IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 26, 2019, accepted April 21, 2019, date of publication April 24, 2019, date of current version May 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2912998

Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment

ASHOK KUMAR DAS[1], (Senior Member, IEEE), MOHAMMAD WAZID[2], (Member, IEEE), ANIMI REDDY YANNAM[1], JOEL J. P. C. RODRIGUES[3,4,5], (Senior Member, IEEE), AND YOUNGHO PARK[6], (Member, IEEE)

[1]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
[2]Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576 104, India
[3]National Institute of Telecommunications (Inatel), 37540-000 Santa Rita do Sapucaí, Brazil
[4]Instituto de Telecomunicações, 1049-001 Lisbon, Portugal
[5]Federal University of Piauí (UFPI), 64049-550 Teresina, Brazil
[6]School of Electronics Engineering, Kyungpook National University, Daegu 41566, South Korea

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

This work was supported in part by the Basic Science Research Program through the National Research Foundation of Korea, Ministry of Science, ICT and Future Planning, under Grant 2017R1A2B1002147, in part by the BK21 Plus Project of the Ministry of Education, South Korea, under Grant 21A20131600011, in part by the Fundação para a Ciência e a Tecnologia under Project UID/EEA/50008/2019, in part by the RNP with resources from MCTIC under the Centro de Referência em Radiocomunicações- (CRR) Project of the Instituto Nacional de Telecomunicações (Inatel), Brazil, under Grant 01250.075413/2018-04, in part by the Brazilian National Council for Research and Development (CNPq) under Grant 309335/2017-5, and in part by the Brazilian National Council for Research and Development (CNPq) under Grant 201155/2015-0.

ABSTRACT For secure communication between any two neighboring sensing devices on the Internet of Things (IoT) environment, it is essential to design a secure device access control and key agreement protocol, in which the two phases, namely, ''node authentication'' and ''key agreement'' are involved. While the node authentication allows two sensing devices to authenticate each other using their own pre-loaded secret credentials in memory, the key agreement phase permits to establish a secret key between them if the mutual authentication is successful. In this paper, we propose a new certificate-based ''lightweight access control and key agreement protocol in the IoT environment, called LACKA-IoT,'' that utilizes the elliptic curve cryptography (ECC) along with the ''collision-resistant one-way cryptographic hash function.'' Through a detailed security analysis using the formal security under the ''Real-Or-Random (ROR) model,'' informal (non-mathematical) security analysis, and formal security verification using the broadly used ''Automated Validation of Internet Security Protocols and Applications (AVISPA)'' tool, we show that the LACKA-IoT can protect various known attacks that are needed for a secure device access control mechanism in the IoT. Furthermore, through a comparative study of the LACKA-IoT and other relevant schemes, we show that there is a better tradeoff among the security and functionality features and communication and computational costs of the LACKA-IoT as compared to other schemes. Finally, the ''practical demonstration using the NS2 simulation'' has been carried out on the LACKA-IoT to measure various network parameters.

INDEX TERMS Internet of Things (IoT), smart devices, device access control, key agreement, security, AVISPA.

I. INTRODUCTION

The Internet of Things (IoT) consists of ''several things (devices) that are interconnected through the public Internet'' [1]. A thing or object could be either physical or virtual that can be assigned a unique identity, such as device ID or IP address. Examples of ''physical objects'' include ''smartphone, sensor, camera, drone, vehicle, and so on'', whereas ''virtual objects'' may be ''agenda, electronic ticket, book, wallet, and so on''. Most of the IoT devices are smart because these can send the data gathered from their surrounding environment and take actions without any human interventions.

Figure 1 [2], [3] illustrates ''a generic IoT network architecture in which different scenarios (e.g., home, transport, community and national) are shown''. The smart devices,

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

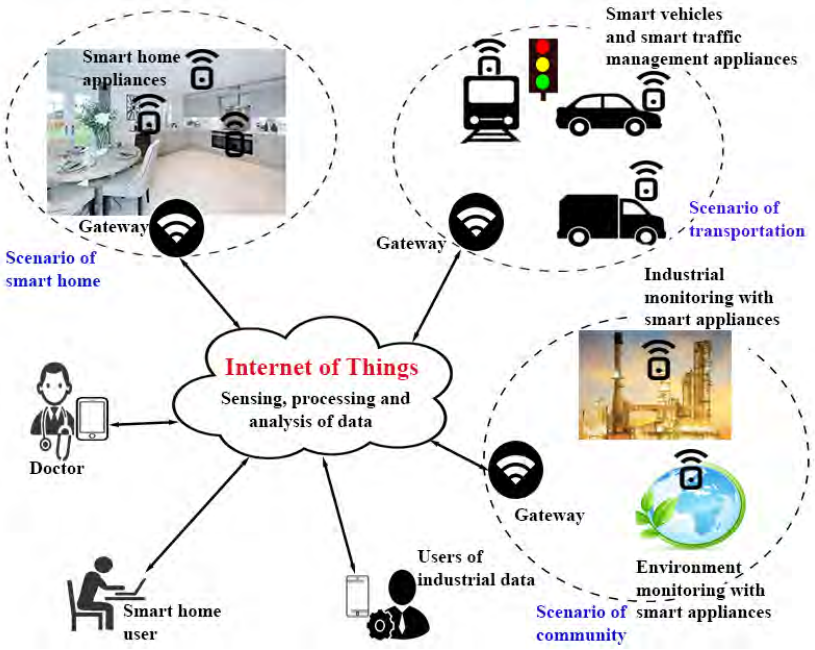

FIGURE 1. A generic IoT environment (Adapted from [2], [3]).

TABLE 1. IoT endpoint spending by category (millions of dollars) [7].

Category	2016	2017	2018	2020
Consumer	532,515	725,696	985,384	1,494,466
Business: cross-industry	212,069	280,059	372,989	567,659
Business: vertical-specific	634,921	683,817	736,543	863,662
Total	1379,505	1,689,572	2,094,881	2,925,787

such as ''sensors'' and ''actuators'' are placed in different applications. The IoT devices are then interconnected to the public Internet through the trusted Gateway Nodes (GWNs). Furthermore, in some applications, the access privilege of IoT smart devices can be given to different users (e.g., ''a smart home user in a home application'' [4] and ''a doctor in a healthcare application'' [5]) [1], [6]. Gartner Inc. [7] predicted that ''the number of connected IoT smart devices will reach 20.4 billion by the year 2020''. As the customers are anticipated to buy more IoT devices in the future, ''business investments are likely to increase in future years'' too. Table 1 tabulates the ''IoT endpoint spending by category (millions of dollars)'' [7]. It is also predicted that, by 2020, ''the hardware spending from both segments may extend to about $3 trillion'' [7].

Das *et al.* [1] provided a taxonomy of various security protocols that are essential for securing an IoT environment. They mainly concentrate on the following security aspects related to IoT environment: key management [8]–[14]; user/device authentication [15]–[30]; device access control [31]–[33]; user access control [34]–[36]; privacy preservation [37]–[39]; and identity management [40], [41]. The details of these security mechanisms are given in [1].

In the IoT environment, some smart devices may be physically captured as discussed in Section I-A2 or their battery may drain out. Therefore, to prolong the lifetime of smart devices in the IoT environment, new smart devices deployment is an important task. The deployed smart devices may not be always assumed to be genuine ones as an adversary may deploy some malicious smart devices in the network. This demands for a ''device access control'' mechanism to prevent malicious devices from entering the IoT network. We consider a device access control mechanism in IoT consisting of the following two tasks [1]:

- *Node (device) authentication:* This requires that ''a newly deployed smart device must authenticate itself to its neighbor smart devices to prove that it is a legitimate smart device for accessing the information from the other smart devices''.
- *Key agreement:* This requires that ''a newly deployed smart device needs to establish shared secret keys with its existing neighbor smart devices to assure secure communication during the transmission of sensing information''.

In addition, a new smart device addition phase is essential for access control process in the IoT network.

In this article, we concentrate on the device access control mechanism, which is treated as one of the most important security protocols that is very much essential for securing IoT environment [1]. We propose a novel certificate-based device access control scheme, which is efficient in computation as well as communication, and also provides better ''security & functionality features'' that are essential for device access control, as compared to existing related device access control protocols.

A. SYSTEM MODELS

In this section, we discuss the following models related to our access control scheme in IoT.

1) NETWORK MODEL

We consider the network model for IoT environment as shown in Figure 1. For a particular application, say healthcare [5] or Industrial IoT (IIoT) [2], [42], several IoT smart devices are placed in a deployment area, called the ''target field''. The gateway node (*GWN*) can be placed at the corner or at the center of the target field depending on the application scenario. The smart devices will communicate with their neighbor devices. The information gathered by the smart devices need to be sent to the *GWN* for further processing or decisions. The smart devices close to the *GWN* will directly communicate with the *GWN*. Since the communication between the devices and also between the *GWN* and devices is done typically through wireless medium, there are possibility of having potential attacks performed by an adversary. For secure communications among the communicating entities in the IoT environment, a ''device access control'' plays a very important role where the neighboring devices will authentication each other (via device authentication) followed by secret key establishment among them if the device authentication is made successful. Thus, the information collected at the *GWN* securely from the smart devices can be also stored in the cloud server(s) so that other users can use those information too.

2) ATTACK MODEL

The broadly-used ''Dolev-Yao threat model (also known as the DY model)'' [43] is applied in the proposed scheme, LACKA-IoT. The entities involved in the IoT environment can communicate among each other using a public channel under the DY model in which the end-point entities (e.g., smart devices) are not treated as trusted entities.

We also adopt the ''current *de facto* standard model in modeling key-exchange protocols, called the CK-adversary model [44], [45]'' in the proposed LACKA-IoT. In the CK-adversary model, ''an adversary $\mathcal{A}$ can not only deliver data as in the DY model, but he/she can compromise the secret credentials (e.g., session keys, private keys and also session state)''. Thus, even if ''some forms of secret credentials are somehow known to $\mathcal{A}$, there should have a minimum possible consequence on the security of other secret credentials of the communicating participants [46]''.

In some applications, the smart devices can be deployed in ''an unattended or hostile environment where monitoring 24×7 of the deployed devices is not possible'', and hence, there is a chance of physical device capture attack by the adversary $\mathcal{A}$. Therefore, ''the secret credentials stored in the captured smart device(s) can be easily extracted by $\mathcal{A}$ with the sophisticated power analysis attacks as explained in [47], [48], and $\mathcal{A}$ can use those extracted information to deploy fake smart devices in the network''. Finally, it is assumed that both the certification authority (*CA*) and the *GWN* are trusted and these will not be compromised by $\mathcal{A}$. The *CA* is the only trusted authority that can issue the valid certificates for the devices and the *GWN*.

B. RESEARCH CONTRIBUTIONS

The ''main research contributions'' made in this article are as follows.

- A novel certificate-based device access control scheme for the IoT environment has been designed, called ''lightweight access control and key agreement protocol in IoT environment (LACKA-IoT)''. The certificates for the smart devices and the *GWN* are issued by the trusted *CA* only. LACKA-IoT is lightweight as it relies on ECC and ''collision-resistant one-way hash function''. Most importantly, LACKA-IoT does not involve the *GWN* for device access control phase between two neighbor smart devices in the IoT environment.
- A detailed security analysis on LACKA-IoT has been carried out which includes ''formal security analysis using the widely-accepted ROR model [49], informal (non-mathematical) security analysis and also formal security verification based on the broadly-applied software verification tool, known as AVISPA tool [50]'' to assure that LACKA-IoT can be made highly secure against various potential attacks needed for an access control scheme in IoT environment.
- A detailed ''comparative study on the parameters, such as communication and computation costs, and security & functionality attributes has been performed on LACKA-IoT and other existing most relevant schemes in the literature, and this study shows that LACKA-IoT has a better trade-off among the considered parameters as compared to those for other schemes in the context of IoT''.
- Finally, the practical demonstration has been also carried out on LACKA-IoT for the important network performance parameters.

C. PAPER ORGANIZATION

The layout of this article is as follows. The related work on the access control mechanism related to IoT and its closed fields is provided in Section II. The detailed description of the proposed scheme (LACKA-IoT) is given in Section III. The formal & informal security analysis of LACKA-IoT is discussed in Section IV, while the ''formal security verification of LACKA-IoT using AVISPA tool'' is illustrated in Section V. Section VI gives a detailed comparative analysis of LACKA-IoT and other schemes. NS2-based simulation for LACKA-IoT is provided in Section VII for practical demonstration purpose, while the concluding remarks are drawn in the final section (Section VIII).

II. RELATED WORK

In the following, we briefly review device access control mechanisms in the IoT environment.

Jang *et al.* [28] proposed an efficient device authentication scheme which works without involvement of a central authority. Their scheme is based on the "Merkle hash-tree" in order to achieve authentication.

Sharaf-Dabbagh and Saad [29] designed an "authentication scheme for the IoT environment". In their scheme, the IoT smart devices use "fingerprinting mechanisms along with the transfer learning method". Their scheme is able to handle "emulation attacks effectively by differentiating normal changes in the fingerprints due to the environment from the changes done by an attacker".

Sciancalepore *et al.* [30] designed a "device authentication and key management scheme". Their scheme is based on the "implicit certificates with the ECC Diffie-Hellman key exchange protocol". Their scheme provides "replay attack protection", "fast re-keying" and "robust key negotiation".

Li *et al.* [31] designed an access control mechanism for wireless sensor networks (WSNs) in the context of the IoT environment by applying their proposed "heterogeneous signcryption scheme (CI-HSC) that permits a sender in the certificateless cryptography (CLC) environment to send a message to a receiver in the identity-based cryptography (IBC) environment". Their mechanism relies on the "identity-based access control (IBAC)" model. In addition, their scheme uses bilinear pairing operations. Their scheme is then costly in terms of computation overheads due to utilization of IBC and bilinear pairing operations. Furthermore, in this scheme, the *GWN* involves in the access control mechanism between two IoT smart devices.

Braeken *et al.* [32] presented "an efficient and distributed authentication protocol (eDAAAS) in order to access end-nodes in an IoT setting for smart homes, authorized by the home owner". eDAAAS is based on "symmetric cryptosystem" and "one-way cryptographic hash function". Though eDAAAS achieves very low computation cost, its communication cost is high. Moreover, in eDAAAS, the *GWN* involves in the access control mechanism between two IoT smart devices.

Luo *et al.* [33] proposed "an efficient access control protocol for WSNs in the cross-domain context of the IoT that permits an Internet user in a CLC environment to communicate with a smart device in an IBC environment with different system parameters". Their scheme is then costly in terms of computation overheads due to utilization of IBC and bilinear pairing operations. In addition, this scheme needs involvement of the *GWN* in the access control mechanism between two devices. Moreover, all the schemes [31]–[33] are vulnerable to the session key security under the "current *de facto* CK-adversary model [44], [45] (discussed in the attack model in Section I-A2)".

III. THE PROPOSED DEVICE ACCESS CONTROL AND KEY AGREEMENT PROTOCOL

In this section, we present an efficient protocol for device access control and key agreement, called LACKA-IoT, in the IoT environment. LACKA-IoT is lightweight as it utilizes "ECC primitives and one-way cryptpographic hash function". To ensure resilience against replay attacks, current timestamps are utilized in LACKA-IoT. Thus, the clocks of all involved entities are assumed to be synchronized. This is a typical assumption in the literature, such as the schemes presented in [2], [4], [51]–[53]. Furthermore, the notations with their significance tabulated in Table 2 are utilized in describing as well as analyzing LACKA-IoT.

TABLE 2. Notations and their description.

Symbol	Significance
CA	Trusted "certification authority"
D_i, ID_i	i^{th} IoT smart device and its identity, respectively
D_j, ID_j	j^{th} IoT smart device and its identity, respectively
GWN	Gateway node
p	A large prime
Z_p	A finite field, $Z_p = \{0, 1, \cdots, p-1\}$
$E_p(a, b)$	Non-singular elliptic curve: $y^2 = x^3 + ax + b \pmod p$; $a, b \in Z_p$ are constants with the condition $4a^3 + 27b^2 \neq 0 \pmod p$
P	A base point in $E_p(a, b)$
$x \cdot P$	ECC scalar (point) multiplication of the point $P \in E_p(a, b)$, $x \cdot P = P + P + \cdots + P$ (x times), $x \in Z_p^*$
$P + Q$	Elliptic curve point addition, $P, Q \in E_p(a, b)$
(x_{CA}, Q_{CA})	Private and public keys pair of the CA, respectively, $Q_{CA} = x_{CA} \cdot P$
(x_i, Q_i)	Private and public keys pair of D_i, respectively, $Q_i = x_i \cdot P$
c_i	D_i's certificate generated by the CA
z_i	D_i's signature signed by its private key x_i
(x_j, Q_j)	Private and public keys pair of D_j, respectively, $Q_j = x_j \cdot P$
c_j	D_j's certificate generated by the CA
z_j	D_j's signature signed by its private key x_j
T_i, T_j, T_i'	Current timestamps generated by D_i and D_j
ΔT	"Maximum allowable transmission delay associated with a message"
$D_i \rightarrow D_j: Msg$	Message Msg is sent by device D_i to device D_j via public channel
SK_{ij}	"Session key shared between the devices D_i and D_j"
$H(\cdot)$	"Collision-resistant one-way cryptographic hash function"
$\oplus, \|$	Bitwise XOR & concatenation operations, respectively
$\mathcal{A}$	Passive/active adversary

LACKA-IoT contains the following phases:

- **System setup phase:** This phase is executed by the trusted certification authority (*CA*) for selecting the system parameters.
- **Device registration phase:** This phase is executed by the *CA* for registration of an IoT smart device D_i belonging to a particular gateway node (*GWN*) depending on the IoT applications as shown in Figure 1. The secret credentials including the certificate are pre-loaded into D_i's memory before it is placed in the IoT environment.
- **Device access control phase:** This phase is responsible for performing authentication between two neighbor IoT smart devices using the pre-loaded credentials including the certificates. At the end of successful mutual authentication, the devices also establish a secret key between them for their secure communications.
- **Dynamic device addition phase:** Sometimes some IoT devices may be physically captured by an adversary due to hostile environment in some IoT applications,

such as healthcare application where an IoT device may be stolen. There may be other possibility that some IoT devices may drain out their power due to resource limitation of battery. Hence, it is also essential to deploy some new IoT devices in the network to continue the secure services.

The detailed descriptions of the above phases are explained in the following subsections.

A. SYSTEM SETUP PHASE

The *CA* performs the system setup phase using the following steps:

- **Step S1.** The CA chooses a ''non-singular elliptic curve $E_p(a, b)$ over a prime finite field Z_p'', where p being a large prime with the condition that $4a^3 + 27b^2 \neq 0 \pmod{p}$ is met. The *CA* then selects a base point P of order n over $E_p(a, b)$ such that $n \cdot P = \mathcal{O}$, where $\mathcal{O}$ is the ''zero point or point at infinity''.
- **Step S2.** The *CA* picks its own private key x_{CA} and calculates the corresponding public key $Q_{CA} = x_{CA} \cdot P$. Here $x_{CA} \cdot P = P + P + \cdots + P$ (x_{CA} *times*) is known as the ''elliptic curve point multiplication or scalar multiplication''.
- **Step S3.** The CA also picks a ''collision-resistant one-way cryptographic hash function'', say $H(\cdot)$.
- **Step S4.** Finally, the system parameters $\{E_p(a, b), p, P, H(\cdot), Q_{CA}\}$ are made public, whereas x_{CA} is considered as the private key that is maintained by the *CA* only.

B. DEVICE REGISTRATION PHASE

All the IoT smart devices, say D_i are registered in offline mode by the *CA* as follows.

- **Step R1.** For each smart device D_i, the *CA* picks a unique identity ID_i, and a unique private key x_i to calculate the corresponding public key $Q_i = x_i \cdot P$. The *CA* also generates a distinct random number l_i for each smart device D_i and computes the following:

$$A_i = (x_i + l_i) \cdot P,$$
$$c_i = x_{CA} + (x_i + l_i)H(ID_i||A_i),$$

  where c_i is known as the certificate of D_i that is generated by the *CA*.
- **Step R2.** The *CA* then pre-loads $\{ID_i, x_i, A_i, c_i, Q_i\}$ in the memory of D_i and declares Q_i as public. It is worth noting that the public system parameters $\{E_p(a, b), p, P, H(\cdot), Q_{CA}\}$ are also available to each device D_i.

C. DEVICE ACCESS CONTROL PHASE

In this phase, two neighbor IoT smart devices, say D_i and D_j will authenticate each other and then establish a secret key among them. The essential steps are as follows.

- **Step A1.** $D_i \rightarrow D_j$: $MSG_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$
  The device D_i first generates current timestamp T_i and a random number r_i. Further, it computes $R_i = r_i \cdot P$ and $z_i = c_i + H(A_i||c_i||R_i||Q_i||T_i)(r_i + x_i)$ as signature on r_i, and then dispatches the ''authentication request message'' $MSG_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$ to its neighbor device D_j via open channel.
- **Step A2.** $D_j \rightarrow D_i$: $MSG_2 = \{ID_j, A_j, c_j, T_j, z_j, R_j, SKV_{ij}, Q_j\}$
  The device D_j receives the ''authentication request message'' MSG_1 from the device D_i and checks the validity of timestamp T_i by using the criteria $|T_i^* - T_i| < \Delta T$, where T_i^* is receiving time of the message MSG_1 and ΔT is ''maximum transmission delay allowed'' for the message. If it fails, the phase is immediately terminated by D_j. Otherwise, D_j calculates

$$U_j = Q_{CA} + H(ID_i||A_i)A_i$$

  and checks if $U_j = c_i \cdot P$. If it is true, it is confirmed that the certificate c_i is issued by the *CA* genuinely for device D_i. D_j further calculates

$$W_j = c_i \cdot P + H(A_i||c_i||R_i||Q_i||T_i)(R_i + Q_i)$$

  and checks if $W_j = z_i \cdot P$. If the signature is valid, it is confirmed that the signature was genuinely generated by D_i. After that D_j generates a random number r_j and current timestamp T_j to compute the following:

$$R_j = r_j \cdot P,$$
$$z_j = c_j + H(A_j||c_j||R_j||Q_j||T_j)(r_j + x_j),$$
$$B_{ij} = r_j R_i = (r_i r_j) \cdot P,$$
$$K_{ij} = x_j Q_i = (x_i x_j) \cdot P,$$

  the session key shared with D_i as

$$SK_{ij} = H(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$$

  and its verifier as $SKV_{ij} = H(SK_{ij}||T_j)$.
  D_j then transmits the ''authentication reply message'' $MSG_2 = \{ID_j, A_j, c_j, T_j, z_j, R_j, SKV_{ij}, Q_j\}$ to the device D_i via open channel.
- **Step A3.** $D_i \rightarrow D_j$: $MSG_3 = \{SKV'_{ij}, T'_i\}$
  The device D_i receives the ''authentication reply message'' MSG_2 from the device D_j and checks the validity of timestamp T_j by applying the criteria $|T_j^* - T_j| < \Delta T$, where T_j^* is receiving time of the message MSG_2. If it fails, the phase is immediately terminated by D_i. Otherwise, D_i calculates

$$U_i = Q_{CA} + H(ID_j||A_j)A_j$$

  and checks if $U_i = c_j \cdot P$. If it is true, it is confirmed that certificate c_j is genuine and it was issued by the *CA* only. D_i then calculates

$$W_i = c_j \cdot P + H(A_j||c_j||R_j||Q_j||T_j)(R_j + Q_j)$$

  and checks if $W_i = z_j \cdot P$. If it is true, it is also confirmed that signature z_j is generated by D_j only. In addition, D_i computes

$$B'_{ij} = r_i R_j = (r_i r_j) \cdot P,$$
$$K'_{ij} = x_i Q_j = (x_i x_j) \cdot P,$$

Smart Device (D_i) $\{ID_i, x_i, A_i, c_i, Q_i\}$	Smart Device (D_j) $\{ID_j, x_j, A_j, c_j, Q_j\}$
Generates current timestamp T_i and random number r_i. Compute $R_i = r_i \cdot P$ and signature on r_i as $z_i = c_i + H(A_i \|\|c_i \|\|R_i \|\|Q_i \|\|T_i)\ (r_i + x_i)$. $MSG_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$ $\longrightarrow$ (via open channel)	
	Check if $\|T_i^* - T_i\| < \Delta T$? If it is valid, calculate $U_j = Q_{CA} + H(ID_i \|\| A_i)A_i$. Check validity of $U_j = c_i \cdot P$. If so, calculate $W_j = c_i \cdot P + H(A_i \|\| c_i \|\| R_i \|\| Q_i \|\| T_i)(R_i + Q_i)$. Check if $W_j = z_i \cdot P$? If so, generate random number r_j and current timestamp T_j. Calculate $R_j = r_j \cdot P$, $z_j = c_j + H(A_j \|\| c_j \|\| R_j \|\| Q_j \|\| T_j)(r_j + x_j)$, $B_{ij} = r_j R_i = (r_i r_j) \cdot P$, $K_{ij} = x_j Q_i = (x_i x_j) \cdot P$, $SK_{ij} = H(B_{ij} \|\| K_{ij} \|\| T_i \|\| T_j \|\| ID_i \|\| ID_j)$, $SKV_{ij} = H(SK_{ij} \|\| T_j)$. $MSG_2 = \{ID_j, A_j, c_j, T_j, z_j, R_j, SKV_{ij}, Q_j\}$ $\longleftarrow$ (via open channel)
Check if $\|T_j^* - T_j\| < \Delta T$? If so, compute $U_i = Q_{CA} + H(ID_j \|\| A_j)A_j$. Check if $U_i = c_j \cdot P$? If so, compute $W_i = c_j \cdot P + H(A_j \|\| c_j \|\| R_j \|\| Q_j \|\| T_j)(R_j + Q_j)$. Verify if $W_i = z_j \cdot P$? If valid, compute $B'_{ij} = r_i R_j = (r_i r_j) \cdot P$, $K'_{ij} = x_i Q_j = (x_i x_j) \cdot P$, $SK'_{ij} = H(B'_{ij} \|\| K'_{ij} \|\| T_i \|\| T_j \|\| ID_i \|\| ID_j)$. Verify if $SKV_{ij} = H(SK'_{ij} \|\| T_j)$? If so, generate current timestamp T'_i. Compute $SKV'_{ij} = H(SK'_{ij} \|\| T'_i)$. $MSG_3 = \{SKV'_{ij}, T'_i\}$ $\longrightarrow$ (via open channel)	
	Check validity of received timestamp T'_i. If so, compute $SKV^*_{ij} = H(SK_{ij} \|\| T'_i)$. Verify whether $SKV'_{ij} = SKV^*_{ij}$? If so, session key is also authenticated.
Both D_i and D_j maintain session key (secret key) SK_{ij} $(= SK'_{ij})$.	

FIGURE 2. **Summary of device access control phase between D_i and D_j.**

the session key as

$$SK'_{ij} = H(B'_{ij} || K'_{ij} || T_i || T_j || ID_i || ID_j).$$

If the condition $SKV_{ij} = H(SK'_{ij} || T_j)$ is valid, D_i further generates current timestamp T'_i and computes $SKV'_{ij} = H(SK'_{ij} || T'_i)$, and then transmits the "authentication acknowledgment message" $MSG_3 = \{SKV'_{ij}, T'_i\}$ to the device D_j via open channel.

- **Step A4.** The device D_j receives the "authentication acknowledgment message" MSG_3 and checks the validity of the timestamp T'_i attached in the message. If it is a valid timestamp, D_j continues to calculate $SKV^*_{ij} = H(SK_{ij} || T'_i)$ using its previously computed session key SK_{ij} in Step A2, and further validates if $SKV'_{ij} = SKV^*_{ij}$. If it fails, the phase is terminated by D_j. Otherwise, the "mutual authentication between D_i and D_j" is successful, and both D_i and D_j store the same session key SK_{ij} $(= SK'_{ij})$ for their secure communication.

The entire phase is briefed in Figure 2.

Remark 1: In order to create secret keys between the smart devices D_i and its nearby gateway node (GWN), the CA needs to pick a unique identity ID_{gwn}, and a unique private key x_{gwn} for calculating the corresponding public key $Q_{gwn} = x_{gwn} \cdot P$

Certification Authority (CA)
For a new IoT smart device D_i^{new} deployment: Pick unique identity ID_i^{new} & unique private key x_i^{new}. Compute public key $Q_i^{new} = x_i^{new} \cdot P$. Choose random number l_i^{new}. Calculate $A_i^{new} = (x_i^{new} + l_i^{new}) \cdot P$, $c_i^{new} = x_{CA} + (x_i^{new} + l_i^{new})H(ID_i^{new}\|\|A_i^{new})$. Pre-load the information $\{ID_i^{new}, x_i^{new}, A_i^{new}, c_i^{new}\}$ in the memory of D_i^{new}. Declare Q_i^{new} as public.

FIGURE 3. Summary of dynamic device addition phase for a new IoT smart device D_i^{new}.

for the *GWN*. Next, the *CA* needs to generate a distinct random number l_{gwn} for the *GWN* to compute the following:

$$A_{gwn} = (x_{gwn} + l_{gwn}) \cdot P,$$
$$c_{gwn} = x_{CA} + (x_{gwn} + l_{gwn})H(ID_{gwn}||A_{gwn}),$$

where c_{gwn} is the certificate of *GWN* generated by the *CA*. Then, the *CA* will store the credentials $\{ID_{gwn}, x_{gwn}, A_{gwn}, c_{gwn}, Q_{gwn}\}$ in the *GWN*'s database and declares Q_{gwn} as public. The public system parameters $\{E_p(a, b), p, P, H(\cdot), Q_{CA}\}$ are also accessible to the *GWN*. For authenticating and establishing secret key between a smart device D_i and its nearby gateway node *GWN*, they will follow the access control phase described in Section III-C.

D. DYNAMIC DEVICE ADDITION PHASE

Suppose a new IoT smart device, say D_i^{new} needs to be placed in the network after initial deployment. This is achieved by the *CA* through the following steps in offline mode:

- **Step DA1.** The *CA* picks a "unique identity" ID_i^{new} and a "unique private key" x_i^{new} to calculate its respective public key $Q_i^{new} = x_i^{new} \cdot P$. It then picks a random number l_i^{new} and calculates

$$A_i^{new} = (x_i^{new} + l_i^{new}) \cdot P,$$
$$c_i^{new} = x_{CA} + (x_i^{new} + l_i^{new})H(ID_i^{new}||A_i^{new}),$$

  where c_i^{new} is the certificate generated by the *CA* for the device D_i^{new}.
- **Step DA2.** The *CA* then pre-loads $\{ID_i^{new}, x_i^{new}, A_i^{new}, c_i^{new}\}$ in the memory of D_i^{new} and declares Q_i^{new} as public. Note that the public system parameters $\{E_p(a, b), p, P, H(\cdot), Q_{CA}\}$ are also accessible to the device D_i^{new}.

After deployment of D_i^{new} in the IoT environment, it will then start authentication with its neighbor smart devices and establish secret keys with them using its own pre-loaded credentials including the certificate with the help of the "device access control phase described in Section III-C".

This phase is also summarized in Figure 3.

IV. SECURITY ANALYSIS

This section covers both formal and informal security analysis on the proposed LACKA-IoT. We define the "collision-resistant cryptographic one-way hash function" and "Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP)" as follows.

Definition 1 (Collision-Resistant Cryptographic One-Way Hash Function): A "collision-resistant cryptographic one-way hash function" H: $\{0, 1\}^* \rightarrow \{0, 1\}^n$ is a "deterministic mathematical function that takes a variable length input string and produces a fixed length output string of n bits". If $Adv_{(A)}^{HASH}(rt)$ is the "advantage of an adversary $\mathcal{A}$ in finding a hash collision", we have

$$Adv_{(A)}^{HASH}(rt) = Pr[(inp_1, inp_2) \in_R \mathcal{A} : inp_1 \neq inp_2, H(inp_1) = H(inp_2)],$$

where the "probability of a random event X" is $Pr[X]$, and "pair $(inp_1, inp_2) \in_R \mathcal{A}$ indicates that the input strings inp_1 and inp_2 are randomly picked by $\mathcal{A}$". An (ϵ, rt)-adversary $\mathcal{A}$ attacking the "collision resistance of $H(\cdot)$" indicates that "the runtime of $\mathcal{A}$ is at most rt and that $Adv_{(A)}^{HASH}(rt) \leq \epsilon$".

Definition 2 (Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP)): Let $P \in E_p(a, b)$ be a point on an elliptic curve $E_p(a, b)$. The ECDDHP is that "given a quadruple $(P, k_1.P, k_2.P, k_3.P)$, decide whether $k_3 = k_1\, k_2$ or a uniform value, where $k_1, k_2, k_3 \in Z_p^*$ and $Z_p^* = \{1, 2, \ldots, p-1\}$".

The ECDDHP becomes "computationally infeasible" when p is chosen large. For intractability of ECDDHP, p should be chosen at least 160-bit prime.

A. ROR-MODEL BASED FORMAL SECURITY ANALYSIS

We apply the "widely-accepted Real-Or-Random (ROR) model" [49] to prove its semantic security. Through the ROR model, we prove that the proposed LACKA-IoT achieves the "session key security (SK-security)". For this purpose, we briefly discuss the ROR model and then prove the SK-security in Theorem 1.

Under the ROR model, an adversary $\mathcal{A}$ interconnects with the t^{th} instance of an executing entity (participant), say $\mathcal{P}^t$. In the proposed LACKA-IoT, the device D_i or D_j can be treated as $\mathcal{P}^t$. Assume that $\mathcal{P}_{D_i}^{t_1}$ and $\mathcal{P}_{D_j}^{t_2}$ denote the t_1^{th} and t_2^{th} instances of D_i and D_j, respectively. In addition, the ROR model takes into consideration of different queries simulating a real (actual) attack, such as *Execute*, *Reveal* and *Test* queries that are tabulated in Table 3. Furthermore, a "collision-resistant cryptographic one-way hash function $H(\cdot)$ is modeled as a random oracle, say *Hash*", which is also accessible by all the participants including the adversary $\mathcal{A}$.

In the following, we prove that the proposed LACKA-IoT achieves the SK-security.

Theorem 1: Assume that an adversary $\mathcal{A}$ runs in "polynomial time t" against the proposed LACKA-IoT, and q_{hash}, $|Hash|$ and $Adv_{\mathcal{A}}^{ECDDHP}(t)$ denote "the number of hash queries, the range space of one-way hash function $H(\cdot)$ and the $\mathcal{A}$'s advantage in breaking ECDDHP", respectively.

TABLE 3. Various queries and their explanation.

Query	Explanation
$Execute(\mathcal{P}_{D_i}^{t_1}, \mathcal{P}_{D_j}^{t_2})$	It makes $\mathcal{A}$ to eavesdrop (intercept) the messages exchanged between D_i and D_j
$Reveal(\mathcal{P}^t)$	With this query execution, the present session key SK_{ij} between $\mathcal{P}^t$ and its partner to $\mathcal{A}$ is revealed
$Test(\mathcal{P}^t)$	$\mathcal{A}$ pleas $\mathcal{P}^t$ for the session key SK_{ij} and $\mathcal{P}^t$ replies a probabilistic outcome of a flipped unbiased coin c

Then, $\mathcal{A}$'s "advantage in breaking LACKA-IoT's semantic security to derive the session key SK_{ij} between any two neighbor IoT smart devices D_i and D_j during the access control phase (Section III-C)" can be approximated by

$$Adv_{\mathcal{A}}^{LACKA-IoT}(t) \leq \frac{q_{hash}^2}{|Hash|} + 2\,Adv_{\mathcal{A}}^{ECDDHP}(t).$$

Proof 1: The proof of this theorem is similar to that as presented in other schemes [2], [4], [52]. We consider the following three games, say $G_j, j \in [0, 2]$, where $Succ_{\mathcal{A}}^{G_j}$ will represent as "the success probability of an event wherein $\mathcal{A}$ can guess the random bit c in the G_j correctly". We then denote "advantage of $\mathcal{A}$ in winning the game G_j by $Adv_{\mathcal{A},G_j}^{LACKA-IoT} = Pr[Succ_{\mathcal{A}}^{G_j}]$".

The details of the games $G_j, j \in [0, 2]$ are outlined below.

- **Game** G_0: This is the "real attack executed by $\mathcal{A}$ against our proposed LACKA-IoT in the ROR model" corresponding to the game G_0. The bit c is picked randomly at the beginning of the G_0. Hence, the following result is followed:

$$Adv_{\mathcal{A}}^{LACKA-IoT}(t) = |2.Adv_{\mathcal{A},G_0}^{LACKA-IoT} - 1| \quad (1)$$

- **Game** G_1: This game corresponds to "an eavesdropping attack" in which $\mathcal{A}$ can intercept all the communicated messages $MSG_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$, $MSG_2 = \{ID_j, A_j, c_j, T_j, z_j, R_j, SKV_{ij}, Q_j\}$ and $MSG_3 = \{SKV'_{ij}, T'_i\}$ during the access control phase (Section III-C) using the *Execute* query mentioned in Table 3. At the end of the game, $\mathcal{A}$ requires to execute the *Reveal* and *Test* queries in order to check "if the derived session key SK_{ij} between D_i and D_j is real or a random key". Note that the session key SK_{ij} between D_i and D_j is calculated as $SK_{ij} = H(B_{ij}||K_{ij}||T_i||T_j||ID_i||ID_j)$ $(= H(B'_{ij}||K'_{ij}||T_i||T_j||ID_i||ID_j))$. It is worth noting that to calculate SK_{ij}, $\mathcal{A}$ requires the temporal (short term) secrets (r_i and r_j) and long term secrets (x_i and x_j) that are not known to $\mathcal{A}$. Therefore, it is evident that only eavesdropping of the messages MSG_1, MSG_2 and MSG_3 does not increase the game G_1's winning probability of $\mathcal{A}$. Since two games G_0 and G_1 are indistinguishable, it follows that

$$Adv_{\mathcal{A},G_1}^{LACKA-IoT} = Adv_{\mathcal{A},G_0}^{LACKA-IoT} \quad (2)$$

- **Game** G_2: In this game, the simulation of the *Hash* query is included so that it can be modeled as "an active attack". In the message MSG_1, the terms z_i and c_i are safeguarded by the "collision-resistant cryptographic one-way hash function $H(\cdot)$ (see Definition 1)". In the message MSG_2, the terms c_j, z_j and SKV_{ij} are protected by $H(\cdot)$. In the message MSG_3, the term SKV'_{ij} is also protected by $H(\cdot)$. Again, from the intercepted $R_i = r_i.P$ and $R_j = r_j.P$, it is "computationally infeasible problem" for the adversary $\mathcal{A}$ to derive $B_{ij} = B'_{ij} = (r_i r_j).P$ due to intractability of ECDDHP (see Definition 2). In a similar way, from the intercepted $Q_i = x_i.P$ and $Q_j = x_j.P$, it is also "computationally infeasible problem" for $\mathcal{A}$ to derive $K_{ij} = K'_{ij} = (x_i x_j).P$ due to intractability of ECDDHP. Hence, to derive the session key SK_{ij} between devices D_i and D_j the adversary $\mathcal{A}$ requires both B_{ij} $(= B'_{ij})$ and K_{ij} $(= K'_{ij})$ which are difficult task as $\mathcal{A}$ needs to solve ECDDHP in polynomial time t. Moreover, deriving r_i and x_i from the intercepted z_i, and r_j and x_j from the intercepted z_j are "computationally infeasible problem" due to "collision-resistant property of $H(\cdot)$". As all the random numbers, current timestamps, identities and secret credentials are used in the messages MSG_1, MSG_2 and MSG_3, no collision occurs if the *Hash* query is executed by $\mathcal{A}$. It is worth noting that both the games G_1 and G_2 are "indistinguishable" except the inclusion of the simulation of the *Hash* query in G_2. With the application of the results obtained from the birthday paradox and the intractability of ECDDHP, we get the following result:

$$|Adv_{\mathcal{A},G_1}^{LACKA-IoT} - Adv_{\mathcal{A},G_2}^{LACKA-IoT}| \leq \frac{q_{hash}^2}{2|Hash|} + Adv_{\mathcal{A}}^{ECDDHP}(t) \quad (3)$$

All the queries are now simulated by $\mathcal{A}$ and it is "only left with guessing the bit c in order to win the game once the *Reveal* query along with *Test* query are executed". It follows that

$$Adv_{\mathcal{A},G_2}^{LACKA-IoT} = \frac{1}{2} \quad (4)$$

Eqs. (1) and (2) give

$$\frac{1}{2}.Adv_{\mathcal{A}}^{LACKA-IoT}(t) = |Adv_{\mathcal{A},G_0}^{LACKA-IoT} - \frac{1}{2}| = |Adv_{\mathcal{A},G_1}^{LACKA-IoT} - \frac{1}{2}| \quad (5)$$

Further, Eqs. (3), (4) and (5) lead to the following result:

$$\frac{1}{2}.Adv_{\mathcal{A}}^{LACKA-IoT}(t) = |Adv_{\mathcal{A},G_1}^{LACKA-IoT} - Adv_{\mathcal{A},G_2}^{LACKA-IoT}| \leq \frac{q_{hash}^2}{2|Hash|} + Adv_{\mathcal{A}}^{ECDDHP}(t) \quad (6)$$

Finally, multiplying both sides of Eq. (6) by a factor of 2, we arrive to the required result:

$$Adv_{\mathcal{A}}^{LACKA-IoT}(t) \leq \frac{q_{hash}^2}{|Hash|} + 2\,Adv_{\mathcal{A}}^{ECDDHP}(t).$$

B. INFORMAL SECURITY ANALYSIS AND OTHER DISCUSSIONS

This section shows how the proposed LACKA-IoT can resist other known attacks that are needed for securing IoT environment through access control mechanism.

Proposition 1: LACKA-IoT is secure against the replay attack.

Proof 2: During the access control phase (Section III-C), all the exchanged messages $MSG_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$, $MSG_2 = \{ID_j, A_j, c_j, T_j, z_j, R_j, SKV_{ij}, Q_j\}$ and $MSG_3 = \{SKV'_{ij}, T'_i\}$ involve the random numbers and current timestamps. The validation of the received timestamps T_i, T_j and T'_i by the respective communicating parties assures whether the messages are fresh or old ones. Since ΔT is usually small, the probability of replaying the same messages MSG_1, MSG_2 and MSG_3 within the period ΔT by an adversary is negligible. Thus, the "replay attack protection" is achieved in LACKA-IoT.

Proposition 2: LACKA-IoT is secure against the man-in-the-middle attack.

Proof 3: Suppose an adversary $\mathcal{A}$ intercepts the messages $MSG_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$, $MSG_2 = \{ID_j, A_j, c_j, T_j, z_j, R_j, SKV_{ij}, Q_j\}$ and $MSG_3 = \{SKV'_{ij}, T'_i\}$ during communication between the devices D_i and D_j. Assume that $\mathcal{A}$ wants to modify the message MSG_1 to make it another valid message so that the device D_j is forced to believe that the modified message is legitimate. For doing so, $\mathcal{A}$ can generate a random number r_a and current timestamp T_a to compute $R_a = r_a.P$. However, $\mathcal{A}$ cannot compute $z_a = c_i + H(A_i || c_i || R_a || Q_i || T_a)(r_a + x_i)$ as the private key x_i of D_i is unknown. Thus, formation of a valid message of the form $MSG'_1 = \{ID_i, A_i, c_i, T_a, z_a, R_a, Q_i\}$ is "computationally infeasible task" for the adversary $\mathcal{A}$. The similar situation arises for modifying other messages MSG_2 and MSG_3 too. This clearly implies that the "man-in-the-middle attack protection" is achieved in LACKA-IoT.

Proposition 3: LACKA-IoT is secure against the device impersonation attack.

Proof 4: In the "device impersonation attack", an adversary $\mathcal{A}$ will try to create a valid message on behalf of a device (D_i or D_j) and convince the other device that the message is generated by its neighbor legitimate device only. Assume that $\mathcal{A}$ wants to impersonate the device D_j to other device D_i. For doing this, $\mathcal{A}$ intercepts the message $MSG_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$ and will try to create the valid message MSG_2. Assume that $\mathcal{A}$ generates a random number r_a and current timestamp T_a to calculate $R_a = r_a.P$ and $B'_{ij} = r_a.R_i = (r_i r_a).P$. However, $\mathcal{A}$ cannot calculate $K_{ij} = x_j Q_i$ and $z_a = c_j + H(A_j || c_j || R_a || Q_j || T_a)(r_a + x_j)$ as the private key x_i of D_i is unknown. In addition, $\mathcal{A}$ cannot calculate the session key and its verifier. Thus, formation of valid message of the form $MSG'_2 = \{ID_j, A_j, c_j, T_a, z_a, R_a, SKV_{ij}, Q_j\}$ is "computationally infeasible task" for the adversary $\mathcal{A}$. In a similar manner, $\mathcal{A}$ cannot also create valid messages MSG_1 and MSG_3 on behalf of the device D_i to fool the device D_j. Hence, LACKA-IoT is secure against the "device impersonation attacks".

Proposition 4: LACKA-IoT is secure against the malicious device deployment attack.

Proof 5: Suppose an adversary $\mathcal{A}$ wants to deploy a fake (malicious) smart device D_f in the existing IoT network so that D_f can establish secret keys with its neighbor devices and send fake information. For this purpose, suppose $\mathcal{A}$ picks a fake identity ID_f and a private key x_f to calculate its corresponding public key $Q_f = x_f.P$. $\mathcal{A}$ can then generate a random number l_f to calculate $A_f = (x_f + l_f).P$. However, $\mathcal{A}$ will not be able to compute the certificate for D_f on behalf of the CA of the form $c_f = x_{CA} + (x_f + l_f)H(ID_f || A_f)$ because the private key x_{CA} is only known to the CA. This means that the deployment of D_f with fake information $\{ID_f, x_f, A_f, c_f\}$ is not possible by $\mathcal{A}$. Hence, LACKA-IoT is secure against the "malicious device deployment attack".

Proposition 5: LACKA-IoT is resilient against the device physical capture attack.

Proof 6: We assume that n_d smart devices are physically captured by an adversary $\mathcal{A}$ as the devices are placed in "unattended/hostile environment" in some IoT applications (e.g., healthcare and military). Therefore, once a device, say D_i is captured, $\mathcal{A}$ can easily extract all the credentials $\{ID_i, x_i, A_i, c_i, Q_i\}$ from the memory of D_i by utilizing the power analysis attacks [47], [48] as explained in the attack model (Section I-A2). It is also worth noticing that the credentials $\{ID_j, x_j, A_j, c_j, Q_j\}$ loaded in the memory of other devices D_j are completely distinct and unique throughout the network as compared to those for the compromised credentials $\{ID_i, x_i, A_i, c_i, Q_i\}$ of captured device D_i. The compromised credentials $\{ID_i, x_i, A_i, c_i, Q_i\}$ do not then help in computing the secret keys SK_{jk} between any two non-compromised smart devices D_j and D_k in the network. This means that "compromise of n_d devices do not lead to compromise the secure communications among the non-compromised devices in the network by the adversary $\mathcal{A}$". This property is known as "unconditional security against device physical capture attack". As a result, LACKA-IoT is resilient against the "device physical capture attack".

Proposition 6: LACKA-IoT is secure against the Ephemeral Secret Leakage (ESL) attack.

Proof 7: In our proposed LACKA-IoT, the established secret key between two neighbor smart devices D_i and D_j during the access control phase (Section III-C) is $SK_{ij} = H(B_{ij} || K_{ij} || T_i || T_j || ID_i || ID_j)$ $(= H(B'_{ij} || K'_{ij} || T_i || T_j || ID_i || ID_j) = SK'_{ij})$. This session key is dependent on both the "session-temporary (ephemeral or short term) secrets" r_i and r_j, and the long-term secrets x_i and x_j. The following two cases are considered here:

- **Case I:** Even if the short term secrets r_i and r_j are revealed through compromise of session states according to the CK-adversary model discussed in the attack model (Section I-A2) to an adversary $\mathcal{A}$, it is "computationally difficult task to compute the secret key SK_{ij} without having the long-term secrets x_i and x_j".

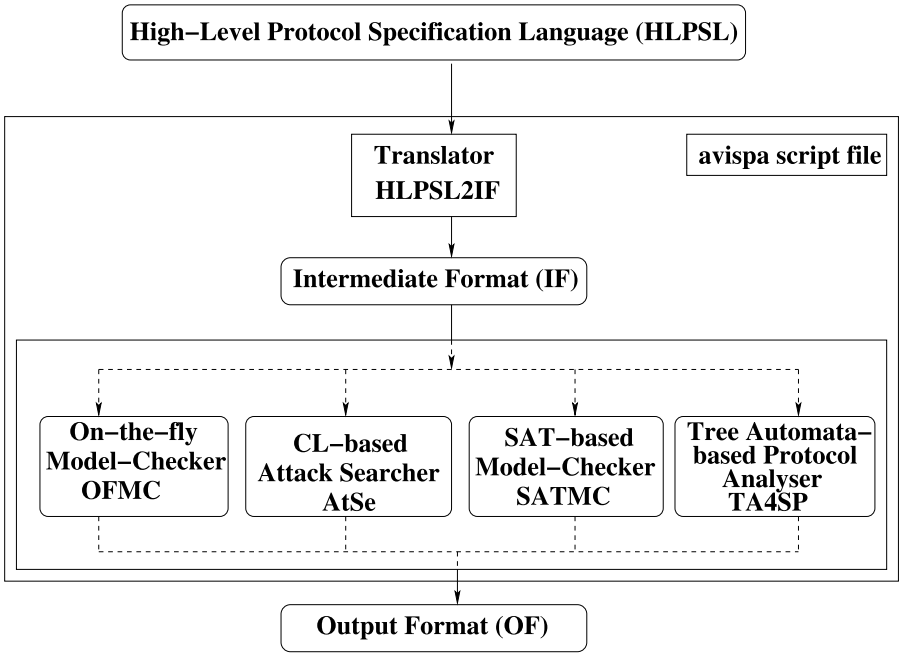

FIGURE 4. Architecture of AVISPA [50].

- **Case II:** Even if the long term secrets x_i and x_j are somehow known to $\mathcal{A}$, it is also ''computationally difficult task to compute the secret key SK_{ij} without having the short-term secrets r_i and r_j''.

Therefore, it is clear from the above two cases that the session key SK_{ij} is only computed if $\mathcal{A}$ compromises both short & long term secrets. Since the secret keys between any two devices are distinct, ''a secret key leakage to $\mathcal{A}$ in a session does not lead to derivation of other secret keys in other sessions and it is computationally infeasible task due to utilization of both short & long term secrets in construction of secret keys''. Furthermore, due to intractability of ECDDHP, it is ''computationally infeasible task for $\mathcal{A}$ to derive $K_{ij} = (x_i x_j).P$ from the intercepted Q_i and Q_j for constructing the secret key SK_{ij}''. Hence, the ''session-temporary information attack is protected in LACKA-IoT, and as a result, LACKA-IoT also preserves perfect forward secrecy''. Thus, LACKA-IoT is secure against ''ESL attack''.

V. FORMAL SECURITY VERIFICATION THROUGH AVISPA TOOL

In this section, we first briefly discuss the ''widely-accepted Automated Validation of Internet Security Protocols and Applications (AVISPA) tool [50] and its implementation details of the proposed device access control and key agreement scheme (LACKA-IoT) using the High-Level Protocol Specification Language (HLPSL) [54]''. Next, the analysis of simulation results using AVISPA is discussed.

AVISPA is treated as a ''push-button tool for the automated validation of Internet security-sensitive protocols and applications, which provides a modular and expressive formal language for specifying protocols and their security properties, and integrates different back-ends that implement a variety of state-of-the-art automatic analysis techniques [50]''. Figure 4 illustrates the architecture of AVISPA.

HLPSL is applied to implement a security protocol to check if the designed protocol is safe or unsafe. In AVISPA, there are four backends, which are listed below [50]:

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

The HLPSL code is first transferred into the ''Intermediate Format (IF)'' which is then given as input to one of the four backends. The IF then produces the ''Output Format (OF)''. The OF has the important characteristics: ''when the analysis of a security protocol has been successful (by finding an attack or not), the OF describes precisely what is the result, and under what conditions it has been

obtained [50]''. The OF has various sections as described below [50].

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

More details about AVISPA and its HLPSL implementation can be found in [50].

In our implementation of LACKA-IoT, we have three basic and two composition roles. The basic roles represent various participants in the protocol (the roles for the smart device D_i, smart device D_j and CA). The composition roles (session and goal & environment) are the mandatory roles that include various scenarios involving basic roles.

Three types of verification were done for the proposed LACKA-IoT: 1) ''executability checking on non-trivial HLPSL specifications''; 2) ''replay attack checking''; and 3) ''Dolev-Yao model checking using the DY model discussed in the attack model in Section I-A2''. The executability check ensures that ''the protocol will reach to a state where a possible attack can happen, during the run of the protocol''. The proposed LACKA-IoT was simulated for the ''execution tests and a bounded number of sessions model checking''. To check the ''replay attack on the proposed protocol (LACKA-IoT)'', the OFMC backend tests if ''the legitimate agents can execute the specified protocol by performing a search of a passive intruder''. This back-end then supplies ''the intruder (i) about the knowledge of some normal sessions between the valid agents''. OFMC backend also checks ''if any man-in-the-middle attack is possible by i for the Dolev-Yao model checking''.

We have used the broadly accepted ''SPAN (Security Protocol ANimator for AVISPA)'' tool [55] in order to perform the formal security verification part through simulation study on our proposed LACKA-IoT. The simulation results under the broadly-used OFMC backend shown in Figure 5 ensure that LACKA-IoT protects both replay & man-in-the-middle attacks.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  C:\progra~1\SPAN\testsuite
    \results\device_accesscontrol.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 59.53s
  visitedNodes: 28404 nodes
  depth: 6 plies
```

FIGURE 5. Analysis of simulation results under OFMC backend.

VI. COMPARATIVE ANALYSIS

This section evaluates the performance of the proposed LACKA-IoT with the relevant recent schemes, such as the schemes proposed by Luo *et al.* [33], Li *et al.* [31] and Braeken *et al.* [32] with respect to the following parameters: 1) ''communication costs'', 2) ''computation costs'', and 3) ''security & functionality attributes''.

A. COMMUNICATION COSTS COMPARISON

For ''comparison of communication costs among the proposed LACKA-IoT and other schemes'', it is assumed that an identity is 160 bits, a random number is 160 bits, hash output (if SHA-1 hashing algorithm [56] is applied) is 160 bits and timestamp is 32 bits. It is assumed that an elliptic curve point of the form $P = (P_x, P_y)$, with P_x and P_y denoting the x and y co-ordinates, respectively, is $(160 + 160) = 320$ bits as ''160-bit ECC security remains same as that for an 1024-bit RSA public key cryptosystem [57]''. Furthermore, it is assumed that a message size is 1024 bits.

In the proposed LACKA-IoT, the three messages $MSG_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$, $MSG_2 = \{ID_j, A_j, c_j, T_j, z_j, R_j, SKV_{ij}, Q_j\}$ and $MSG_3 = \{SKV'_{ij}, T'_i\}$ are exchanged between two IoT smart devices D_i and D_j which require the communication costs as $|MSG_1| = (160 + 320 + 160 + 32 + 160 + 320 + 320) = 1472$ bits, $|MSG_2| = (160 + 320 + 160 + 32 + 160 + 320 + 160 + 320) = 1632$ bits and $|MSG_3| = (160 + 32) = 192$ bits, respectively. As a result, total communication cost needed for LACKA-IoT is $\sum_{i=1}^{3} |MSG_i| = (1472 + 1632 + 192) = 3296$ bits.

Table 4 tabulates the ''comparative study on communication costs'' for the proposed LACKA-IoT and other schemes. The total communication costs needed for the schemes of Luo *et al.* [33], Li *et al.* [31] and Braeken *et al.* [32] are 3040 bits, 3488 bits and 3552 bits, respectively. LACKA-IoT demands less communication cost as compared to other schemes [31], [32]. Though the scheme [33] requires less communication cost as compared to LACKA-IoT, it fails to preserve or support several ''security and functionality attributes'' as mentioned in Table 6 while those are compared with LACKA-IoT.

TABLE 4. Comparison of communication costs.

Protocol	No. of messages	Total cost (in bits)
LACKA-IoT	3	3296
Luo *et al.* [33]	2	3040
Li *et al.* [31]	2	3488
Braeken *et al.* [32]	3	3552

B. COMPUTATION COSTS COMPARISON

To evaluate the ''computation costs comparison among the proposed LACKA-IoT and other schemes'', the following symbols are used: T_h to denote the ''time needed to execute a one-way cryptographic hash function'', T_{ecm} to denote the ''time needed to execute an elliptic curve point (scalar) multiplication'', T_{eca} to denote the ''time needed to execute an elliptic curve point addition'', T_{sed} to denote the ''time needed to execute a symmetric encryption/decryption function'', and T_{me} to denote ''time needed to execute a modular exponentiation operation in Z_p^*''. During the device access control phase of the proposed LACKA-IoT, the device D_i needs 7 T_{ecm} + 3 T_{eca} + 6 T_h computation cost, whereas its neighbor device D_j also requires 7 T_{ecm} + 3 T_{eca} + 6 T_h computation cost. Thus, the average computation cost needed for an IoT smart device for node authentication and also for establishment of secret key with one of its neighbor devices is 7 T_{ecm} + 3 T_{eca} + 6 T_h.

To estimate ''rough computation time (in milliseconds)'', we use the experimental results based the user's device in [58] as $T_{ecm} \approx 13.405$ ms, $T_{eca} \approx 0.081$ ms, $T_h \approx 0.056$ ms, $T_{bp} \approx 32.713$ ms, and $T_{me} \approx 2.249$ ms. We also assume that $T_{sed} \approx T_h$. In the proposed LACKA-IoT, a smart device's computation time becomes 7 T_{ecm} + 3 T_{eca} + 6 $T_h \approx$ 94.414 ms.

Table 5 tabulates the ''comparative study on computation costs and also rough estimated time in milliseconds'' for the proposed LACKA-IoT and other schemes. It is noted that LACKA-IoT demands less computation cost as compared with other schemes [31], [33]. On the other hand, the scheme [32] needs very less computation cost as compared to LACKA-IoT, Luo *et al.*'s scheme [33] and Li *et al.*'s scheme [31]. This is primarily because Braeken *et al.*'s scheme [32] is based on ''symmetric encryption/decryption'' and ''one-way hash function''. However, Braeken *et al.*'s scheme fails to preserve or support several ''security and functionality attributes'' as mentioned in Table 6 while those are compared with LACKA-IoT.

C. SECURITY AND FUNCTIONALITY ATTRIBUTES COMPARISON

Finally, in Table 6 we tabulate the comparative study on ''functionality & security attributes'' for the proposed LACKA-IoT and other schemes [31]–[33]. It is worth noting that all the compared existing schemes [31]–[33] do not support or preserve the attributes FSA_3, SFA_8, SFA_{10} and SFA_{11}. On the other hand, LACKA-IoT fulfills all the mentioned attributes FSA_1–FSA_{11}.

TABLE 5. Comparison of computation costs.

Protocol	Smart (sensing) device cost	Total cost	Total rough cost (in milliseconds)
LACKA-IoT	$7T_{ecm} + 6T_h$ $+3T_{eca}$	$7T_{ecm} + 6T_h$ $+3T_{eca}$	94.414
Luo *et al.* [33]	$T_{bp} + T_h$	$3T_{ecm} + 4T_{bp}+$ $4T_h + T_{eca} + T_{me}$	173.621
Li *et al.* [31]	$T_{bp} + T_h$	$3T_{ecm} + 5T_{bp}+$ $2T_h + 2T_{eca}$	204.054
Braeken *et al.* [32]	$11T_h + T_{sed}$	$23T_h + 2T_{sed}$	1.400

TABLE 6. Comparison of functionality & security attributes.

Attribute	Luo *et al.* [33]	Li *et al.* [31]	Braeken *et al.* [32]	LACKA-IoT
FSA_1	✓	✓	✓	✓
FSA_2	✓	✓	✓	✓
FSA_3	×	×	×	✓
SFA_4	✓	✓	✓	✓
SFA_5	✓	✓	✓	✓
SFA_6	✓	✓	✓	✓
SFA_7	✓	✓	✓	✓
SFA_8	×	×	×	✓
SFA_9	✓	✓	✓	✓
SFA_{10}	×	×	×	✓
FSA_{11}	×	×	×	✓

FSA_1: replay attack; FSA_2: man-in-the-middle attack; FSA_3: mutual authentication; FSA_4: key agreement; FSA_5: device impersonation attack; FSA_6: malicious device deployment attack; FSA_7: resilience against device physical capture attack; SFA_8: formal security verification using AVISPA tool; FSA_9: formal security analysis; FSA_{10}: whether works without involving gateway node during the authentication (access control) phase; FSA_{11}: ESL attack under the CK-adversary model.
✓: "a scheme is secure or it supports a functionality feature"; ×: "a scheme is insecure or it does not support a functionality feature".

VII. PRACTICAL PERSPECTIVE: NS2 SIMULATION STUDY

LACKA-IoT is simulated under the widely-used ''networking simulation tool, NS2 2.35 simulator'' [59] on the ''Ubuntu 16.04.5 LTS platform''.

A. SIMULATION PARAMETERS

The details of different parameters related to simulation are tabulated in Table 7. The ''network coverage area'' is taken as an 100 × 150 m^2 area. The ''communication ranges'' of the ''gateway node (*GWN*)'' and ''IoT smart devices'' are taken as 200 m and 50 m, respectively. Furthermore, the ''network simulation time'' is taken as 1800 seconds or 30 minutes. In addition, we have applied the standard ''Ad hoc On-Demand Distance Vector (AODV)'' protocol for the routing purpose.

B. SIMULATION ENVIRONMENT

The following three cases are taken into account during the simulation of the proposed LACKA-IoT. All the cases consider one *GWN*. Moreover, the remaining parameters are common in all the cases.

- **Case 1.** Under this case, five IoT smart devices are deployed.
- **Case 2.** Under this case, eleven IoT smart devices are deployed.

TABLE 7. Different simulation parameters.

Parameter	Description
Platform	Ubuntu 16.04.5 LTS
Network coverage area	$100 \times 150\ m^2$
Simulation cases considered	1, 2 and 3
"Number of gateway nodes (GWN)"	1 for all cases
"Number of IoT smart devices"	5, 11, 17 for Cases 1, 2 and 3, respectively
Simulation time	1800 seconds
"Routing protocol"	AODV
"Communication range of GWN"	200 m
"Communication range of IoT smart devices"	50 m

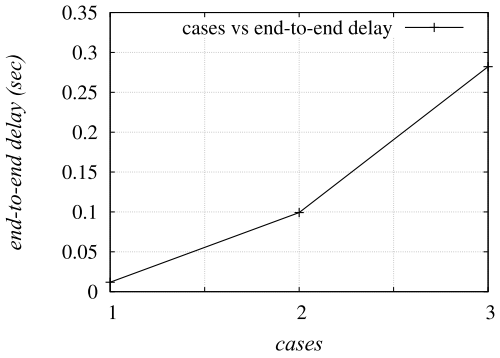

FIGURE 6. End-to-end delay.

- **Case 3.** Under this case, seventeen IoT smart devices are deployed.

In each of the above cases, the following messages are exchanged between different network entities in LACKA-IoT: $MSG_1 = \{ID_i, A_i, c_i, T_i, z_i, R_i, Q_i\}$ of 1472 bits, $MSG_2 = \{ID_j, A_j, c_j, T_j, z_j, R_j, SKV_{ij}, Q_j\}$ of 1632 bits and $MSG_3 = \{SKV'_{ij}, T'_i\}$ of 192 bits, respectively (detailed calculation is shown in Section VI-B).

C. DISCUSSIONS ON SIMULATION RESULTS

The network performance parameters: "end-to-end delay (in seconds)", "throughput (in bps)" and "packet loss rate" are measured and analyzed during the simulation of LACKA-IoT.

1) IMPACT ON END-TO-END DELAY

The "end-to-end delay (EED)" is measured as "the average time taken by the data packets to arrive at the destination from a source". It can be "mathematically computed as $\sum_{i=1}^{\nu_p}(T_{rec_i} - T_{send_i})/n_p$, where T_{rec_i} & T_{send_i} are the receiving and sending time of a packet i, respectively, and ν_p the total number of packets". The EEDs of LACKA-IoT for various simulation cases are given Fig. 6, where the EED values are 0.01182, 0.09917 and 0.28211 seconds for Cases 1, 2 and 3, respectively. The EED increases a bit in Cases 2 and 3, because in these cases more number of IoT smart devices are considered as compared to Case 1 which reflects in "more number of messages exchanged in the network". This further reflects in congestion which increases EED accordingly.

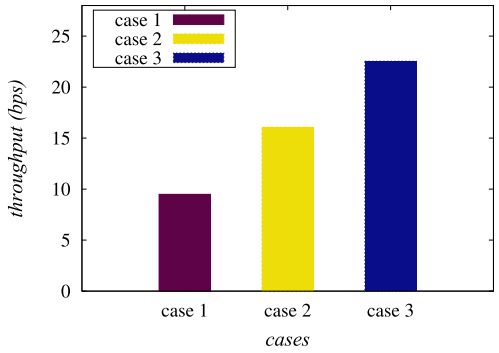

FIGURE 7. Throughput.

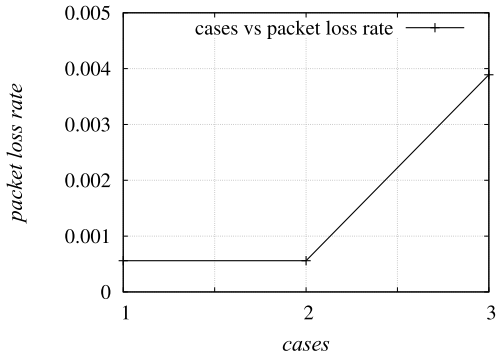

FIGURE 8. Packet loss rate.

2) IMPACT ON THROUGHPUT

The "throughput" is measured as "the number of bits transmitted per unit time which is computed as $(\nu_r \times |\delta|)/T_d$, where T_d represents total time (in seconds), $|\delta|$ is the size of a packet, and ν_r is the total number of received packets". The simulation time mentioned in the simulation is also taken as the actual total time, that is, 1800 seconds. Fig. 7 provides the details of the "network throughput (in bps)" of LACKA-IoT under different simulation cases. The throughput values becomes as 9.49, 16.07 and 22.54 bps for Cases 1, 2 and 3, respectively. The "throughput" increases with an increase in the IoT smart devices. Due to the increment in IoT smart devices, "more number of messages are exchanged in the network", and as a consequence, the "network throughput" also increases.

3) IMPACT ON PACKET LOSS RATE

The "packet loss rate (plr)" is also a crucial network performance parameter which is defined by "the number of packets loss per unit time and it is mathematically formulated as $plr = \frac{\nu_{lp}}{T_d}$, where T_d is the total time (in seconds) and ν_{lp} the total number of lost packets". For a dependable network communication, the plr needs to be kept as less as possible. The plrs of LACKA-IoT for different simulation cases are given in Fig. 8. It is also noted that the "considered simulation time is 1800 seconds, which is the total time". The plr values of LACKA-IoT are 0.00056, 0.00056 and 0.00389 for Cases 1, 2 and 3, respectively. The plr increases when

we add more number of IoT smart devices in the network, because with an increase of IoT smart devices, more messages are also interchanged. It further reflects in congestion, and as a consequence, the *plr* also rises in Case 3.

VIII. CONCLUDING REMARKS

In this article, we attempted to design a novel device access control mechanism, called LACKA-IoT, in the IoT environment. LACKA-IoT is lightweight scheme as it utilizes ''ECC and one-way cryptographic hash function''. In LACKA-IoT, through the ''device authentication process'' any two neighbor smart devices first authenticate each other using their pre-loaded certificates and other secret credentials, while the ''key agreement process'' allows those authenticated devices to construct secret key among them for secure data communication. LACKA-IoT is shown to be highly secure through a detailed security analysis using ''formal security under the widely-accepted ROR model, informal security analysis and also formal security verification under the broadly-applied AVISPA software verification tool''. A detailed comparative analysis of LACKA-IoT and other schemes (see Tables 4–6) reveals that LACKA-IoT has a better trade-off among the considered parameters (communication and computation costs, and security & functionality attributes) as compared to those for other schemes in the context of IoT. The ''practical demonstration using NS2 simulation'' on LACKA-IoT is also carried out on the ''network performance parameters (end-to-end delay, throughput and packet loss rate)'', which are shown in Figures 6–8.

In the future, we target to evaluate LACKA-IoT in a real-world environment. It will allow us to fine-tune LACKA-IoT, if necessary, to offer better security and performance in a real-world deployment including device anonymity and untraceability preservation properties.

ACKNOWLEDGMENTS

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

REFERENCES

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

[2] 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.

[3] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, ''Authentication in cloud-driven IoT-based big data environment: Survey and outlook,'' *J. Syst. Archit.*, to be published. doi: 10.1016/j.sysarc.2018.12.005.

[4] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, ''Secure remote user authenticated key establishment protocol for smart home environment,'' *IEEE Trans. Dependable Secure Comput.*, to be published. doi: 10.1109/TDSC.2017.2764083.

[5] J. Srinivas, A. K. Das, N. Kumar, and J. P. C. Rodrigues, ''Cloud centric authentication for wearable healthcare monitoring system,'' *IEEE Trans. Dependable Secure Comput.*, to be published. doi: 10.1109/TDSC.2018.2828306.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, ''Internet of Things (IoT): A vision, architectural elements, and future directions,'' *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] (2019). *Information Matters. The Business of Data and the Internet of Things (IoT)*. [Online]. Available: http://informationmatters.net/internet-of-things-statistics/

[8] L. Eschenauer and V. D. Gligor, ''A key-management scheme for distributed sensor networks,'' in *Proc. 9th ACM Conf. Comput. Commun. Secur.*, Washington, DC, USA, Nov. 2002, pp. 41–47.

[9] H. Chan, A. Perrig, and D. Song, ''Random key predistribution schemes for sensor networks,'' in *Proc. IEEE Symp. Secur. Privacy*, Berkeley, CA, USA, May 2003, pp. 197–213.

[10] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, ''Perfectly-secure key distribution for dynamic conferences,'' in *Proc. CRYPTO*, vol. 740, 1993, pp. 471–486.

[11] D. Liu, P. Ning, and R. Li, ''Establishing pairwise keys in distributed sensor networks,'' *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 1, pp. 41–77, 2005.

[12] D. Liu and P. Ning, ''Improving key predistribution with deployment knowledge in static sensor networks,'' *ACM Trans. Sensor Netw.*, vol. 1, no. 2, pp. 204–239, Nov. 2005.

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

[14] I. C. Tsai, C. M. Yu, H. Yokota, and S. Y. Kuo, ''Key management in Internet of Things via kronecker product,'' in *Proc. 22nd Pacific Rim Int. Symp. Dependable Comput.*, Christchurch, New Zealand, Jan. 2017, pp. 118–124.

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

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

[17] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller, ''Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications,'' *IEEE Access*, vol. 3, pp. 1503–1511, 2015.

[18] M. Turkanović, B. Brumen, and M. Hölbl, ''A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion,'' *Ad Hoc Netw.*, vol. 20, pp. 96–112, Sep. 2014.

[19] Q. Feng, D. He, S. Zeadally, and H. Wang, ''Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment,'' *Future Gener. Comput. Syst.*, vol. 84, pp. 239–251, Jul. 2018.

[20] X. Jia, D. He, L. Li, and K. K. R. Choo, ''Signature-based three-factor authenticated key exchange for internet of things applications,'' *Multimedia Tools Appl.*, vol. 77, no. 14, pp. 18355–18382, Jul. 2018.

[21] D. He and S. Zeadally, ''An analysis of RFID authentication schemes for Internet of Things in healthcare environment using elliptic curve cryptography,'' *IEEE Internet Things J.*, vol. 2, no. 1, pp. 72–83, Feb. 2015.

[22] C. Lin, D. He, X. Huang, K. K. R. Choo, and A. V. Vasilakos, ''BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0,'' *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, Aug. 2018.

[23] C. T. Li, C. C. Lee, and C. Y. Weng, ''Security and efficiency enhancement of robust ID based mutual authentication and key agreement scheme preserving user anonymity in mobile networks,'' *J. Inf. Sci. Eng.*, vol. 34, no. 1, pp. 155–170, Jan. 2018.

[24] C. T. Li, C. L. Chen, C. C. Lee, C. Y. Weng, and C. M. Chen, ''A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps,'' *Soft Comput.*, vol. 22, no. 8, pp. 2495–2506, Apr. 2018.

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

[26] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo, ''A robust and energy efficient authentication protocol for industrial Internet of Things,'' *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1606–1615, Jun. 2018. doi: 10.1109/JIOT.2017.2787800.

[27] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, ''A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things,'' *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3599–3609, Aug. 2018. doi: 10.1109/TII.2017.2773666.

[28] S. Jang, D. Lim, J. Kang, and I. Joe, "An efficient device authentication protocol without certification authority for Internet of Things," *Wireless Pers. Commun.*, vol. 91, no. 4, pp. 1681–1695, Dec. 2016.
[29] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of Things," in *Proc. 17th Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, Coimbra, Portugal, Jun. 2016, pp. 1–3.
[30] S. Sciancalepore, G. Piro, G. Boggia, and G. Bianchi, "Public key authentication and key agreement in IoT devices with minimal airtime consumption," *IEEE Embedded Syst. Lett.*, vol. 9, no. 1, pp. 1–4, Mar. 2017.
[31] 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.
[32] A. Braeken, P. Porambage, M. Stojmenovic, and L. Lambrinos, "eDAAAS: Efficient distributed anonymous authentication and access in smart homes," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 12, pp. 1–11, Dec. 2016.
[33] 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. doi: 10.1155/2018/6140978.
[34] X. H. Le *et al.*, "An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography," *J. Commun. Netw.*, vol. 11, no. 6, pp. 599–606, Dec. 2009.
[35] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," *IEEE Trans. Wirless Commun.*, vol. 10, no. 10, pp. 3473–3481, Oct. 2011.
[36] S. Chatterjee, A. K. Das, and J. K. Sing, "An enhanced access control scheme in wireless sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 21, nos. 1–2, pp. 121–149, Jan. 2014.
[37] V. Oleshchuk, "Internet of things and privacy preserving technologies," in *Proc. 1st Int. Conf. Wireless Commun., Veh. Technol., Inf. Theory Aerosp. Electron. Syst. Technol.*, Aalborg, Denmark, May 2009, pp. 336–340.
[38] P. P. Jayaraman, X. Yang, A. Yavari, D. Georgakopoulos, and X. Yi, "Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation," *Future Gener. Comput. Syst.*, vol. 76, pp. 540–549, Nov. 2017.
[39] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1844–1852, Dec. 2017.
[40] D. van Thuan, P. Butkus, and D. van Thanh, "A user centric identity management for Internet of Things," in *Proc. Int. Conf. IT Converg. Secur. (ICITCS)*, Beijing, China, Oct. 2014, pp. 1–4.
[41] J. B. Bernabe, J. L. Hernandez-Ramos, and A. F. S. Gomez, "Holistic privacy-preserving identity management system for the Internet of Things," *Mobile Inf. Syst.*, vol. 2017, pp. 1–20, Aug. 2017, Art. no. 6384186, doi: 10.1155/2017/6384186.
[42] 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.*, to be published. doi: 10.1109/TDSC.2018.2857811.
[43] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.
[44] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Amsterdam, The Netherlands, 2002, pp. 337–351.
[45] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography—PKC*, vol. 3386. Berlin, Germany: Springer, 2005, pp. 65–84.
[46] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 3, pp. 1900–1910, May 2018.
[47] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology*, vol. 1666. Berlin, Germany: Springer-Verlag, 1999, pp. 388–397.
[48] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.
[49] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography—PKC*. Les Diablerets, Switzerland: Springer, 2005, pp. 65–84.
[50] AVISPA. (2019). *Automated Validation of Internet Security Protocols and Applications*. [Online]. Available: http://www.avispa-project.org/
[51] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 357–366, Jan. 2016.
[52] 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.
[53] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment," *IEEE Internet Things J.*, to be published. doi: 10.1109/JIOT.2018.2888821.
[54] D. von Oheimb, "The high-level protocol specification language hlpsl developed in the eu project avispa," in *Proc. 3rd APPSEM II* , 2005, pp. 1–17.
[55] AVISPA. (2019). *SPAN, the Security Protocol ANimator for AVISPA*. [Online]. Available: http://www.avispa-project.org/
[56] Secure Hash Standard. (Apr. 1995). *FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce*. [Online]. Available: http://www.umich.edu/ x509/ssleay/fip180/fip180-1.htm
[57] E. Barker, "Recommendation for Key Management," NIST, Gaithersburg, MD, USA. Tech. Rep. 01/2016, 2018.
[58] L. Wu, J. Wang, K. R. Choo, and D. He, "Secure key agreement and key protection for mobile device user authentication," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 319–330, Feb. 2019.
[59] (2018). *The Network Simulator-ns-2*. [Online]. Available: https://www.isi.edu/nsnam/ns/index.html

ASHOK KUMAR DAS (M'17–SM'18) received the M.Tech. degree in computer science and data processing, the M.Sc. degree in mathematics, and the Ph.D. degree in computer science and engineering from IIT Kharagpur, India. He is currently an Associate Professor with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. He has authored over 185 papers in international journals and conferences in the above-mentioned areas, including over 162 reputed journal papers. Some of his research findings are published in top cited journals, such as the IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Smart Grid, IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Transactions on Vehicular Technology, IEEE Transactions on Consumer Electronics, IEEE Journal of Biomedical and Health Informatics (formerly IEEE Transactions on Information Technology in Biomedicine), *IEEE Consumer Electronics Magazine*, IEEE Access, *IEEE Communications Magazine*, *Future Generation Computer Systems*, *Computers & Electrical Engineering*, *Computer Methods and Programs in Biomedicine*, *Computer Standards & Interfaces*, *Computer Networks*, *Expert Systems With Applications*, and *Journal of Network and Computer Applications*. His current research interests include cryptography, wireless sensor network security, hierarchical access control, security in vehicular ad hoc networks, smart grid, the Internet of Things (IoT), cyber–physical systems (CPS) and cloud computing, and remote user authentication. He has served as a Program Committee Member for many international conferences. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He also severed as one of the Technical Program Committee Chairs of the International Congress on Blockchain and Applications (BLOCKCHAIN'19), Ávila, Spain, in 2019. He is on the Editorial Board of the *KSII Transactions on Internet and Information Systems*, *International Journal of Internet Technology and Secured Transactions* (Inderscience), and *IET Communications*. He is also the Guest Editor of *Computers & Electrical Engineering* (Elsevier) for the special issue on Big Data and the IoT in e-Healthcare and the *ICT Express* (Elsevier) for the special issue on Blockchain Technologies and Applications for the 5G Enabled IoT.

MOHAMMAD WAZID (S'13–M'17) received the M.Tech. degree in computer network engineering from Graphic Era University, Dehradun, India, and the Ph.D. degree in computer science and engineering from the International Institute of Information Technology, Hyderabad, India. He was a Postdoctoral Researcher with Cyber Security and Networks Laboratory, Innopolis University, Innopolis, Russia. He is currently an Assistant Professor with the Department of Computer Science and Engineering, Manipal Institute of Technology, India. He has published more than 60 papers in international journals and conferences in the above-mentioned areas. His current research interests include security, remote user authentication, the Internet of Things (IoT), and cloud computing. He was a recipient of the University Gold Medal and the Young Scientist Award by UCOST, Department of Science and Technology, Government of Uttarakhand, India. He also received the Dr. A. P. J Abdul Kalam Award for his innovative research works.

ANIMI REDDY YANNAM is currently pursuing the B.Tech. degree in computer science and engineering from the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India. His research interests include network security and security in the Internet of Things.

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

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