IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON RELIABILITY IN SENSOR-CLOUD SYSTEMS AND APPLICATIONS (SCSA)

Received June 28, 2020, accepted July 15, 2020, date of publication July 27, 2020, date of current version August 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3012121

A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems

SHEHZAD ASHRAF CHAUDHRY[1], KHALID YAHYA[2], FADI AL-TURJMAN[3,4], (Member, IEEE), AND MING-HOUR YANG[5], (Member, IEEE)

[1]Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, 34310 stanbul, Turkey
[2]Department of Mechatronics Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, 34310 stanbul, Turkey
[3]Department of Artificial Intelligence Engineering, Near East University, 99138 Nicosia, Turkey
[4]Research Center for AI and IoT, Near East University, 99138 Nicosia, Turkey
[5]Department of Information and Computer Engineering, Chung Yuan Christian University, Taoyuan City 32023, Taiwan

Corresponding author: Ming-Hour Yang (mhyang@cycu.edu.tw)

This work was supported by the Ministry of Science and Technology under Grant MOST 108-2221-E-033-016.

ABSTRACT Among other security concerns, the reliable device to device direct communication is an important research aspect in sensor cloud system application of Internet of things (IoT). The access control mechanism can ensure the reliability through secure communication among two IoT devices without mediation of intermediate agent. Mainly, it requires twofold strategy involving the authentication of each other and session key establishment. Quite recently, in 2019, Das *et al.* proposed a certificate based lightweight access control and key agreement scheme for IoT devices (LACKA-IoT) to ensure smooth and secure access control and claimed LACKA-IoT to withstand the several attacks. Specifically, it is claimed that LACKA-IoT can resist device impersonation and man in middle attacks. However, the proof in this article refutes their claim and it is shown here, that LACKA-IoT is insecure against both device impersonation and man in middle attacks. An adversary just by using public parameters and by listening the communication channel can impersonate any device. Moreover, the same can also launch successful man in middle attack using public parameters and listened messages from public channel. An improved protocol iLACKA-IoT is then proposed in the paper. The iLACKA-IoT provides resistance against various types of threats and provides the required level of security, for evidence both formal validation through random or real (ROR) model as well as the informal validation through discussion on attack resilience is provided. The iLACKA-IoT is not only better in security but also provides performance efficiency as compared with LACKA-IoT and related schemes.

INDEX TERMS Device access control, device impersonation, forged message, IoT access, reliability.

I. INTRODUCTION

Consisting of several interconnected things including both physical smart-devices like sensors, mobiles, road and aerial vehicles etc. and soft/virtual objects like electronic wallets, tickets etc., the internet of things facilitates the accumulation of data and the decision making using the accumulated data. The IoT encompasses a wide range of applications which has empowered the sharing of information between the physical and virtual things directly or through some interfaces provided by high computing infrastructures like cloud computing to augment the low capacity personal smart devices, all this is achieved via public internet [1]–[3]. Typical IoT application scenarios as illustrated in Fig 1 includes smart homes, smart vehicles, smart industry, smart healthcare etc. The large range of IoT based applications are mainly aimed at providing Quality of service (QoS) and enhancing the life quality, through employing smart and intelligent methods in all such applications of day to day routine and corporate life. The IoT should support the user requirements, while consuming low resources including finance, energy and time [4]. Despite all such benefits and enhancement of quality life, the IoT services are subject to various security threats and attacks including Denial of services (DoS), impersonation, privacy invasion, replaying and IoT network disruption, the distributed and vendor specified data format and huge data involved can also play negative role for forensics [1]. To counter these threats and to ensure the availability and

The associate editor coordinating the review of this manuscript and approving it for publication was A. Taufiq Asyhari.

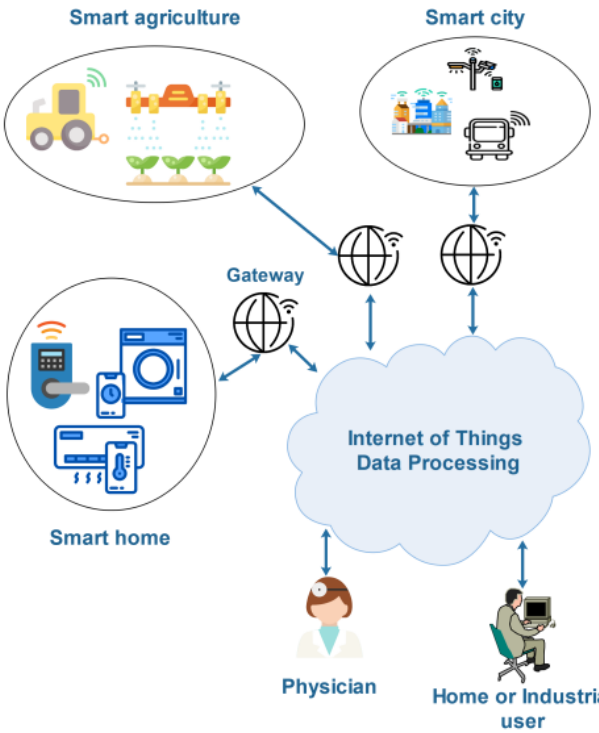

FIGURE 1. IoT Application domain example.

integrity of services along with privacy provision, the tailored IoT authentication methods are necessary [5]. Various authentication schemes were proposed to secure IoT and related systems [6]–[21]. However, many such schemes were insecure or inefficient. In 2016 Li *et al.* [7] proposed an access control protocol for IoT based sensor networks using pairing based operations powered with elliptic curve cryptography (ECC). Due to the usage of pairing operation, the scheme completes access control cycle using comparatively high computation power. Moreover, later it was proved as insecure against some related attacks. Likewise, in 2017, Challa *et al.* [8] proposed a purely ECC based scheme for access control for IoT based systems. However, Chaudhry *et al.* [22] argued that the scheme of Challa *et al.* entails correctness issues and cannot complete operation normally. Challa *et al.* proposed another scheme [20], which was suggested as weak against many attacks by Ali *et al.* [23]. In 2018, Luo *et al.* [11] presented their designed scheme for access control in sensor networks. In 2019, Jia *et al.* [12] also proposed a new IoT authentication scheme using pairing and ECC. Despite high consumption of computation power, both of these [11], [12] do not provide direct device to device (D2D) authentication. Additionally, the scheme of Luo *et al.* [11] entails some other insecurities [13]. Another scheme of securing industrial IoT was presented by Das *et al.* [14] in 2019. However, Hussain *et al.* [24] in their comments suggested some critical weaknesses in their scheme [14]. Another scheme for secure data collection was proposed in [25], in addition to a recent scheme for securing smart grid based communication [26].

A. MOTIVATION AND CONTRIBUTIONS

Very recently, Das *et al.* [13] proposed another D2D access control scheme purely based on ECC and symmetric key functions. Das *et al.* emphasized two main aspects for access control 1) device authentication, to provide legitimate access control between the neighboring devices, and 2) key agreement, which is the result of successful authentication and can be used for exchange of data between the authenticated devices. Das *et al.* claimed the scheme [13] to provide all required security features and resistance against known attacks. Specifically, it was claimed by Das *et al.* that the scheme presented in [13] is secure against device impersonation and man in middle attacks. The in-depth analysis in subsequent sections, however, nullifies their claim. We show that the scheme of Das *et al.* is insecure against device impersonation and man in middle attacks. We then proposed an improved scheme to mitigate the insecurities and to provide computational and communication efficiencies. The proposed scheme is free of any pairing based expensive operations and provides required security level and performance. Rest of the paper is organized as follows: The notation guide is presented in Table 1. The adopted threat model is presented in Subsection I-B. Section II provides the revisit of the scheme of Das *et al.*, while its' weaknesses are shown in Section III. The proposed iLACKA-IoT is presented in Section IV. The formal and informal security analysis of the proposed iLACKA-IoT is conducted in Section V. The performance and security comparisons are solicited in Section VI. Finally, Section VII concludes the paper.

TABLE 1. Notations guide.

Symbols	Representations
CA, D_k	Certificate Authority, 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 $E_p(\alpha, \beta)$
$Q_{CA} = x_{CA}.P$	Private key of CA
$Q_k = x_k.P$	Private key of device D_k
c_k, z_k	Certificate and signatures of D_k
$A_k, \mathcal{A}$	Certificate related parameter, Adversary
B_{ij}, K_{ij}	Dynamic parameters related to Session key
$\|\|, H(..)$	Concatenation and Hash functions
SKV_{ij}	Session key Verification parameter
$D_i \rightarrow D_j : Msg_x$	x^{th} Message sent from D_i to D_j
$\stackrel{?}{=}$	Relational Equality Checking

B. THREAT MODEL

The common threat model based on Dolev-Yao and Canetti-Krawczyk is adopted in this paper [27]–[34]. As per the adopted threat model, the adversary $\mathcal{A}$ has following capabilities:

1) The $\mathcal{A}$ has control over insecure channel being used among the participants for data exchange and $\mathcal{A}$ can eavesdrop, delete, replay or alter any data during transmission. $\mathcal{A}$ can also forge and transmit a message to any device pretending itself as another device of the system.

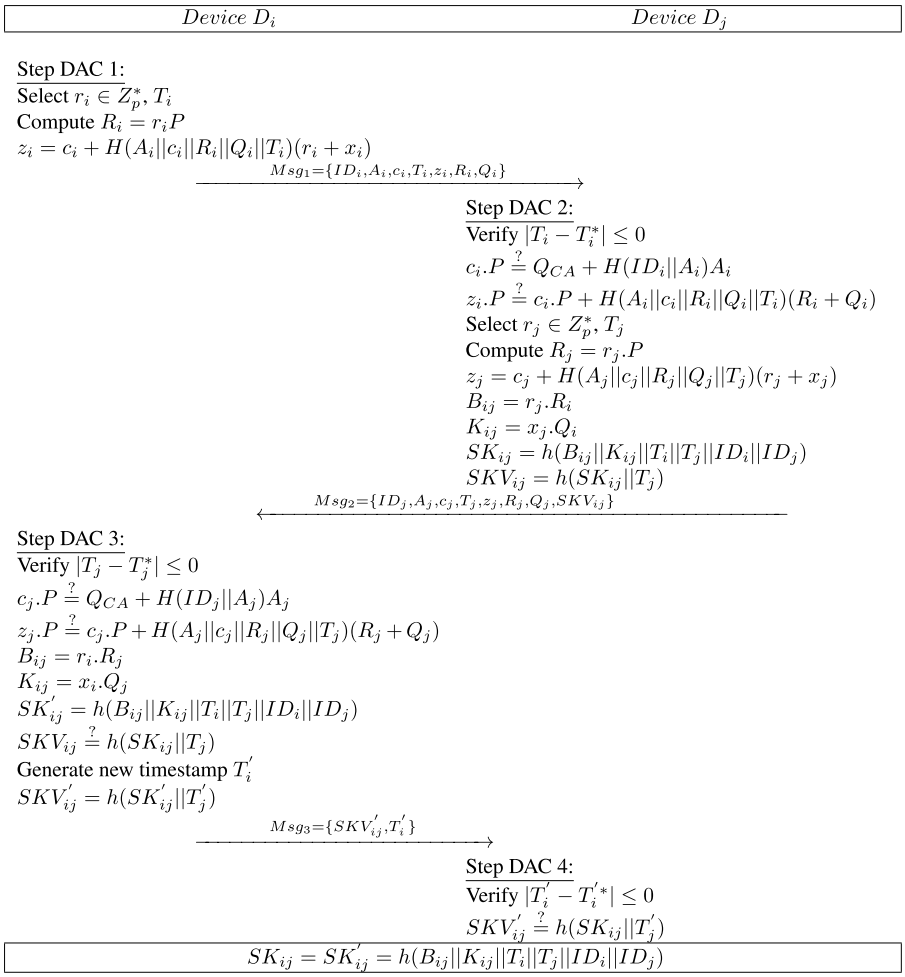

FIGURE 2. Das *et al.*'s device access method.

2) $\mathcal{A}$ can expose the parameters stored on a physically captured device using power analysis.
3) $\mathcal{A}$ can be an insider (a curious device) or an external entity.
4) The public system parameters including public keys and identities of all the system entities (certificate authority and communicating devices) are accessible to insiders and outsiders.
5) The private key of the certificate authority (CA) is safe and $\mathcal{A}$ does not have capabilities to expose the private key of the CA.

II. DEVICE ACCESS CONTROL SCHEME OF DAS *et al.*

In this section, the device access control (DAC) scheme of Das *et al.* is revisited. The DAC mainly involves two types of entities: the certificate authority (CA) which governs the registration process by assigning public and private key pair to each device along with related device specific certificate. After registration, two registered IoT devices can communicate directly through DAC phase. The subsequent subsections provide the brief review of each phase of Das *et al.*'s scheme:

A. SYSTEM SETUP

For system setup, the CA selects non singular Elliptic Curve (EC) $E_p(\alpha, \beta)$ and a point P over EC. The CA then selects its private/public key pair $\{x_{CA} \in Z_p^*, Q_{CA} = x_{CA}.P\}$. CA also selects a oneway $H(.)$ function. Finally, CA publishes $\{E_p(\alpha, \beta), P, Q_{CA}, H(.)\}$ and keeps x_{CA} secret.

B. DEVICE REGISTRATION PHASE

For registration purposes, CA selects an identity ID_k for each device $\{D_k|k = 1, 2 \ldots n\}$. The CA then selects private key x_k and computes public key $Q_k = x_k.P$ for D_k. CA generates l_k randomly and computes $A_k = (x_k + l_k).P$ and certificate $c_k = x_{CA} + (x_k + l_k)H(ID_k||A_k)$. Finally CA stores $\{ID_k, A_k, c_k, x_k, Q_k\}$ along with public parameters of the system $\{E_p(\alpha, \beta), P, Q_{CA}, H(.)\}$ on the memory of device D_k.

C. DAS et al.'s DEVICE ACCESS CONTROL

By executing device access control phase, a registered device can access the data/information stored/collected in another device. For granting access both devices should authenticate each other. This phase as shown in Fig. 2 is initiated by an

IoT device D_i, when it needs to communicate with another device D_j. The access control phase completes by execution of following steps between both devices i.e. D_i and D_j:

DAC 1: $\boldsymbol{D_i \rightarrow D_j : \{Msg_1\}}$

Initially, D_i construct an access control request and for this D_i selects $r_i \in Z_p^*$ and timestamp T_i. D_i further computes $R_i = r_iP, z_i = c_i + H(A_i||c_i||R_i||Q_i||T_i)(r_i + x_i)$ and sends $Msg_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$ to D_j.

DAC 2: $\boldsymbol{D_j \rightarrow D_i : \{Msg_2\}}$

On receiving Msg_1, D_j first verifies the freshness of time stamp through $|T_i - T_i^*| \leq 0$, where T_i^* denotes the receiving timestamp on D_j side. The D_j on success scenario verifies: 1) $c_i.P \stackrel{?}{=} Q_{CA} + H(ID_i||A_i)A_i$ and 2) $z_i.P \stackrel{?}{=} c_i.P + H(A_i||c_i||R_i||Q_i||T_i)(R_i + Q_i)$, terminates the access control request if both or any of 1 or 2 does not hold. Otherwise, D_j selects random nonce and current timestamp pair $\{r_j \in Z_p^*, T_j\}$ and computes $R_j = r_j.P, z_j = c_j + H(A_j||c_j||R_j||Q_j||T_j)(r_j + x_j)$, $B_{ij} = r_j.R_i$, $K_{ij} = x_j.Q_i$ along with session key $SK_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ and its' verifier $SKV_{ij} = h(SK_{ij}||T_j)$. D_j at last sends $Msg_2 = \{ID_j, A_j, c_j, T_j, z_j, R_j, Q_j, SKV_{ij}\}$ to D_i.

DAC 3: $\boldsymbol{D_i \rightarrow D_j : \{Msg_3\}}$

On receiving Msg_2, D_i first verifies the freshness of time stamp through $|T_j - T_j^*| \leq 0$, where T_j^* denotes the receiving timestamp on D_i side. The D_i on success scenario verifies: 1) $c_j.P \stackrel{?}{=} Q_{CA} + H(ID_j||A_j)A_j$ and 2) $z_j.P \stackrel{?}{=} c_j.P + H(A_j||c_j||R_j||Q_j||T_j)(R_j + Q_j)$, terminates the access control request if both or any of 1 or 2 does not hold. Otherwise, D_i computes $B_{ij} = r_i.R_j$, $K_{ij} = x_i.Q_j$ and session key $SK'_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$. D_i then checks the validity of SK'_{ij} through $SKV_{ij} \stackrel{?}{=} h(SK_{ij}||T_j)$. If verified successfully, D_i generate new timestamp T'_i and computes its' own key verifier $SKV'_{ij} = h(SK'_{ij}||T'_j)$ and sends $Msg_3 = \{SKV'_{ij}\}$ to D_j.

DAC 4: On receiving Msg_3, D_j first verifies the freshness of time stamp through $|T'_i - T'^*_i| \leq 0$, where T'^*_i denotes the receiving timestamp on D_j side. The D_j on success verifies $SKV'_{ij} \stackrel{?}{=} h(SK_{ij}||T'_j)$. Upon success D_j considers D_i authenticated with $SK_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ as the session key shared among the peer.

III. WEAKNESSES OF DAS *et al.*'s SCHEME

This section explores some of the weaknesses of Das *et al.*'s device access scheme. In forthcoming subsections, it is to prove that any attacker (insider or outsider) with capabilities to listen and transmit a message, by using only the public parameters can easily impersonate himself as any registered device.

A. DEVICE IMPERSONATION ATTACK

Consider an ordinary attacker $\mathcal{A}$ (insider or outsider), wants to impersonate and share a session key on behalf of a registered device D_k, where D_k can be the initiating or the responding device. For simplicity, we consider D_k as the initiating device. $\mathcal{A}$ waits for D_k to initiate an access control request by sending $Msg_1 = \{ID_k, A_k, c_k, T_k, z_k, R_k, Q_k\}$ to the responding device D_s. $\mathcal{A}$ intercepts the message and stores $\{ID_k, A_k, c_k\}$ in it's memory. Now, using the stored parameters, $\mathcal{A}$ can impersonate as himself as D_k and can share session key with any-other device of the system. The attack can be simulated as follows:

DDIA 1: $\mathcal{A}$ picks x_a as fake private key and computes $Q_a = x_a.P$ as fake public key.

DDIA 2: $\mathcal{A}$ selects $r_a \in Z_p^*$ randomly and generates current time stamp T_a. $\mathcal{A}$ now computes $R_a = r_aP$ and

$$z_a = c_k + H(A_k||c_k||R_a||Q_a||T_a)(r_a + x_a) \quad (1)$$

$\mathcal{A}$ sends $Msg_{a1} = \{ID_k, A_k, c_k, T_a, z_a, R_a, Q_a\}$ to the responding device D_s.

DDIA 3: Upon receiving Msg_{a1}, D_s verifies freshness of the message through comparing the received time stamp T_a with current timestamp T_a^*, as T_a is freshly picked, so this freshness holds.

DDIA 4: Now, D_s checks following equalities:

$$c_k.P \stackrel{?}{=} Q_{CA} + H(ID_k||A_k)A_k \quad (2)$$

$$z_a.P \stackrel{?}{=} c_k.P + H(A_k||c_k||R_a||Q_a||T_a)(R_a + Q_a) \quad (3)$$

DDIA 5: If both Eqs. 2 and 3 hold, D_s considers the initiating party as legitimate D_k and proceeds further by selecting $r_s \in Z_p^*$ randomly and then generates fresh T_s to compute $R_s = r_s.P$, $z_s = c_s + H(A_s||c_s||R_s||Q_s||T_s)(r_s + x_s)$, $B_{ks} = r_s.R_a$, $K_{ks} = x_s.Q_a$, $SK_{ks} = h(B_{ks}||K_{ks}||T_a||T_s||ID_k||ID_s)$ and $SKV_{ks} = h(SK_{ks}||T_s)$. D_s now sends $Msg_2 = \{ID_s, A_s, c_s, T_s, z_s, R_s, Q_s, SKV_{ks}\}$ to D_k.

DDIA 6: $\mathcal{A}$ intercepts the message verifies $c_s.P \stackrel{?}{=} Q_{CA} + H(ID_s||A_s)A_s$ and $z_s.P \stackrel{?}{=} c_s.P + H(A_s||c_s||R_s||Q_s||T_s)(R_s + Q_s)$ after checking freshness of the time stamp and then computes $B_{ks} = r_k.R_s$, $K_{ks} = x_k.Q_s$, $SK'_{ks} = h(B_{ks}||K_{ks}||T_k||T_s||ID_k||ID_s)$, $SKV_{ks} \stackrel{?}{=} h(SK_{ks}||T_s)$. $\mathcal{A}$ now generate new timestamp T'_k and computes $SKV'_{ks} = h(SK'_{ks}||T'_s)$. At last, $\mathcal{A}$ sends $Msg_3 = \{SKV'_{ks}\}$ to D_s.

DDIA 7: D_s receives Msg_3 and verifies timestamp freshness as well as following equality:

$$SKV'_{ij} \stackrel{?}{=} h(SK_{ij}||T'_j) \quad (4)$$

Proposition 1: In the device access control system of Das *et al.*, an attacker $\mathcal{A}$ by using public parameters and listening to the communication channel can easily authenticate himself as a legitimate device D_k from a device D_s and can share a session key with D_s.

Proof 1: $\mathcal{A}$ computes and sends $Msg_{a1} = \{ID_k, A_k, c_k, T_a, z_a, R_a, Q_a\}$ to D_s, and D_s on reception of the message authenticates $\mathcal{A}$ on behalf of D_k subject to timestamp freshness and the verification of equalities shown in Eqs. 2 and 3. As the timestamp T_a is freshly generated by $\mathcal{A}$, so $\mathcal{A}$ passes

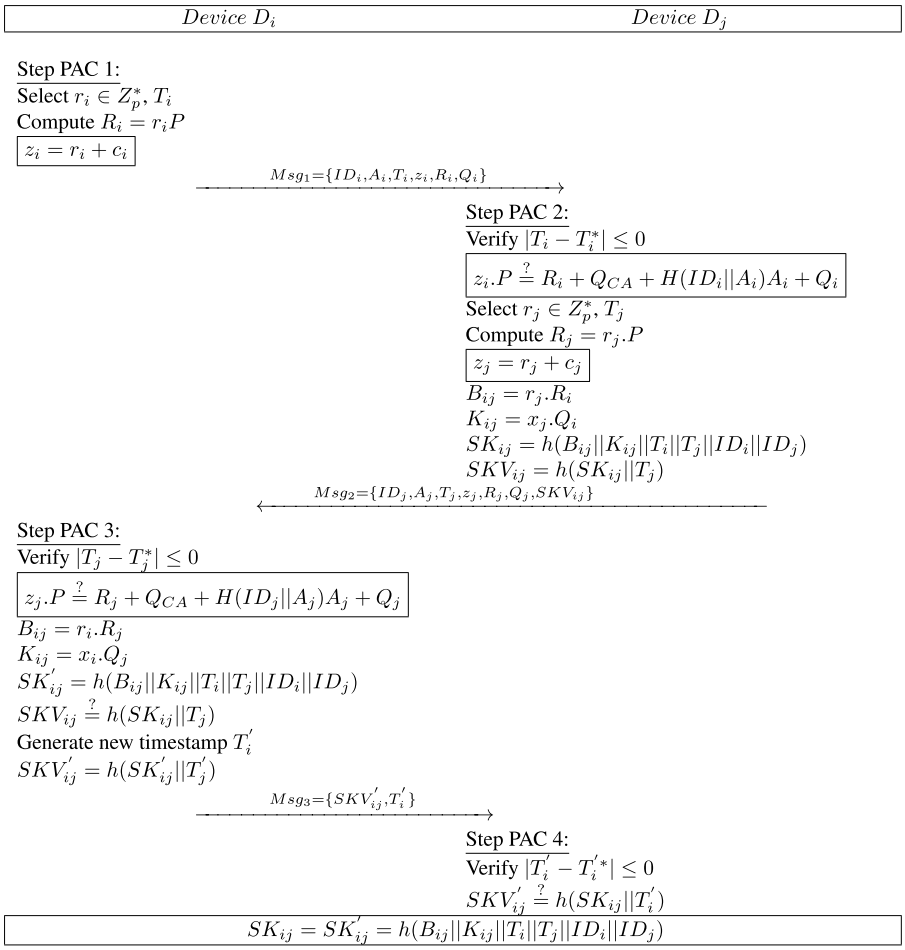

FIGURE 3. iLACKA-IoT device access method.

this test. Moreover, $\mathcal{A}$ used the original certificate c_k and A_k along with identity ID_k, intercepted in some previous session from the public channel, therefor Eq. 2 ($c_k.P \stackrel{?}{=} Q_{CA} + H(ID_k||A_k)A_k$) also holds. $\mathcal{A}$ computes z_a in Eq. 1 using intercepted $\{c_k, A_k\}$ and self selected and/or computed $\{r_a, T_a, x_a, R_a = r_a.P, Q_a = c_a.P\}$. All parameters makes a valid relationship and if z_a is multiplied with base point P, it can be clearly seen that Eq. 3 holds. Therefore, the device access control scheme of Das *et al.* is insecure against device impersonation attack.

Likewise, quite similar procedure can be simulated to show the weakness of Das *et al.*'s scheme against the impersonation of responding device.

B. MAN IN MIDDLE ATTACK

The scheme of Das *et al.* is also vulnerable to man in middle attack and any attacker, whether insider or outsider can launch this attack. This attack can be simulated very similar to device impersonation attack as simulated in subsection III-A, proved through proposition 1 and it's proof. The attacker just needs to listen and stop the message flow and accordingly sent on both sides the forged public key of the other side along with genuine certificate captured during listening. As the steps are very similar, as given in subsection III-A, therefore, are not being reproduced here.

IV. PROPOSED SCHEME

The proposed improved scheme (iLACKA-IoT) is presented in this section. Following subsections provide brief explanation of each of the corresponding phase of the iLACKA-IoT which is also illustrated in Fig. 3:

A. DEVICE REGISTRATION PHASE

For registration purposes, CA selects an identity ID_k for each device $\{D_k | k = 1, 2 \ldots n\}$. The CA then selects private key x_k and computes public key $Q_k = x_k.P$ for D_k. CA generates l_k randomly and computes $A_k = (x_k + l_k).P$ and certificate $c_k = x_{CA} + (x_k + l_k)H(ID_k||A_k) + x_k$. Finally CA stores $\{ID_k, A_k, c_k, x_k, Q_k\}$ along with public parameters of the system $\{E_p(\alpha, \beta), P, Q_{CA}, H(.)\}$ on the memory of device D_k.

B. PROPOSED DEVICE ACCESS CONTROL PHASE

In proposed iLACKA-IoT, this phase is initiated by an IoT device D_i, when it needs to communicate with another device

D_j. The access control phase completes by execution of following steps between both devices i.e. D_i and D_j:

PAC 1: $\boldsymbol{D_i \rightarrow D_j : \{Msg_1\}}$

Initially, D_i construct an access control request and for this D_i selects $r_i \in Z_p^*$ and timestamp T_i. D_i further computes $R_i = r_i P$, $z_i = r_i + c_i$ and sends $Msg_1 = \{ID_i, A_i, T_i, z_i, R_i, Q_i\}$ to D_j.

PAC 2: $\boldsymbol{D_j \rightarrow D_i : \{Msg_2\}}$

On receiving Msg_1, D_j first verifies the freshness of time stamp through $|T_i - T_i^*| \leq 0$, where T_i^* denotes the receiving timestamp on D_j side. The D_j on success scenario verifies $z_i.P \stackrel{?}{=} R_i + Q_{CA} + H(ID_i||A_i)A_i + Q_i$, terminates the access control request in fail case. Otherwise, D_j selects random nonce and current timestamp pair $\{r_j \in Z_p^*, T_j\}$ and computes $R_j = r_j.P$, $z_j = r_j + c_j$, $B_{ij} = r_j.R_i$, $K_{ij} = x_j.Q_i$ along with session key $SK_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ and its' verifier $SKV_{ij} = h(SK_{ij}||T_j)$. D_j at last sends $Msg_2 = \{ID_j, A_j, T_j, z_j, R_j, Q_j, SKV_{ij}\}$ to D_i.

PAC 3: $\boldsymbol{D_i \rightarrow D_j : \{Msg_3\}}$

On receiving Msg_2, D_i first verifies the freshness of time stamp through $|T_j - T_j^*| \leq 0$, where T_j^* denotes the receiving timestamp on D_i side. The D_i on success scenario verifies $z_j.P \stackrel{?}{=} R_j + Q_{CA} + H(ID_j||A_j)A_j + Q_j$ and 2) $z_j.P \stackrel{?}{=} c_j.P + H(A_j||c_j||R_j||Q_j||T_j)(R_j + Q_j)$, terminates the access control request in fail case. Otherwise, D_i computes $B_{ij} = r_i.R_j$, $K_{ij} = x_i.Q_j$ and session key $SK'_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$. D_i then checks the validity of SK'_{ij} through $SKV_{ij} \stackrel{?}{=} h(SK_{ij}||T_j)$. If verified successfully, D_i generate new timestamp T'_i and computes its' own key verifier $SKV'_{ij} = h(SK'_{ij}||T'_j)$ and sends $Msg_3 = \{SKV'_{ij}\}$ to D_j.

PAC 4: On receiving Msg_3, D_j first verifies the freshness of time stamp through $|T'_i - T'^*_i| \leq 0$, where T'^*_i denotes the receiving timestamp on D_j side. The D_j on success verifies $SKV'_{ij} \stackrel{?}{=} h(SK_{ij}||T'_j)$. Upon success D_j considers D_i authenticated with $SK_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ as the session key shared among the peer.

V. SECURITY ANALYSIS

In this section, we conduct formal security analysis using *ROR* (Real-Or-Random) oracle model along with a comprehensive discussion on attack resilience of the proposed iLACKA-IoT, especially against the device impersonation and man in middle attacks. Following subsections provide formal and informal analysis:

A. FORMAL SECURITY ANALYSIS

The formal *ROR* (Real-Or-Random) oracle model [35] is adopted to prove the security of proposed device to device access control (iLACKA-IoT) in internet of things based architecture. This subsection proves the secrecy of the shared authenticated session key SK_{ij} among two IoT devices D_i and D_j. The investigation in *ROR* initiates by using semantic security and after then the SK_{ij} security of the proposed iLACKA-IoT protocol follows in Theorem 1. All the below mentioned queries are executed by $\mathcal{A}$- the adversary as well as the collision resistant $H(..)$ function is considered to be accessible by all participants including $\mathcal{A}$; whereas, $H(..)$ is modeled as a random oracle (RO) termed as HS_f, following components describe the execution of *ROR* model:

Participants. By and large two entities/devices (D_i and D_j) communicates for successful and normal completion of the authentication procedure in the proposed iLACKA-IoT; whereas, *CA* furnishes the device registration and dynamic device addition procedures. We use $\Pi_{D_i}^{d_1}$ and $\Pi_{D_j}^{d_2}$ to illustrate the instances d_1 (for D_i) and d_2 (for D_j) for each of the device, and are called RO instances.

Following queries are solicited:

Execute($\Pi_{D_i}^{d_1}$, $\Pi_{D_j}^{d_2}$), the execute is a simulation of the eavesdropping the communication between D_i and D_j. The attacker gets the messages shared on public channel through this query.

CorruptDevice($\Pi_{D_i}^{d_1}$) This supports in stealing the stored parameters from compromised and/or stolen device D_i or D_j.

Reveal(Π^d) Applying this query, $\mathcal{A}$ can expose the key SK_{ij} shared between D_i and D_j (i.e between (Π^d) and counterpart device).

Test(Π^d) Applying this query, $\mathcal{A}$ can test the genuineness of SK_{ij}, while Π^d results a random out put of an impartial flipping of a coin (say *co*).

Accepted State The "accepted state" occurs for an instance Π^d, when the last message is accepted and it shows the messages communicated are in sequence with an *Sid* of Π^d (the session identifier) for the session being executed.

Partnering The instances Π^{d_1} and Π^{d_2} are termed as mutual-partners subject to trueness of following properties:

-Π^{d_1} and Π^{d_2} both are in accepted states.

-Π^{d_1} and Π^{d_2} share *Sid*.

-Π^{d_1} and Π^{d_2} are mutual participant of each other.

Freshness Any instance Π^{d_1} or Π^{d_2} is termed as fresh subject to $\mathcal{A}$ incapability to expose SK_{ij} constituted among both the partner-devices by applying $reveal(\Pi^d)$.

Definition 1 illustrates the semantic security of the proposed ($iLACKA - IoT$), which is proved in Theorem 1.

Definition (*Semantic Security*). The advantage for $\mathcal{A}$ to break semantic security of iLACKA-IoT in polynomial time t_{pl} to expose SK_{ij} between D_i and D_j can be expressed as $ADV_{\mathcal{A}}^{iLACKA-IoT}(t_{pl}) = |2Pr[co' = co] - 1|$, with co' denotes the original and *co* the guessed bits.

Theorem 1. The advantage for an active $\mathcal{A}$ to expose the SK_{ij} between D_i and D_j with polynomial time $t_{pl}$and q_{HS_f} number of queries are allowed in t_{pl}, during access control phase of iLACKA-IoT can be approximated as:

$$ADV_{\mathcal{A}}^{iLACKA-IoT}(t_{pl}) \leq \frac{q_{hs_f}^2}{HS_f} + ADV_{\mathcal{A}}^{ECDDHP}(t_{pl}).$$

Proof. The proof consists of three games $G_n^{\mathcal{A}}|n = 1, 2, 3$ for $\mathcal{A}$ [13], [36] with win probability of an event, where $\mathcal{A}$ can correctly guess a bit *co* can be denoted as $Sucp_{G_n}^{\mathcal{A}}$. $\mathcal{A}$'s

advantage is solicited as: $ADV_{\mathcal{A},G_n}^{iLACKA-IoT} = Pr[Sucp_{G_n}^{\mathcal{A}}]$. The games are simulated as follows:

$\mathbf{G}_1^{\mathcal{A}}$. The game depicts the real attack on $iLACKA - IoT$ protocol under ROR conditions. $\mathcal{A}$ is required to pick a bit co randomly before initiation of this $G_1^{\mathcal{A}}$ Using definition 1, following is the result:

$$ADV_{\mathcal{A}}^{iLACKA-IoT}(t_{pl}) = 2ADV_{\mathcal{A},G_1}^{iLACKA-IoT}(t_{pl}) \tag{5}$$

$\mathbf{G}_2^{\mathcal{A}}$. Through $G_2^{\mathcal{A}}$, $\mathcal{A}$ performs eavesdropping over the public channel during device access control (DAC) phase of $iLACKA - IoT$. $\mathcal{A}$ can launch Execute query for the interception of communicated messages, i.e $Msg_1 = \{ID_i, A_i, T_i, z_i, R_i, Q_i\}$ from D_i to D_j, $Msg_2 = \{ID_j, A_j, T_j, z_j, R_j, Q_j, SKV_{ij}\}$ return challenge from D_j to D_i and $Msg_3 = \{SKV'_{ij}\}$ response from D_i to D_j. Based on eavesdropping, $\mathcal{A}$ tries to construct $SK_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ and $\mathcal{A}$ is required to verify the correctness of SK_{ij} by simulating *reveal* and *Test* queries. $\mathcal{A}$ is unaware of both the temporary secret pair $\{r_i, r_j\}$ and long term secret pair $\{x_i, x_j\}$. Therefore, the winning probability of $\mathcal{A}$ remains unchanged and both $G_1^{\mathcal{A}}$ and $G_2^{\mathcal{A}}$ are indistinguishable. Therefore:

$$ADV_{\mathcal{A},G_2}^{iLACKA-IoT} = ADV_{\mathcal{A},G_1}^{iLACKA-IoT} \tag{6}$$

$\mathbf{G}_3^{\mathcal{A}}$. It imitates an active attack, where HS_f and *CorruptDevice* are simulated. The proposed $iLACKA - IoT$ complete the access control procedure in three (3) messages and in Msg_1 the dynamic alias certificate z_i is protected by oneway function $H(.)$, which is collision resistant (CR); whereas, in Msg_2 both Z_j and SKV_{ij} and in Msg_3 the SKV'_{ij} are secure under CR property of $H(..)$. $\mathcal{A}$ could use the intercepted $R_i = r_i.P$ and $R_j = r_j.P$ and try to construct $B_{ij} = r_i r_j.P$ and from publicly available and /or intercepted $Q_i = x_i.p$, and $Q_j = r_j.P$ try to construct $K_{ij} = x_i x_j.P$, computing each of B_{ij} and K_{ij} is a computationally infeasible *ECDHHP* problem, which cannot be solved in polynomial time t_{pl}. Likewise, due to the usage of random numbers i.e r_i and r_j in z_i and z_j, makes it computationally infeasible to extract these random numbers and/or the device certificates. The digest HS_f is always unique because each computation consists of either current time timestamp or some random variable. Moreover, querying *CorruptDevice*, $\mathcal{A}$ gets the secrets stored in specific device D_i, which can help in forming a session key but the random numbers and timestamps as well as private keys of the non-compromised devices are important. On exclusion of the HS_f and *CorruptDevice* from $G_3^{\mathcal{A}}$, the games $G_2^{\mathcal{A}}$ and $G_3^{\mathcal{A}}$ are "indistinguishable". Using thr birthday paradox and hardness of ECDDHP, following relation is reached:

$$ADV_{\mathcal{A},G_2}^{iLACKA-IoT} - ADV_{\mathcal{A},G_3}^{iLACKA-IoT} \leq \frac{q_{hs_f}^2}{2|HS_f|} + ADV_{\mathcal{A}}^{iLACKA-IoT}(t_{pl}) \tag{7}$$

After executing all queries, $\mathcal{A}$ is left with guessing the coined bit co correctly to win $\mathbf{G}_3^{\mathcal{A}}$, it's clear that:

$$ADV_{\mathcal{A},G_3}^{iLACKA-IoT} = \frac{1}{2} \tag{8}$$

Eq. 5 gives:

$$\frac{1}{2}ADV_{\mathcal{A}}^{iLACKA-IoT}(t_{pl}) = |ADV_{\mathcal{A},G_1}^{iLACKA-IoT} - \frac{1}{2}| \tag{9}$$

Eqs. 6-8 and the triangular inequality will lead to the following computations:

$$\begin{aligned}\frac{1}{2}ADV_{\mathcal{A}}^{iLACKA-IoT}(t_{pl}) &= |ADV_{\mathcal{A},G_1}^{iLACKA-IoT} - ADV_{\mathcal{A},G_3}^{iLACKA-IoT}| \\ &= |ADV_{\mathcal{A},G_2}^{iLACKA-IoT} - ADV_{\mathcal{A},G_3}^{iLACKA-IoT}| \\ &\leq \frac{q_{hs_f}^2}{2|HS_f|} + ADV_{\mathcal{A}}^{ECDDHP}(t_{pl}).\end{aligned} \tag{10}$$

Finally, multiplying the Eq. 10 by 2, the result is obtained as: $ADV_{\mathcal{A}}^{iLACKA-IoT}(t_{pl}) \leq \frac{q_{hs_f}^2}{|HS_f|} + 2ADV_{\mathcal{A}}^{ECDDHP}(t_{pl})$.

B. SECURITY DISCUSSION

Following subsections present the discussion on attack resilience of the proposed iLACKA-IoT:

1) DEVICE IMPERSONATION ATTACK

In proposed iLACKA-IoT, the attacker $\mathcal{A}$ can try to launch device impersonate attack (DIA). For DIA, $\mathcal{A}$ has to create a valid and legal request $Msg_1 = \{ID_i, A_i, T_i, z_i, R_i, Q_i\}$ or response message $Msg_2 = \{ID_j, A_j, T_j, z_j, R_j, Q_j, SKV_{ij}\}$. For the sake of simplicity, the discussion provided here is confined to request message Msg_1 and there is symmetry with reply message from the responding device. The $\mathcal{A}$ has access to all public parameters including identities and public keys of all the participants $\{Q_i = x_i.P, Q_{CA} = x_{CA}.P, ID_i, ID_j, P, E_p(\alpha, \beta)\}$. Moreover, under the DY threat model as described in subsection I-B, $\mathcal{A}$ has captured the messages previously exchanged between the two entities say $Msg_1^{Pre} = \{ID_i, A_i, T_i^{Pre}, z_i^{Pre}, R_i^{Pre}, Q_i\}$ and $Msg_2 = \{ID_j, A_j, T_j^{Pre}, z_j^{Pre}, R_j^{Pre}, Q_j, SKV_{ij}^{Pre}\}$. Now, $\mathcal{A}$ can use the public parameters and the captured messages to create a new login request, for that $\mathcal{A}$ can replay the public parameters $\{ID_i, A_i, Q_i\}$ along with new timestamp T_i^{new}. Let $\mathcal{A}$ created the request message $Msg_1^{\mathcal{A}} = \{ID_i, A_i, T_i^{new}, z_i^{\mathcal{A}}, R_i^{\mathcal{A}}, Q_i\}$. There are following two possibilities:

1) $\mathcal{A}$ just replaces the previous timestamps and use old values of $\{z_i, R_i\}$, in this case $\mathcal{A}$ can pass the initial test $z_i.P \stackrel{?}{=} c_i.P + H(A_i||c_i||R_i||Q_i||T_i)(R_i + Q_i)$ but as $\mathcal{A}$ does not know r_i and cannot extract it from $R_i = r_i.P$; therefore, $\mathcal{A}$ will not be able to generate $B'_{ij} = r_i.R_j$, moreover the computation of $K_{ij} = x_i.Q_j$ also requires the private x_i of D_i. Hence, $\mathcal{A}$ cannot compute session key $SK'_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ and ultimately is unable to pass $SKV'_{ij} \stackrel{?}{=} h(SK_{ij}||T'_i)$ test.

2) $\mathcal{A}$ tries to create new values of $\{z_i, R_i\}$, in this case $\mathcal{A}$ can not generate valid $\{R_i = r_iP, z_i = r_i + c_i\}$ pair without having the secret certificate of D_i. Even if the secret certificate $c_i = x_{CA} + (x_i + l_i)H(ID_i||A_i) + x_i$ is exposed to $\mathcal{A}$, without knowing the secret key x_i of D_i, $\mathcal{A}$ is unable to compute $K_{ij} = x_i.Q_j$ and session key $SK'_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ and fails $SKV'_{ij} \stackrel{?}{=} h(SK_{ij}||T'_i)$ test. $\mathcal{A}$ can also try to forge public key of D_i by selecting $x_i^{\mathcal{A}} \in z_p^*$ and computing $Q_i^{\mathcal{A}} = x_i^{\mathcal{A}}.P$ (as it can be forged in the original scheme of Das *et al.* proved in subsection III-A). However, the original certificate c_i (of D_i) now becomes irrelevant because it is not useful without genuine secret and public key pair $\{x_i, Q_i\}$ and now $\mathcal{A}$ cannot pass initial $z_i.P \stackrel{?}{=} c_i.P + H(A_i||c_i||R_i||Q_i||T_i)(R_i + Q_i)$ test.

Therefore, considering all the possible options including the leakage of original certificate, no adversary $\mathcal{A}$ has advantage to impersonate on behalf of any-other device without having the private key of the victim. Therefore, iLACKA-IoT is safe from DIA.

2) MAN IN MIDDLE ATTACK

In proposed iLACKA-IoT, the attacker $\mathcal{A}$ can try to launch man in middle attack (MIMA). For this purpose, $\mathcal{A}$ has to create two valid messages: 1) $Msg_1 = \{ID_i, A_i, T_i, z_i, R_i, Q_i\}$ to be sent to the responding device D_i and 2) $Msg_2 = \{ID_j, A_j, T_j, z_j, R_j, Q_j, SKV_{ij}\}$ to be sent to the receiving device D_j. Now, again there are following two cases:

1) $\mathcal{A}$ just forward original message $Msg_1 = \{ID_i, A_i, T_i, z_i, R_i, Q_i\}$, captured from public channel, to the responding device D_j and after capturing the reply message $Msg_2 = \{ID_j, A_j, T_j, z_j, R_j, Q_j, SKV_{ij}\}$ sent it as it is to requesting device D_i. This case is just like passive listening and $\mathcal{A}$ is having no advantage to compute session key.
2) $\mathcal{A}$ tries to forge both messages $Msg_1^{\mathcal{A}} = \{ID_i, A_i, T_i^{new}, z_i^{\mathcal{A}}, R_i^{\mathcal{A}}, Q_i\}$ and $Msg_2^{\mathcal{A}} = \{ID_j, A_j, T_j^{new}, z_j^{\mathcal{A}}, R_j^{\mathcal{A}}, Q_j, SKV_{ij}^{\mathcal{A}}\}$. In this case, it is already proved in subsection V-B1 that $\mathcal{A}$ cannot constitute any of the valid message without forging the device specific certificate and private key and both of these are hard. Therefore, proposed iLACKA-IoT has capabilities to resist MIM attack.

3) REPLAY ATTACK

In the device access control phase of proposed iLACKA-IoT, all the three messages $Msg_1 = \{ID_i, A_i, T_i, z_i, R_i, Q_i\}$, $Msg_2 = \{ID_j, A_j, T_j, z_j, R_j, Q_j, SKV_{ij}\}$ and $Msg_3 = \{SKV'_{ij}, T'_i\}$ contain respective timestamps and these timestamps are also included in session key formation process $SK'_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ as well as are also used in verification parameter $SKV'_{ij} = h(SK'_{ij}||T'_j)$. Therefore, replay messages are detected at first stage and even if $\mathcal{A}$ tries to replace the old timestamp with the new freshly generated $T_i^{\mathcal{A}}$, due to different timestamp used in formation of session key and verification parameter, $\mathcal{A}$ is unable to get it self authenticated from other device and cannot generate the session key. Hence, iLACKA-IoT is not a prey of replay attack.

4) MALICIOUS DEVICE DEPLOYMENT

$\mathcal{A}$ may try to deploy a fake/malicious device in the system, which can further get authenticated and share a session key with legitimate devices with an ultimate desire to spread fake information/illegal access to legitimate information. However, $\mathcal{A}$ needs to assign it some identity say $ID_{\mathcal{A}}$ and to compute the device specific certificate $c_{\mathcal{A}} = x_{CA} + (x_{\mathcal{A}} + l_{\mathcal{A}})H(ID_{\mathcal{A}}||A_{\mathcal{A}}) + x_{\mathcal{A}}$, related parameter $A_{\mathcal{A}} = (x_{\mathcal{A}} + l_{\mathcal{A}}).P$ along with public and private key pair $\{x_{\mathcal{A}}, Q_{\mathcal{A}} = x_{\mathcal{A}}.P\}$. $\mathcal{A}$ can select $x_{\mathcal{A}} \in z_p^*$ as private key and can compute public key $Q_{\mathcal{A}} = x_{\mathcal{A}}.P$. However, the computation of certificate $c_{\mathcal{A}} = x_{CA} + (x_{\mathcal{A}} + l_{\mathcal{A}})H(ID_{\mathcal{A}}||A_{\mathcal{A}}) + x_{\mathcal{A}}$ and binding it with device specific key pair $\{x_{\mathcal{A}}, Q_{\mathcal{A}} = x_{\mathcal{A}}.P\}$ needs the private key x_{CA} of the certificate authority. Hence, malicious device cannot be deployed in the system until $\mathcal{A}$ has private key x_{CA} of the certificate authority.

5) DEVICE PHYSICAL CAPTURE ATTACK

In proposed iLACKA-IoT, even if an adversary $\mathcal{A}$ captures one or more devices, $\mathcal{A}$ has no benefit to compute private key/ certificate of any-other device of the system. This is because, every device say D_k has device specific certificate $c_k = x_{CA} + (x_k + l_k)H(ID_k||A_k) + x_k$, private key x_k and other related parameters $\{ID_k, A_k = (x_k + l_k).P, Q_k = x_k.P\}$ stored in it and in no way, these parameters give any useful information beneficial to expose parameters related to other devices in the system. Moreover, using the parameters $\mathcal{A}$ cannot expose any useful information for extraction private key x_{CA} of the certificate authority, as x_{CA} is hidden within certificate $c_k = x_{CA} + (x_k + l_k)H(ID_k||A_k) + x_k$ using other parameters including l_k, which is also unknown in addition to x_{CA}. Even if $\mathcal{A}$ captures several (m) device $D_k : \{k = 1, 2 \ldots m\}$, $\mathcal{A}$ is having no benefit to forge any non-compromised device.

6) EPHEMERAL SECRETS LEAKAGE ATTACK (ESLA)

The leakage of ephemeral secrets in proposed iLACKA-IoT do not help to reveal the session key $SK_{ij} = h(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ as it depends on both the temporary secrets ($B_{ij} = r_j.R_i = r_i.R_j = r_i.r_j.P$) r_i and r_j as well as the long term private keys of both communicating devices ($K_{ij} = x_j.Q_i = x_i.Q_j = x_i.x_j.P$) x_i and x_j of the D_i and D_j, respectively. So, if temporary secret pair $\{r_i, r_j\}$ are exposed, it can help an adversary $\mathcal{A}$ to compute $B_{ij} = r_i.r_j.P$ but without private key of any participant, $\mathcal{A}$ has no benefit to compute ($K_{ij} = x_i.x_j.P$). Similarly, if $\mathcal{A}$ gets private keys x_i and x_j and does not have access to one or both temporary secrets r_i and r_j, the $\mathcal{A}$ has advantage in computing $K_{ij} = x_i.x_j.P$ but $\mathcal{A}$ has no advantage of computing $B_{ij} = r_i.r_j.P$ without knowing one or both temporary secrets r_i and r_j. Hence proposed scheme resists ESLA.

VI. COMPARISONS WITH RELATED SCHEMES

In following sections, a brief discussion on performance including computation and communication cost along with provision of security features comparisons between proposed iLACKA-IoT and related schemes [7], [8], [11]–[13] is given:

A. PERFORMANCE COMPARISONS

In this subsection, the comparisons of the proposed scheme with related schemes [7], [8], [11]–[13] relating to computation and communication costs are provided. For comparing the computation costs, following notations along with corresponding running time as per the experiment performed by Kilinc and Yanik [37] on a dual PC (E2200) with 2 GB RAM and 2.20 processor speed over Ubuntu OS and PBC library are introduced in Table 2.

TABLE 2. Guide for computation costs.

Operation	Notation	Time (ms)
Bilinear-pair mapping	T_{pg}	≈ 5.811
Point multiplication	T_{em}	≈ 2.226
Point addition	T_{ea}	≈ 0.0288
Symmetric enc/dec-ryption	T_{sc}	≈ 0.0046
One-way hash function	T_{hf}	≈ 0.0023
Fuzzy Extractor	T_{fp}	≈ 2.226

The initiating device in proposed iLACKA-IoT performs $5T_{em}$, $6T_{ea}$ and $8T_{hf}$, the same computation cost is required in receiving device. Therefore, total computation cost to complete a single procedure in proposed scheme is $10T_{em} + 6T_{ea} + 8T_{hf}$ with running time of $\approx$ 22.4512 ms; whereas, the scheme of Das *et al.* [13] is $18T_{em} + 6T_{ea} + 12T_{hf}$ with running time $\approx$ 31.3644. Referring Table 3 proposed iLACKA-IoT has least running time as compared with all the schemes [7], [8], [11]–[13].

TABLE 3. Performance comparisons.

↓Protocols/Cost→	Computation (ms)	Bits
Our	$10T_{em} + 6T_{ea} + 8T_{hf} \approx 22.4512$	2944
Das et al. [13]	$18T_{em} + 6T_{ea} + 12T_{hf} \approx 31.3644$	3296
Jia et al. [12]	$3Tpg + 7T_{em} + 14T_{hf} \approx 33.0472$	2560
Luo et al. [11]	$4T_{pg} + 3T_{em} + 2T_{ea} + 2T_{hf} \approx 29.9312$	3040
Challa et al. [8]	$14T_{em} + T_{fp} + 12T_{hf} \approx 33.4176$	2528
Li et al. [7]	$6T_{pg} + 3T_{em} + 1T_{sc} + 2T_{hf} \approx 41.6062$	3488

The common parameter sizes are selected for computing the comparative communication costs of the proposed and related schemes [7], [8], [11]–[13], we have considered $SHA-1$ with 160 bit size, the size of RSA modular parameters and ECC point are taken as 1024 and 320 bits, as per the recommended size by NIST, the size of identity and random numbers are fixed as 160 bits, while size of timestamps is taken as 32 bits long. The proposed iLACKA-IoT completes authentication in 3 message exchanges. During $Msg_1 = \{ID_i, A_i, T_i, z_i, R_i, Q_i\}$ transmitted by initiating device D_i total $\{160 + 320 + 32 + 160 + 320 + 320\} = 1312$ bits are sent to receiving device D_j, while the reply message $Msg_2 = \{ID_j, A_j, T_j, z_j, R_j, Q_j, SKV_{ij}\}$ from D_j completes by sending $\{160 + 320 + 32 + 160 + 320 + 320 + 160\} = 1472$ bits to initiating device D_i. The last message $Msg_3 = \{SKV'_{ij}, T'_i\}$, from D_i to D_j contains 160 bits transfer. Therefore, proposed iLACKA-IoT accomplishes the access control procedure with communication cost of 2944, which is less than [7], [11], [13] and is slight higher than schemes proposed in [8], [12].

TABLE 4. Security features.

↓ Features/Protocol →	Our	[13]	[12]	[11]	[8]	[7]
Correctness	✓	✓	✓	✓	✗	✓
D2D Direct Communication	✓	✓	✗	✗	✓	✓
Mutual Authentication	✓	✓	✓	✗	✓	✗
Device Impersonation	✓	✗	✓	✓	✓	✓
Resist Replay	✓	✓	✓	✓	✓	✓
Malicious Device Deploy.	✓	✓	✓	✓	✓	✓
Resist Physical Capture	✓	✓	✓	✓	✓	✓
Resist ESL	✓	✓	✓	✗	✓	✗
Key Agreement	✓	✓	✓	✓	✓	✓
Resist Man in Middle	✓	✗	✓	✓	✓	✓
Formal Security	✓	✓	✓	✗	✓	✗

B. SECURITY FEATURES

This subsection elaborates the comparisons of security properties and attack resilience of the proposed iLACKA-IoT and related schemes [7], [8], [11]–[13]. Referring the summary of said comparisons in Table 4, the scheme of Das *et al.* is insecure against device impersonation and man in middle attacks; whereas, the both the schemes [11] presented by Luo *et al.* and [7] presented by Li *et al.* are weak against ephemeral secret leakage (ESL) attack and do not provide mutual authentication as well as lack the formal security proof. Furthermore, [11] also does not provide direct D2D access control and needs an intermediate agent for completion of authentication procedure. The scheme presented in [8] has correctness issues, where the receiving device is forced to get authenticated with an unknown device. Moreover, the scheme is static and cannot provide authentication between different devices; while the scheme [12] proposed by Jia *et al.* also needs an intermediate agent for completion of authentication between two entities and cannot provide direct D2D authentication. Out of the related and compared schemes, only proposed iLACKA-IoT provides attack resilience and extends the important known security features.

VII. CONCLUSION

In this paper, we first analyzed a recent access control scheme proposed recently by Das *et al.* We have shown that the scheme LACKA-IoT is insecure against device impersonation and man in middle attacks. An improved scheme iLACKA-IoT is then proposed to overcome the weaknesses of LACKA-IoT. The security of the proposed scheme is proved using formal and informal methods. The proposed iLACKA-IoT provides better security and performance than related schemes, specifically it has low computation, communication cost as compared with LACKA-IoT and it overcomes the weaknesses of the same. The proposed iLACKA-IoT completes the access control and the key establishment phase

in just 22.4512 ms and by exchanging 2944 bits. The proposed iLACKA-IoT has reduced approximately 39.7% computation and 12% communication overhead as compared with previous LACKA-IoT scheme proposed by Das *et al.* Therefore, proposed iLACKA-IoT is a good candidate for deployment in real scenarios.

REFERENCES

[1] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, "Internet of Things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Gener. Comput. Syst.*, vol. 92, pp. 265–275, Mar. 2019.

[2] Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, "Internet of Things-aided smart grid: Technologies, architectures, applications, prototypes, and future research directions," *IEEE Access*, vol. 7, pp. 62962–63003, 2019.

[3] M. A. Rahman, A. T. Asyhari, S. Azad, M. M. Hasan, C. P. C. Munaiseche, and M. Krisnanda, "A cyber-enabled mission-critical system for post-flood response: Exploiting TV white space as network backhaul links," *IEEE Access*, vol. 7, pp. 100318–100331, 2019.

[4] P. Asghari, A. M. Rahmani, and H. H. S. Javadi, "Internet of Things applications: A systematic review," *Comput. Netw.*, vol. 148, pp. 241–261, Jan. 2019.

[5] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Gener. Comput. Syst.*, vol. 108, pp. 909–920, Jul. 2020.

[6] Z. Zhang, Q. Qi, N. Kumar, N. Chilamkurti, and H.-Y. Jeong, "A secure authentication scheme with anonymity for session initiation protocol using elliptic curve cryptography," *Multimedia Tools Appl.*, vol. 74, no. 10, pp. 3477–3488, May 2015.

[7] F. Li, Y. Han, and C. Jin, "Practical access control for sensor networks in the context of the Internet of Things," *Comput. Commun.*, vols. 89–90, pp. 154–164, Sep. 2016.

[8] 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.

[9] M. N. Aman and B. Sikdar, "ATT-auth: A hybrid protocol for industrial IoT attestation with authentication," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 5119–5131, Dec. 2018.

[10] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IoT systems using physical unclonable functions," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327–1340, Oct. 2017.

[11] 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.

[12] 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, Nov. 2019.

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

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

[15] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "Cloud centric authentication for wearable healthcare monitoring system," *IEEE Trans. Dependable Secure Comput.*, early access, Apr. 19, 2018, doi: 10.1109/TDSC.2018.2828306.

[16] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial Internet of Things," *IEEE Trans. Dependable Secure Comput.*, early access, Jul. 19, 2018, doi: 10.1109/TDSC.2018.2857811.

[17] 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.

[18] K. Mansoor, A. Ghani, S. Chaudhry, S. Shamshirband, S. A. K. Ghayyur, and A. Mosavi, "Securing IoT-based RFID systems: A robust authentication protocol using symmetric cryptography," *Sensors*, vol. 19, no. 21, p. 4752, Nov. 2019.

[19] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. N. Saqib, "Security and key management in IoT-based wireless sensor networks: An authentication protocol using symmetric key," *Int. J. Commun. Syst.*, vol. 32, no. 16, p. e4139, Nov. 2019.

[20] S. Challa, A. K. Das, V. Odelu, N. Kumar, S. Kumari, M. K. Khan, and A. V. Vasilakos, "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Electr. Eng.*, vol. 69, pp. 534–554, Jul. 2018.

[21] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al-Barakati, and T. Shon, "An anonymous device to device authentication protocol using ECC and self certified public keys usable in Internet of Things based autonomous devices," *Electronics*, vol. 9, no. 3, p. 520, Mar. 2020.

[22] 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, Mar. 2020.

[23] 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, Jun. 2020, Art. no. 102502.

[24] S. Hussain and S. A. Chaudhry, "Comments on 'biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of Things deployment,'" *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10936–10940, Dec. 2019.

[25] H. Tao, M. Z. A. Bhuiyan, M. A. Rahman, T. Wang, J. Wu, S. Q. Salih, Y. Li, and T. Hayajneh, "TrustData: Trustworthy and secured data collection for event detection in industrial cyber-physical system," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3311–3321, May 2020.

[26] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: A certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[27] 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, Dec. 2019.

[28] 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, Aug. 2019.

[29] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for Internet of Vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

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

[31] M. S. Farash, O. Nawaz, K. Mahmood, S. A. Chaudhry, and M. K. Khan, "A provably secure RFID authentication protocol based on elliptic curve for healthcare environments," *J. Med. Syst.*, vol. 40, no. 7, p. 165, Jul. 2016.

[32] 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.

[33] A. Irshad, S. A. Chaudhry, O. A. Alomari, K. Yahya, and N. Kumar, "A novel pairing-free lightweight authentication protocol for mobile cloud computing framework," *IEEE Syst. J.*, early access, Jun. 19, 2020, doi: 10.1109/JSYST.2020.2998721.

[34] 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.

[35] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Public Key Cryptogr. (PKC)*, Les Diablerets, Switzerland, 2005, pp. 65–84.

[36] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020.

[37] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 1005–1023, 2nd Quart., 2014.

SHEHZAD ASHRAF CHAUDHRY received the master's and Ph.D. degrees (Hons.) from the International Islamic University Islamabad, Pakistan, in 2009 and 2016, respectively. He is currently working as an Associate Professor with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, stanbul, Turkey. He has authored over 100 scientific publications appeared in different international journals and proceedings, including more than 73 in SCI/E journals. With an H-index of 23 and an I-10 index 48, his work has been cited over 1750 times. He has also supervised over 35 graduate students in their research. His current research interests include lightweight cryptography, elliptic/hyper elliptic curve cryptography, multimedia security, E-payment systems, MANETs, SIP authentication, smart grid security, IP multimedia subsystem, and next generation networks. He occasionally writes on issues of higher education in Pakistan. He has served as a TPC member of various international conferences. He is an Active Reviewer of many ISI indexed journals. He was a recipient of the Gold Medal for achieving 4.0/4.0 CGPA in his Masters. Considering his research, Pakistan Council for Science and Technology granted him the Prestigious Research Productivity Award, while affirming him among Top Productive Computer Scientist in Pakistan.

KHALID YAHYA received the Ph.D. degree in electrical engineering from Kocaeli University, Kocaeli, Turkey, in 2018. He is currently working as an Assistant Professor of mechatronics engineering with Istanbul Gelisim University, Turkey. He has published over a dozen articles in prestigious journals and conferences. He is an active reviewer of many conferences and journals. His current research interests include microelectronic circuit analysis and design, renewable energy resources, power electronics, and MPPT designs for energy harvesting systems and information security.

FADI AL-TURJMAN (Member, IEEE) received the Ph.D. degree in computer science from Queen's University, Kingston, ON, Canada, in 2011. He is currently a Full Professor and a Research Center Director of Near East University, Nicosia, Cyprus. He is a leading authority in the areas of smart/intelligent, wireless, and mobile networks' architectures, protocols, deployments, and performance evaluation. His publication history spans over 250 publications in journals, conferences, patents, books, and book chapters, in addition to numerous keynotes and plenary talks at flagship venues. He has authored and edited more than 25 books about cognition, security, and wireless sensor networks' deployments in smart environments, published by Taylor and Francis, Elsevier, and Springer. He received several recognitions and best papers' awards at top international conferences. He also received the prestigious Best Research Paper Award from Elsevier Computer Communications Journal for the period 2015–2018, in addition to the Top Researcher Award for 2018 at Antalya Bilim University, Turkey. He has led a number of international symposia and workshops in flagship communication society conferences. He also serves as an Associate Editor and the Lead Guest/Associate Editor for several well reputed journals, including *IEEE Communications Surveys and Tutorials* (IF 22.9) and the Elsevier Sustainable Cities and Society (IF 4.7).

MING-HOUR YANG (Member, IEEE) received the Ph.D. degree in computer science & information engineering from National Central University, Taiwan. His research interests include network security and system security with particular interests on security issues in RFID and NFC security communication protocols. Topics include: mutual authentication protocols, secure ownership transfer protocols, polymorphic worms, and tracing mobile attackers.