recent identity and bilinear pairing-based authentication scheme for IoT designed by Zhou *et al.* [29] is insecure against sensor node impersonation attack. We then put forward a pairing free lightweight and unlinkable authentication scheme for distributed IoT devices (PFLUA-DIoT), designed specifically to provide security and privacy alongside the performance efficiency in IoT-based systems. The security of the PFLUA-DIoT is demonstrated using the formal RoR model, in addition to the discussion of security features provision of PFLUA-DIoT. Moreover, the comparisons conducted in this article show that the proposed scheme provides all security features and has better performance than the related schemes. Specifically, it has reduced more than 50% computation cost as compared with Zhou *et al.* [29] and most of the related schemes by providing the identity-based authentication without the use of costly bilinear pairing operations. The low cost and better security properties render PFLUA-DIoT as the more practical and better security option for IoT-based systems.

REFERENCES

[1] A. Vilmos, C. Medaglia, and A. Moroni, “Vision and challenges for realising the internet of things,” *Hot Work Technol.*, vol. 35, no. 2, pp. 59–60, 2010.

[2] 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*, Apr. 2014, pp. 2728–2723.

[3] H. Hu, Y. Liu, H. Zhang, and R. Pan, “Optimal network defense strategy selection based on incomplete information evolutionary game,” *IEEE Access*, vol. 6, pp. 29806–29821, 2018.

[4] H. Hu, Y. Liu, H. Zhang, and Y. Zhang, “Security metric methods for network multistep attacks using AMC and big data correlation analysis,” *Secur. Commun. Netw.*, vol. 2018, pp. 1–14, Jun. 2018.

[5] A. K. Das, “Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks,” *Int. J. Netw. Secur.*, vol. 14, no. 1, pp. 1–21, 2012.

[6] J. Liu, Y. Xiao, and C. L. P. Chen, “Authentication and access control in the internet of things,” in *Proc. 32nd Int Conf. Distrib. Comput. Syst. Workshops*, vol. 34, no. 1, Jun. 2012, pp. 588–592.

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

[8] B. Ndibanje, H.-J. Lee, and S.-G. Lee, “Security analysis and improvements of authentication and access control in the internet of things,” *Sensors*, vol. 14, no. 8, pp. 14786–14805, 2014.

[9] M. L. Das, “Two-factor user authentication in wireless sensor networks,” *IEEE Trans. Wireless Commun.*, vol. 8, pp. 1086–1090, Mar. 2009.

[10] M. Turkanovic, B. Brumen, and M. Holbl, “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, 2014.

[11] M. S. Farash, M. Turkanovic, S. Kumari, and M. Holbl, “An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment,” *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016.

[12] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, “Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks,” *Comput. Netw.*, vol. 36, pp. 42–62, Jun. 2016.

[13] R. Amin and G. Biswas, “A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks,” *Ad Hoc Networks*, vol. 36, pp. 58–80, 2016.

[14] F. Wu *et al.*, “An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in iot deployment,” *J. Netw. Comput. Appl.*, vol. 89, pp. 72–85, 2017.

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

[16] Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. H. Islam, and D. Giri, "A robust authentication and access control protocol for securing wireless healthcare sensor networks," *J. Inf. Secur. Appl.*, vol. 52, 2020, Art. no. 102502.

[17] C.-T. Li, T.-Y. Wu, C.-L. Chen, C.-C. Lee, and C.-M. Chen, "An efficient user authentication and user anonymity scheme with provably security for iot-based medical care system," *Sensors*, vol. 17, no. 7, 2017, Art. no. 1482.

[18] 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, 2017.

[19] A. Karati, S. K. H. Islam, and M. Karuppiah, "Provably secure and lightweight certificateless signature scheme for IIoT environments," *IEEE Trans. Ind. Inform.*, vol. 14, pp. 3701–3711, Aug. 2018.

[20] M. Luo, Y. Luo, Y. Wan, and Z. Wang, "Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the iot," *Secur. Commun. Netw.*, vol. 2018, pp. 1–10, Aug. 2018.

[21] X. Jia, D. He, N. Kumar, and K.-K. R. Choo, "Authenticated key agreement scheme for fog-driven iot healthcare system," *Wireless Netw.*, vol. 25, no. 8, pp. 4737–4750, 2019.

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

[23] C. Wang and Y. Zhang, "New authentication scheme for wireless body area networks using the bilinear pairing," *J. Med*, vol. 39, no. 11, Sep. 2015.

[24] S. Challa *et al.*, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[25] S. Bakhtiari-Chehelcheshmeh and M. Hosseinzadeh, "A new certificateless and secure authentication scheme for ad hoc networks," *Wireless Pers. Commun.*, vol. 94, pp. 2833–2851, Jun. 2017.

[26] F. Li, Y. Han, and C. Jin, "Practical access control for sensor networks in the context of the internet of things," *Comput. Commun.*, vol. 89, pp. 154–164, Sep. 2016.

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

[28] H. Xiong and Z. Qin, "Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, pp. 1442–1455, Jul. 2015.

[29] Y. Zhou, T. Liu, F. Tang, and M. Tinashe, "An unlinkable authentication scheme for distributed iot application," *IEEE Access*, vol. 7, pp. 14757–14766, 2019.

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

[31] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, New York, NY, USA: Springer, 2001 pp. 453–474.

[32] M. N. Aman, M. H. Basheer, and B. Sikdar, "Data provenance for iot with light weight authentication and privacy preservation," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10441–10457, 2019.

[33] C. Chen, B. Xiang, Y. Liu, and K. Wang, "A secure authentication protocol for internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

[34] S. H. Islam, "A provably secure id-based mutual authentication and key agreement scheme for mobile multi-server environment without esl attack," *Wireless Pers. Commun.*, vol. 79, no. 3, pp. 1975–1991, 2014.

[35] S. A. Chaudhry, "Correcting PALK: Password-based anonymous lightweight key agreement framework for smart grid," *Int. J. Elect. Power & Energy Syst.*, vol. 125, 2021, Art. no. 106529.

[36] C.-M. Chen, K.-H. Wang, K.-H. Yeh, B. Xiang, and T.-Y. Wu, "Attacks and solutions on a three-party password-based authenticated key exchange protocol for wireless communications," *J. Ambient Intell. Humanized Comput.*, vol. 10, no. 8, pp. 3133–3142, 2019.

[37] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2411–2419, Sep. 2017.

[38] M. N. Aman, M. H. Basheer, and B. Sikdar, "Two-factor authentication for iot with location information," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3335–3351, Apr. 2019.

[39] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[40] S. A. Chaudhry, T. Shon, F. Al-Turjman, and M. H. Alsharif, "Correcting design flaws: An improved and cloud assisted key agreement scheme in cyber physical systems," *Comput. Commun.*, vol. 153, pp. 527–537, 2020.

[41] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *International Workshop on Public Key Cryptography*, New York, NY, USA: Springer, 2005, pp. 65–84.

[42] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Commun.*, vol. 10, no. 14, pp. 1795–1802, 2016.

[43] X. Li, F. Wu, S. Kumari, L. Xu, A. K. Sangaiah, and K.-K. R. Choo, "A provably secure and anonymous message authentication scheme for smart grids," *J. Parallel Distrib. Comput.*, vol. 132, pp. 242–249, 2019.

[44] K. Y. Choi, J. Y. Hwang, D. H. Lee, and I. S. Seo, "ID-based authenticated key agreement for low-power mobile devices," in *Australasian Conference on Information Security and Privacy*, New York, NY, USA: Springer, 2005, pp. 494–505.

[45] H. H. Kilinc and T. Yanik, "A survey of sip authentication and key agreement schemes," *IEEE Commun. Surv. Tut.*, vol. 16, no. 2, pp. 1005–1023, Oct.–Dec. 2013.

Shehzad Ashraf Chaudhry received the Ph.D. degree in computer science from the International Islamic University, Islamabad, Pakistan, in 2016.

He has authored over 100 scientific publications in different international journals and proceedings, including 80 in SCI/E journals. With an H-index of 25 and an I-10 index 51, his work has been cited over 2000 times. Some of his findings are published in top cited journals like the *ACM Transactions on Internet Technology* IEEE Internet of Things Journal, IEEE Transactions on Reliability, IEEE Systems Journal, IEEE Transactions on Industry Applications, Elsevier *Future Generation Computing Systems*, *International Journal of Electrical Power & Energy Systems, Computer Communications* etc.

Dr. Chaudhry was a recipient of the Gold Medal for achieving 4.0/4.0 CGPA in his master's and has received prestigious Research Productivity Award from PCST. Recently, he also received the Best Paper Award from International Conference on Forthcoming Networks and Sustainability in the IoT Era.

Mohammad Sabzinejad Farash received the B.Sc. degree in electronic engineering from Shahid Chamran College of Kerman, in 2006, the M.Sc. degree in communication engineering from AlHussein University, Amman, Jordan, in 2009 and the Ph.D. degree in cryptographic mathematics from Tarbiat Moallem University, Tehran, Iran, in 2013.

His research interests are security protocols and provable security models.

Neeraj Kumar (Senior Member, IEEE) received Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra (J&K), India, in 2009, and Postdoctoral fellowship from Coventry University, Coventry, U.K.

He has authored or coauthored more than 400 technical papers at top journals like IEEE Transactions on Industrial Informatics, IEEE Internet of Things Journal, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Intelligent Transportation Systems, etc.

Mohammed H. Alsharif received the Ph.D. degree in electrical engineering from the National University of Malaysia, in 2015, joined Sejong University, South Korea, in 2016, where he is currently working as an Assistant Professor with the Department of Electrical Engineering.

His current research interests include wireless communications and networks, including wireless communications, network information theory, the Internet of Things (IoT), green communication, energy-efficient wireless transmission techniques, wireless power transfer, and wireless energy harvesting