IEEE Open Journal of the Computer Society

Received 10 April 2024; accepted 23 May 2024. Date of publication 3 June 2024;
date of current version 13 June 2024. The review of this article was arranged by Associate Editor Zhaolong Ning.

Digital Object Identifier 10.1109/OJCS.2024.3406142

ECC-PDGPP: ECC-Based Parallel Dependency RFID-Grouping-Proof Protocol Using Zero-Knowledge Property in the Internet of Things Environment

SUMAN MAJUMDER [1], SANGRAM RAY [1] (Senior Member, IEEE), DIPANWITA SADHUKHAN [1,2], MOU DASGUPTA [3] (Senior Member, IEEE), ASHOK KUMAR DAS [4] (Senior Member, IEEE), AND YOUNGHO PARK [5] (Member, IEEE)

[1]Department of Computer Science and Engineering, National Institute of Technology Sikkim, Ravangla 737139, India
[2]Department of Computer Science, Siksha O Anusandhan (Deemed-to-be-University), Bhubaneshwar 751030, India
[3]Department of Computer Application, National Institute of Technology Raipur, Raipur 492010, India
[4]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India
[5]School of Electronics Engineering, School of Electronic and Electrical Engineering, Kyungpook National University, Daegu 41566, South Korea

CORRESPONDING AUTHORS: SANGRAM RAY; YOUNGHO PARK (e-mail: sangram.ism@gmail.com; parkyh@knu.ac.kr)

This work was supported in part by the Ministry of Education, Govt. of India, in part by the National Research Foundation of Korea (NRF) funded by the Ministry of Education through Basic Science Research Program under Grant 2020R1I1A3058605, and in part by BK21 FOUR Project funded by the Ministry of Education, Korea under Grant 4199990113966.

ABSTRACT Radio Frequency Identification (RFID) promotes the fundamental tracking procedure of the Internet of Things (IoT) network due to its autonomous data collection as well as transfer incurring low costs. To overcome the insecure exchange of tracking data and to prevent unauthorized access, parallel dependency RFID grouping-proof protocol is applied by the reader to authenticate tags simultaneously. However, conventional grouping-proof authentication schemes are not sufficient for the memory constraint RFID tags due to the recurrent utilization of a 128-bit PRNG (Pseudo Random Number Generator) function. Alternatively, the existing parallel-dependency grouping-proof schemes are not able to overcome numerous limitations regarding session establishment, efficient key management, and multicast message communication within the specified group. In this research, a lightweight, secure, and efficient communication protocol is proposed to overcome the aforementioned limitations using Elliptic Curve Cryptography (ECC) and Zero-Knowledge property to establish a session key among the participated tags, reader, and remote server. The proposed scheme can work in offline mode. The proposed ECC-based parallel dependency grouping-proof scheme is referred to as ECC-PDGPP which abides by the rules of the EPC class-1 gen-2 (C1 G2) standard of RFID tags. Finally, the proposed protocol is analyzed using a formal random oracle model and simulated using a well-known AVISPA simulation tool that shows the proposed scheme is well protected against all potential security threats.

INDEX TERMS Elliptic curve discrete logarithm problem (ECDLP), Internet of Things (IoT), pseudo random number generator (PRNG), radio frequency identification (RFID).

I. INTRODUCTION

IoT, Grouping-proof and Zero-Knowledge Protocol: IoT network is considered as an infrastructure where small nodes with limited communication capabilities are connected via communicating network [1], [2] to execute common goals [2], [3], [4] that contain connected a range of smart objects or things like –actuators, tiny microprocessors, RFID tags, sensors, power sources, communication devices, etc. Moreover, using various communication protocols, IoT has self–configuring ability and dynamic infrastructure [1], [2],

[3], [4]. Generally, its infrastructure utilizes five layers of protocol - i) at the physical level- IEEE 802.15.4 protocol is used, ii) at the adaptation level - IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) protocol is used [2], [5], [6], [7], iii) at the network level- ROLL and RPL are utilized and iv) at the application level –MQTT, XMPP, AMQP, and CoAP are exercised [8]. An IoT object communicates with each other through wired or wireless connection (Wi-Fi, Low Energy Network like Bluetooth, connectivity using Intranet or Internet, communication using mobile phones, IEEE 802.15.4, etc.) [1], [2], [5], [6], [7], [8]. In IoT, RFID is used to identify the object [3], [8] as a unique addressing scheme that contains three key components: (i) tag, (ii) reader as well as (iii) backend applications [4], [8]. Tags are usually affixed with client-side (generally with things/objects) to accumulate different information about identification, manufacturing location, etc. The Reader is responsible for broadcasting messages between the backend application and the tag. Backend applications also can compute several events to afford a variety of services for both readers and tags [3], [4], [8]. Security and privacy of RFID tags can be segregated into two different groups: i) software solution and ii) hardware solution [9], [10], [12]. A Software solution is derived from mutual authentication substituting communication messages among entities and devoid of using the hash function. A Hardware solution is derived from some process or control used in integrated circuits like - blocking or killing of tags. But most software solution generally utilizes several hash functions (such as SHA-1 and MD4) to carry out their message integrity and access control mechanism. However, due to limited computational resources and wireless medium, authentication, as well as security limitations between reader and tag still exist for low-cost tags [3], [9], [12]. Hence, authorization of identity is required using a dynamic authentication process for each object/tag to track the object since they move between readers [10], [13]. So existing protocols, did not address non-repudiation, un-cloneability issues and injection of fake objects [10], [14], [15], [16], [17], [18], [19], [20].

In the initialization phase of the grouping-proof schemes, the verifier or server inserts the secret information into the reader and participating tags. In the later phases, the server does not remain connected to either the reader or the participating tags in the grouping-proof protocol; that means in the construction phase, only offline communication is executed among the reader and participating tags within the group and the reader decides which tag or the group of tags will participate in the group within specific time range or session. Next, the reader contracts the group with the group-related secret information in the presence of the group of tags. Further, the reader sends the proof to the server for verification. The server constructs the proof with the stored secret parameters and validates the grouping-proof information received from the reader for further communication. In parallel dependency grouping-proof protocol, the reader transmits the messages to all the participating tags in the group at the construction phase. In the present situation, either Zero-Knowledge Protocol (ZKP) or Tiny ZKP is used to protect the privacy of the grouping-proof property. ZKP is a procedure by which a tag or group of tags participate in the group and convince the verifier or server regarding their presence without revealing their identities or tracking information to the reader or the attacker. Generally, the server sends a secret value to the tag during the initialization phase and based on the secret value, the challenge value is calculated by the tag. The tag generates a random value (r_t) and depending on the challenge value, the tag either transmits the square ($r_t{}^2 mod\, p$) or pseudo square$\{w.(r_t{}^2 mod\, p)\}$ to the reader where w is a secret value shared by the server to the tag along with the secret value. The verifier/server separates the square from the pseudo square using the prime factor modulus p from the proof sent by the reader.

II. RELATED WORKS

This section discusses some existing and related schemes for a group of tags using yoking-proofs, Zero Knowledge Protocol (ZKP) schemes, general grouping-proof schemes, and encryption mechanisms, and grouping proof schemes with proper tracking with anonymous identities.

Discussion regarding the Yoking-proofs scheme: The Yoking-proofs scheme, introduced by Juels [1], is the foremost protocol for demonstrating group membership. It entails only two tags. The protocol proves that any pair of tags can be scrutinized concurrently. However, any adversary can intercept the credentials/identifiers, at least by simply eavesdropping on the channel between the reader and tags, and can hamper the privacy of the RFID system. Hence, the protocol failed to defend against privacy leakage. Saito and Sakurai [2] and Burmester et al. [6] cryptanalyzed the Yoking-proof protocol and found that it is prone to replay attacks, tag impersonation attacks, and unable to resist joining any unauthorized tags to the network. Additionally, the protocol is vulnerable to interleaving attacks [2].

Discussion regarding the ZKP scheme: In 2013, Ma et al. [11] introduced a tiny ZKP that is used for the wireless network using different actuators and sensors. The tiny ZKP is used for authentication purposes and to authenticate the identity of the sensor node by the verifier. This proposal is segregated into two different processes – a) the registration phase and b) the authentication phase.

Discussion regarding the grouping proof schemes: In 2015, Sundaresan et al. [12], [13] considered several typical requirements for any grouping-proof protocol to propose a secure grouping-proof protocol for the EPC C1 G2 tags. It utilizes serial signature mode to collect the grouping proof evidence from each tag, which degrades its efficiency. However, the protocol is unable to withstand a DoS attack. Additionally, a reader is authorized to complete the grouping proof only after it is authenticated. When there are only some un-trusted readers near the verifier, then they cannot be authorized to complete a grouping-proof [15]. Furthermore, Rostampour et al. [14] proposed a novel scalable grouping-proof scheme using a 64-bit *PRNG* function, which is specially used for low-powered systems. This scheme contains three steps -a)

registration phase, b) authentication phase, and c) server validation phase. However, this scheme fails to provide proper threat resistance during communication and is susceptible to server forgery attacks [14], [15].

In 2016, Huang and Mu [18] introduced a grouping-proof protocol using a new methodology of key allocation. The protocol only utilizes lightweight functions to reduce the computing overheads of the low-resourced tags. However, the protocol renewed the secret key of tags twice for each grouping-proof period and the tag is unable to authenticate the reader since their secret keys are different. Hence, the de-synchronization attack persists and it fails to resist the DoS attack. Moreover, the protocol suffers from reader impersonation attacks and tracing attacks and becomes unsuccessful in preserving the privacy of the tags [15], [18].

Shen et al. [19] adopted simple bitwise operations in their practical grouping-proof protocol. However, the protocol also used serial signature which requires increased time for collecting grouping-proof evidence. Otherwise, an adversary can deduce the group's key and the tag's sequence number by eavesdropping the sessions. Hence, the protocol does not preserve both the privacy of the system and forward security.

Hong-yan [20] analyzed the ECC-based grouping-proof protocol proposed by Batina et al. [21] and discovered that it does not preserve forward security and suffers from scalability issues for grouping-proof applications between two tags. Hence, it is not appropriate for multiple tags.

Sun and Mu [22] analyzed the protocol proposed by Liu et al. [23] and found that it is vulnerable to replay attacks, forgery attacks, tracking attacks, and denial of service attacks. Additionally, in the protocol, the adversary can successfully compromise all secrets of tags and readers and further impersonate an authorized reader or a legal tag.

Zhang et al. [24] proposed a scalable grouping-proof protocol using a pruning query tree to reduce the collision between tags considering that the reader is trusted. The protocol suffers from de-synchronization attacks as the secret key updating problem among the tags and the reader. It is also unable to resist DoS attacks [15], [24].

Discussion regarding the grouping proof schemes with authentication and encryption mechanisms: In 2019 and later in 2020, Cherneva and Trahan, projected a Serial Dependency Grouping-proof Protocol (SDGPP) based on earlier SDZ protocol [25], [26] controlling the period of communicating messages between reader and tag. Further, it expands the privacy policies and security limitations of the SDZ protocol. Alternatively, SDGPP diminishes protection breaches, gets rid of third-party servers, and segregates the proof from the compromised tag. It also minimizes destructive attacks of the relevant tag. It preserves a special time interval called "settling" of tags to direct the time extent of the protocol. However, the protocol suffers from a de-synchronization attack.

Another scheme "Parallel Dependency Grouping-proof Protocol," was proposed by Cherneva and Trahan [27] in 2020, an effort to parallel broadcast the nature where the reader transmits and initiates the communication sending messages to group tags. All tags simultaneously receive messages, validate and compute the same then transmit the messages consecutively derived from the time slot window generated using the SDGPP scheme to reduce the overlapping [16], [27].

In 2021, Sahu and Pattniak [28], proposed an n-party grouping-proof scheme for secure communication and authentication between tags and readers to mitigate compromised tag attacks. However, this scheme faces issues regarding high computation costs and improper encryption/decryption mechanisms.

In June 2022, Safkhani et al. [29] proposed a generalized, secure, and lightweight mutual authentication protocol using a message authentication code (MAC) for RFID tags to mitigate the reply and de-synchronization attacks for the tags that participated in a group. However, this scheme cannot be applicable in real-time schemes for tracking of RFID tags participated in a group due to high communication overhead.

In 2022, Li et al. [30] proposed a scheme for tracking RFID tags within or across groups while ensuring secure communication with readers. This method improved the functionality and reduced storage demands of traditional grouping-proof mechanisms. However, the scheme is limited by its high communication and computational demands, making it less suitable for lightweight applications, and has concerns regarding anonymity.

Discussion regarding the grouping proof scheme with anonymous identity: In 2023, Gong et al. [31] proposed a cross-domain mutual authentication and tracking scheme using anonymous identity and key negotiation mechanisms for RFID tags used in IoT networks. This scheme considers various security limitations, and security performance is analyzed using a random oracle model. However, the proper encryption/decryption scheme is still lagging for messages communicated in different steps.

Recently, in 2024, Cao et al. [64] introduced a novel lightweight RFID authentication protocol based on an improved hash function, addressing vulnerabilities to replay and asynchronous attacks. It focuses on enhancing security and computational efficiency for RFID tags in decentralized environments. However, this scheme narrowly focused on RFID tags, potentially limiting broader applicability.

A motivation and contribution of the research work: From the above discussion, it is summarized that many grouping-proof schemes are mostly connecting a group of tags rather than multiple tag groups. Sometimes, it contains only two tags. Often, it is observed that the grouping-proof scheme fails to be initialized when some untrusted readers are present near a server. Some of the grouping-proof schemes adopt serial signature mode to collect grouping-proof evidence, which limits the effectiveness of those schemes. Some grouping-proof schemes cannot provide forward security and are vulnerable to privacy leakage attacks [24], [32], [44], [49], [50], [56], [57], [58], [59], [60], [61], [62], [63]. The aforementioned

limitations motivate us to design an ECC-based grouping-proof scheme for secure IoT communication with anonymous identities and the ZKP scheme.

The major contributions of the proposed scheme are summarized below:

1) This scheme introduces a lightweight grouping-proof application based on Elliptic Curve Cryptography (ECC). This scheme involves a reader and multiple groups of tags, taking into account the possibility that the reader may be trusted or untrusted. The preliminary objective is to establish mutual authentication among various network participants, including the server, the reader, and the group of tags. This novel ECC-based grouping-proof scheme, projected for parallel dependency, is denoted as ECC-PDGPP.
2) In this scheme, the reliability and privacy of the sent message are ensured by employing unidirectional, efficient hash functions and establishing secure session keys based on the Elliptic Curve Diffie-Hellman (ECDH) among the reader and the group of tags.
3) Both the Zero-Knowledge protocol and ECC-based discrete logarithmic problem are utilized to provide the required security for establishing offline communication.
4) ECC-PDGPP has been devised to withstand both active and passive security threats, as well as various types of attacks like man-in-the-middle and impersonation attacks, etc.
5) The scheme preserves the property of forward secrecy and is resilient to de-synchronization attacks.
6) A novel activate-sleep mechanism is proposed in this scheme for managing tag activity during the grouping-proof period to decrease the likelihood of collisions and reduce the computational burden on tags. This method involves activating tags relevant to the current operation while keeping all other tags in a sleeping state. Consequently, when the reader interacts with the tags, only the activated ones respond, leading to a significant reduction in both computational workload and collision probability for the tags.

Organization of the Article: The remaining part of this article is organized as: Section II describes the background studies of the previously established literature in this domain. In Section III, a detailed discussion of the preliminaries is given. Section IV explains the functional working procedures of ECC-PDGPP. Section V demonstrates security analysis using the Random Oracle Model and Section VI presents the simulation results using AVISPA whereas Section VII represents the performance analysis of the proposed scheme. Finally, Section VIII, concludes the article.

III. PRELIMINARIES

In this section, the fundamental concepts of the functional model, essential communication model, and threat model are illustrated.

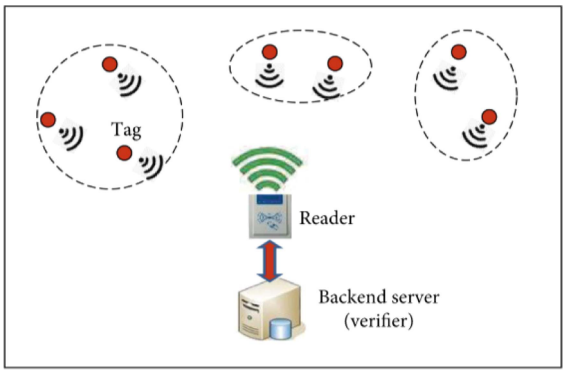

FIGURE 1. Functional model of RFID system.

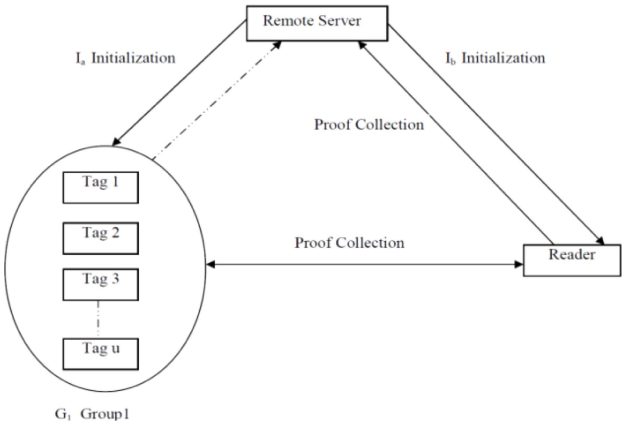

FIGURE 2. Communication Model of ECC-PDGPP.

A. FUNCTIONAL MODEL OF RFID SYSTEM

This model is used to execute secure communication among the reader, participating tags, and validating server [17], [60], [61]. A secure group-oriented message communication is performed with the help of a session key. This model includes the following participated entities as represented in Fig. 1.

1) *Participating Tags:* They are registered and valid tags.
2) *Reader:* This is a registered and valid reader.
3) *Validating Server:* This server initializes various parameters to the tags and reader and validates the proof before execution.

B. COMMUNICATION MODEL

Based on the functionality of the server during the grouping-proof period, the schemes are classified into two diverse modes: online and offline. The communication model is shown in Fig. 2.

1) For online mode, the server is implicated to complete the grouping-proof process. In offline mode, the server can only send challenges to the reader and it does not need to be present during the entire grouping-proof period. The effectiveness of the offline mode is superior to online mode. Consequently, grouping-proof schemes might use offline mode.

2) Based on the tag sequence for their signature, the grouping-proof schemes are classified into two types: serial mode and parallel mode. For serial mode, one tag can commence its signature only after another tag finishes its sign to generate its grouping-proof evidence. For the other mode, all tags can finish their signatures simultaneously. Hence, the second mode is more efficient than the first one.

C. THREAT MODEL

This model is generally considered in a situation where message-based communication must be performed through the insecure channel which is controlled by the adversary $\mathcal{A}$ and the whole communication of the participating entities can be compromised. To design this scheme, a standard threat model - Dolav-Yao (DY) [42] is considered for this scheme. On the other hand, Canetti and Krawczyk's secure adversary model [43], [59] is also used to mitigate the security issues of the contributory session key.

It is presumed that the adversary has the following abilities

1) It can fully control the communication channel among the reader, server, and tags. That means, the adversary can eavesdrop, alter, delete, replay, delay, and change any of the communicating messages during transmission.
2) It can transfer its messages to the reader (impersonating a tag) and to tags (impersonating a reader).
3) It can endeavor to destroy grouping-proof evidence in diverse ways, including generating proofs of any absent tag or vice versa.
4) It can acquire secret data to track any specific tag of the groups.

IV. THE PROPOSED SCHEME

There are mainly four main phases of the ECC-PDGPP scheme- i) Set-Up Phase, ii) Node Initialization Phase, iii) Grouping- proof Collection Phase, and iv) Verification Phase. In the Node Initialization Phase, entities involved are the data nodes that contain readers tags and server nodes in addition to based on some common secret values, a secure session key is generated based on the principle that each data node is within the range of at least one server node for secure communication within the group and maintain a greater aspect of scalability. In the Grouping-proof collection phase, two protocols (Reader and Tag Round I -Parallel and Reader and Tag Round II-Parallel) are working independently and the server does not connect to either reader or tags and an announcement is done amid group tags and the reader in offline mode. The following notations used in the ECC-PDGPP scheme are exhibited in Table 1. The different phases are demonstrated below where $U \rightarrow V : M$ signifies that the sender U forwards M (message for communication) to the receiver V and *Step n* is the respective number of step (s) of the protocol.

The scheme considers that the reader is un-trusted and required to collect grouping-proof evidence. When the grouping-proof process is started, the reader and the tags first initialize the process sending the initialization request to the server/verifier [15], [19], [60], [63]. After receiving it, the server sends a response to both the reader and the tags. Then, the reader accumulates the coexistence evidence of the group of those tags and transfers those evidence to the server respectively. Finally, the server evaluates the authenticity of the given evidence.

TABLE 1. Descriptions of Individual Notations

Notation	Description
T	Tag
S	Server/verifier
R	Reader
F_p	A prime large finite field above p
$E_p(a,b)$	Based on F_p, an elliptic curve E_p is described
P	Based on $E/F_p(a,b)$ of order n, a generator point is defined
TID_i	Identity of the respective tag
RID_i	Identity of the reader
ID_g	Group identity
SV_1,SV_2,SV_3	Unique secrets known only to server node.
SK	From server end, generated dynamic session identity
K_{ts}	Symmetric key shared between tag and server where $K_{ts}=q_{t..}Q_S$
K_{rs}	Symmetric key shared by reader and server where $K_{rs}=q_{r..}Q_S$
K_g	Symmetric group key generated by server where $K_g=r_{g..}P$
p,w	Values for Zero-Knowledge proof
ta_i	Unique tag alias identifier
$h(.)$	Secure one-way hash function for instance *SHA1*
E/D	Algorithm based on symmetric encryption/decryption process
(q_s, Q_S)	Server generated public- private key pair $Q_S=q_s.P$
(q_t, Q_t)	Tag generated public-private key pair $Q_t=q_t.P$
(q_r, Q_r)	Reader generated public-private key pair $Q_r=q_r.P$
$PRNG( )$	Pseudo-random number generator
h, h_1	Hash functions used for group-based point multiplication operation and random value-based applications respectively
$\|\|$	Concatenation

The protocol involves four individual steps: (i) a reader initiates the grouping-proof process after sending the initialization request, (ii) the server sets up a timestamp and sends the blinded identifier of the group (for those tags) to the reader, (iii) the reader accumulates grouping-proof evidence and sends those evidence to the server and(iv) if it is not timeout, the server completes the authentication procedure of the tags and verifies the grouping-proof evidence.

A. SETUP PHASE

This phase involves the primary arrangement of the scheme and the setup of necessary parameters essential for the next phases by the participants. The procedure followed in this phase is given below.

- The server considers an elliptic curve E/F_p over a prime finite field F_p that satisfies the equation $y^2 = x^3+ax+b$ where $(a, b, x, y) \in F_p$ and $4a^3+27b^2 \neq 0 \bmod p$. A point P over $E/F_p(a,b)$ is also selected as the generator along with a sub-group $\mathbb{Z}_p$ that is generated of large prime order p.
- Next, the server chooses a one-direction hash function $h(.): \{0,1\}* \rightarrow \mathbb{Z}_p{}^*$.
- The server selects its private key q_s and generates its public key using elliptic curve point multiplications as $Q_S = q_s.P$.

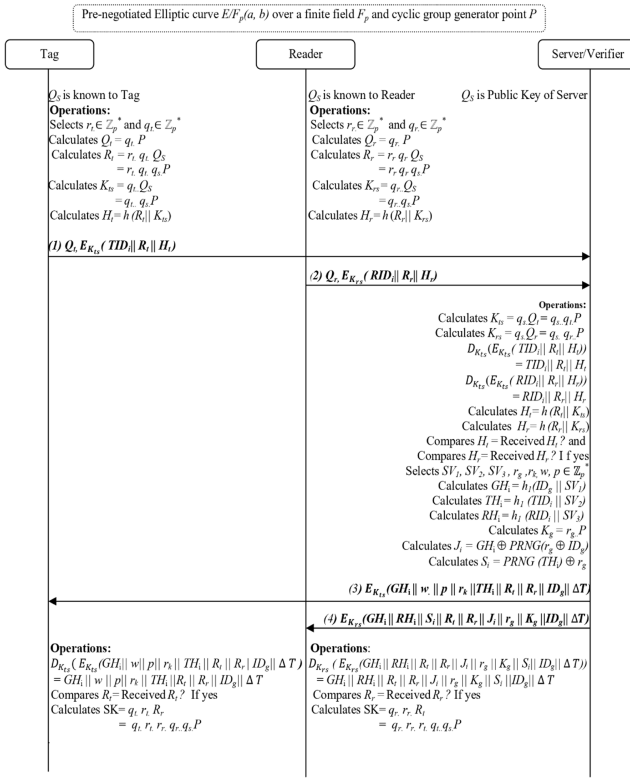

FIGURE 3. Node initialization phase.

- Finally, the server affirms the $\{a, b, p, q, E/F_p, P, h(.), Q_S\}$ as public parameters.
- The tag selects its private key q_t and generates its public key using elliptic curve point multiplications as $Q_t = q_t.P$.
- The reader selects its private key q_r and generates its public key using elliptic curve point multiplications as $Q_r = q_r.P$.

B. NODE INITIALIZATION PHASE

In the node initialization phase (shown in Fig. 3.), the entities involved are the data nodes (which contain readers and tags) and server node. It establishes a secure session key between readers and tags.

In this regard, a registered tag performs the following operations in *Step1*.

Step1: $T \rightarrow S$: $Q_t, E_{K_{ts}}(TID_i || R_t || H_t)$

- Selects a random number $r_t \in_R \mathbb{Z}_p^*$ and computes random point $R_t = r_t.q_t.Q_S = r_t.\ q_t.q_s.P$ using ECPM.
- Computes symmetric key K_{ts} between the tag and the server $K_{ts} = q_t.Q_S = q_t..q_s\ .P$ using ECPM.
- Computes $H_t = h(R_t || K_{ts})$ for additional communication among the server and reader using hash operations.
- Sends initialization request that contains $\{Q_t,\ E_{K_{ts}}(TID_i || R_t || H_t)\}$ to the server.

Following a similar procedure, a reader performs the operations as mentioned below in *Step2*.

Step2: $R \rightarrow S$: $Q_r, E_{K_{rs}}(RID_i || R_r || H_r)$

- Selects a random number $r_r \in_R \mathbb{Z}_p^*$ and computes random point $R_r = r_r.q_r.Q_S = r_r.q_r.q_s.P$ using ECPM.
- Computes symmetric key K_{rs} between the reader and the server $K_{rs} = q_r.Q_S = q_r.\ .q_s..P$
- Computes $H_r = h(R_r || K_{rs})$ for additional communication among the server and reader using hash operations.
- Sends initialization request that contains $Q_r,\ E_{K_{rs}}(RID_i || R_r || H_r)$ to the server.

Step 3 & 4: S $\rightarrow$T: $E_{K_{ts}}(GH_i || w. || p || r_k || TH_i || R_t || R_r || ID_g || \Delta T)$ $S \rightarrow R$: $E_{K_{rs}}(GH_i || RH_i || R_t || R_r || J_i || r_g || K_g || S_i || ID_g || \Delta T)$

The server/verifier pre-computes the information for the protocol run for each group and stores the information in the reader and also in each participating tag in the group.

Reader: As the reader broadcasts information to group tags, the server stacks those values that are not specific to every tag and initializes those values as per requirement:

Group specific: $\{GH_i, r_g, K_g, S_i, ID_g\}$
Independent of the group: $\{RH_i,\ \Delta T\ \}$
Group and run specific: $\{R_t, R_r, J_i\}$
Tags: The server initializes each Tag_i with the following values.
Group specific: $\{GH_i, r_k, ID_g, w, p\ \}$
Independent of the group: $\{TH_i\ \ \Delta T\ \}$
Group and run specific: $\{R_t, R_r\}$

C. GROUPING-PROOF COLLECTION PHASE

During this phase, the server is not connected with either tags or the reader, rather all tags are placed in a group in an open state by the reader and the time for secure communication of each frame is controlled by a time limit ΔT that is initialized by the server in the initialization phase. For secure communication, the reader needs to select a group of valid RFID tags to generate the proof, where the reader can automatically identify, track and monitor the objects attached with tags globally in real-time. Since RFID is often seen as a prerequisite for IoT communication, a standard is required to be maintained. For this purpose, the recent standard EPC C1G2 (Electronic Product Code Class 1 Generation 2) is considered since this standard contains different layers that define the communication between the reader as well as tags and involves the Identification phase (anti-collision scheme) and the Sense phase (sensor read scheme) related to secure communication for memory limited tags. This phase is further divided into two phases – Round I (Shown in Fig. 4.) and Round II (Shown in Fig. 5.) as described below.

Round I Reader:

Step 1: R $\rightarrow$T: $E_{SK}(J_{ir} || ID_{gr} || S_{ir} || T_1\ )$

In this step,

- A fresh pseudo-random number r_{gr} is produced by the reader and it is derived from the random number r_g.
- Further, perform the *XOR* operation between r_{gr} with the initialized values to produce J_{ir}, ID_{gr} and S_{ir}.

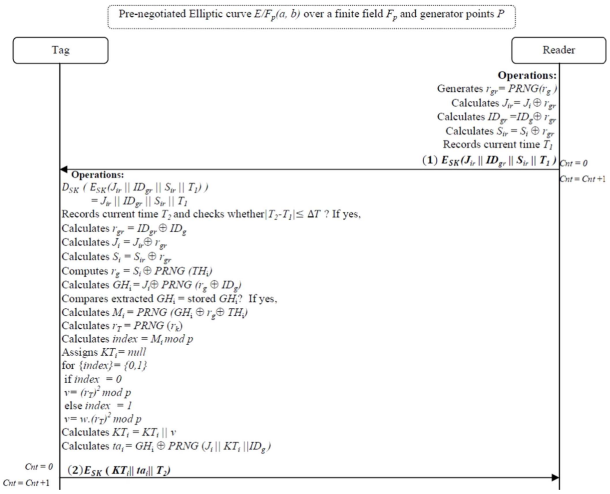

FIGURE 4. Round I, grouping-proof collection phase.

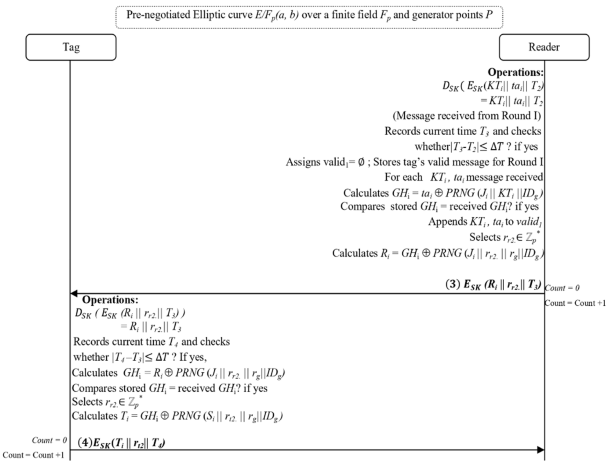

FIGURE 5. Round II, Grouping-proof Collection Phase.

- Further, the reader records the current time T_1. The reader sends the content to all group tags after encrypting with the session key - $E_{SK}(J_{ir} || ID_{gr} || S_{ir} || T_1)$.

Round I Tag_i:

Step 2: $T \rightarrow R$**:**$E_{SK}(KT_i || ta_i || T_2)$

- In this round, Tag_i first validates the reader, and checks and confirms the integrity of all the messages sent by the reader in addition to using the Zero-Knowledge protocol, the tag computes its response.
- Tag records current time T_2 and checks whether$|T_2\text{-}T_1| \leq \Delta T$, if the validation becomes successful, then tag extracts J_i ,r_g and GH_i .
- Then tag validates the extracted GH_i with the received one and if the validation becomes successful, then Tag_i authenticates that the reader is authorized by the server and confirms the integrity of the received messages.
- Later on, using XOR function among the GH_i, r_g and TH_i, Tag_i calculates the message M_i and using *PRNG* on the tag secret r_k, it calculates r_T.
- After that, Tag_i calculates the *index* using the modulus operation on M_i using Zero-Knowledge proof p and based on the *index* value, Tag_i further concatenates random squares and random pseudo squares to generate KT_i and using this value, calculates ta_i to enable the reader to authenticate the Tag_i and verify the integrity of the messages and Tag_i sends $E_{SK}(KT_i || ta_i || T_2)$ to reader.

Round II Reader:

Step3: R $\rightarrow$T**:** E_{SK} $(R_i || r_{r2.} || T_3)$

- Reader decrypts the encrypted message and gets the values KT_i, ta_i and T_2, records current time T_3 and validates whether$|T_3\text{-}T_2| \leq \Delta$T.
- Based on successful validation, a list $valid_1$ will be initialized by the reader to store the valid messages of the tag for Round I.
- Further using XOR operation between the ta_i and *PRNG* $(J_i || KT_i || ID_g)$, the reader extracts GH_i and validates the extracted GH_i with the previously stored one.
- If the validation is successful then the reader authenticates the Tag_i and confirms the integrity of all the received messages and appends those values KT_i and ta_i to $valid_1$andrepeats this process for all the group tags.
- Later, reader selects the random value r_{r2} and calculates R_i using the XOR operation between the GH_i and *PRNG* $(J_i || r_{r2.} || r_g || ID_g)$. Finally, sends the encrypted message $E_{SK}(R_i || r_{r2.} || T_3)$ to tags.

Round II Tag_i:

Step 4: $T \rightarrow R$**:**$E_{SK}(T_i || r_{t2} || T_4)$

- Tag decrypts the encrypted message and gets the values R_i, $r_{r2,}$ and T_3, records current time T_4 and validates whether$|T_4\text{-}T_3| \leq \Delta T$.
- Upon successful process validation, tag further extracts the information of GH_i using the XOR operation between the R_i and *PRNG* $(J_i || r_{r2.} || r_g || ID_g)$ and validates the extracted GH_i with the previously stored one.
- Later, the tag selects the random value $r_{t2.}$ and calculates T_i using the XOR operation between the GH_i and *PRNG* $(S_i || r_{t2.} || r_g || ID_g)$. Finally, sends the encrypted message $E_{SK}(T_i || r_{t2} || T_4)$ to the reader.

D. VERIFICATION PHASE

This phase is demonstrated in this subsection and in Fig. 6 using the following steps.

Step 1: $R \rightarrow S$**:** $E_{K_{rs}}(PF || K_g)$

- The values T_i, $r_{t2}$and $T4$ are decrypted by reader. Later on, records current time T_5 and validates whether$|T_5\text{-}T_4| \leq \Delta T$ after decrypting the incoming messages.
- Later, the tag extracts the information of GH_i using the XOR operation between the T_i and *PRNG* $(S_i || r_{t2.} || r_g || ID_g)$ and validates the extracted GH_i with the previously stored one.
- If the validation becomes successful, then the reader constructs the proof $PF = \{GH_i, RH_i, K_g, R_i, T_i, J_i, S_{i.}\}$, encrypts PF using $K_{rs,}$ and sends the proof using the

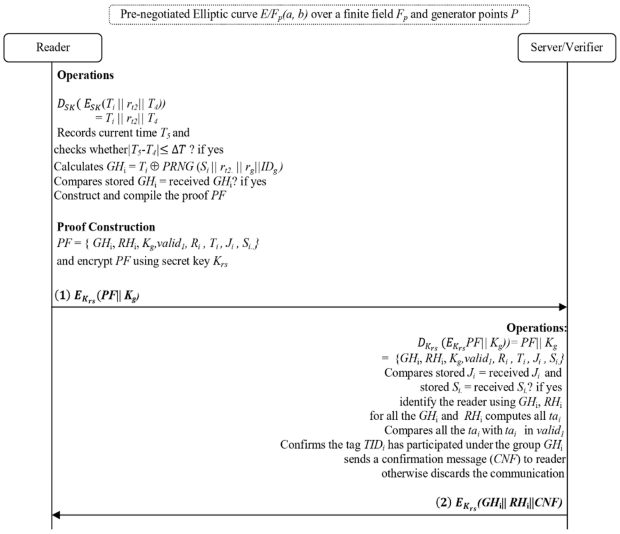

FIGURE 6. Verification Phase.

encrypted message $E_{K_{rs}}(PF \| K_g)$ to the server for further validation.

Step 2: $S \rightarrow R$**:** $E_{K_{rs}}(GH_i \| RH_i \| CNF)$

- Server decrypts the encrypted message and gets the proof - GH_i, RH_i, K_g, $valid_1$, R_i, T_i, J_i, and S_i.
- Later, validate stored J_i with the received J_i as well as stored S_i with the received S_i, and derived from the validation, the server further identifies the reader using GH_i and RH_i with the stored values.
- For all the GH_i and RH_i, the server further computes alias identities ta_i of all the tags and compares all with ta_i stored in $valid_1$by the reader, confirms whether the tag TID_i has participated under the group GH_i, and sends a confirmation message (CNF) to reader otherwise discards the communication. The functionalities of this phase are shown in Fig. 6 below.

V. SECURITY ANALYSIS

All the related security features as well as security attacks are analyzed in this section to establish the robustness of ECC-PDGPP. The subsequent paragraphs illustrate both formal security analysis using Random Oracle Model as well as informal security analysis using practical assumptions.

A. FORMAL SECURITY ANALYSIS USING RANDOM ORACLE MODEL (ROM)

ROM was proposed by Phillip Rogaway, Bellare, and Mihir in 1993 as a turning machine that works as a probabilistic polynomial time (PPTTM) [33], [43] and is utilized to test the security-related limitations of various authentication protocols where a game is played between the adversary $\mathcal{A}$ and the challenger C. A detailed description of the ROR model is given in Appendix 1.

1) SECURITY PROOF

The verification of semantic security for the ECC-PDGPP scheme is described in Theorem 1 using Real-or-Random mode and described below:

Theorem 1: It is presumed that the adversary $\mathcal{A}$ runs an e-Voting transaction against the ECC-PDGPP scheme at polynomial time t to rupture the semantic security and acquire the benefit in the ROM model. So, the advantage function of $\mathcal{A}$ is illustrated below: $Adv_{\text{ECC}-\text{PDGPP}}^{ASKE}(t) \leq \frac{q_h^2}{|Hash|} + \frac{q_{send}}{2^{l-1}.\,|D|} + 2Adv_{\text{ECC}-\text{PDGPP}}^{ECDLP}(t)$.

Where q_h ,q_{send} ,l, $|Hash|$, $|D|$, $Adv_{ECC-PDGPP}^{ECDLP}(t)$ represent the number of queries related to hash operations, a number of queries related to sending operations, numbers of bits required Zero-Knowledge proofs, range related information of one-way hash function $h(.)$, size of uniformly distributed directory for the password, in polynomial time t, the advantage for breaking the ECDLP transaction by $\mathcal{A}$.

Theorem 1 states that the advantage of breaking the semantic security of ECC-PDGPP in polynomial time is negligible. The adversary cannot guess the final round secret key from the current secret key. So, s/he cannot reveal the previous sessions and the grouping-proof scheme is forward-secure.

B. INFORMAL SECURITY ANALYSIS

In this segment, we exhibit the analysis of diverse features for informal security of ECC-PDGPP using arithmetical practices with the considerations of realistic hypotheses.

1) MAN-IN-THE-MIDDLE ATTACK:

Suppose a challenger $\tilde{A}$ is surreptitiously listening to communication among the reader, tag and server,, intercepts initiation messages containing Q_t, $E_{K_{ts}}(TID_i \| R_t \| H_t)$and Q_r, $E_{K_{rs}}(RID_i \| R_r \| H_r)$and intends to modify those messages such a way that such messages look as if approaching from legitimate participants but with the substituted values of H_t or H_r of the adversary. Though, each participating entities computes the contributory symmetric $K_{ts}=q_s.Q_t=q_t.q_s.P$, and $K_{rs}=q_s.Q_p=q_p.q_s.P$ using ECDH. Further, using the symmetric keys, the server computes $H_{t=}\ h(R_t \| K_{ts})$ and $H_{r=}\ h(R_r \| K_{rs})$ and validates the retrieved H_t and H_r with the received messages. Any unsuccessful validation leads to communication termination. Furthermore, if $\tilde{A}$ attempts to extract the random variable from R_t or R_r, it is impossible due to the hardness of cracking ECDLP in polynomial time. Hence, the ECC-PDGPP is strong against such Attacks.

2) DENIAL OF SERVICES ATTACK (DOS):

In the grouping-proof collection phase**,** both the reader and tag sends their message within a specific time limit ΔT seconds and three diverse attempts otherwise both the tag and readers will be disabled for a specific time duration. A variable *cnt* is initialized with an initial value of 0 and increased to 1 for every unsuccessful communication otherwise the communication is terminated. Every entity obtains no more than 3 endeavors to send their communication messages. Hence, an

adversary $\tilde{A}$ will not be able to make the services unavailable. Thus ECC-PDGPP manages the DoS attack.

3) REPLAY ATTACK:

In grouping-proof collection phase of the ECC-PDGPP scheme, the message $E_{SK}(J_{ir} \,||\, ID_{gr} \,||\, S_{ir} \,||\, T_1)$ is corresponded by the registered reader to the legitimate tag. If $\tilde{A}$ obtains the message and tries to reply it in such a manner just replacing the value of ID_{gr} *to* $ID_{gr}{}^{x}$ as $E_{SK}\,(J_{ir} \,||\, ID_{gr}{}^{x} \,||\, S_{ir} \,||\, T_1)$. After obtaining such message, tag computes $J_i = J_{ir} \oplus r_{gr}$ using XOR operation and further validates it with the received one to validate any disparity that occurred with the obtained J_i. In that case, the session will be terminated by the tag. Alternatively, if the adversary $\tilde{A}$ acquires the communicating message and tries to reply to the tag just change the value of current time T_1 to $T_1{}'$ and forward the message $E_{SK}(J_{ir} \,||\, ID_{gr} \,||\, S_{ir} \,||\, T_1{}')$ to current tag. However, the device fingerprinting $DF = |T_2\text{-}T_1| \leq \Delta T$ will not be identical. Therefore, the tag concludes the session. As the current timestamp is not only communicated rather it is integrated as a part of the message. Hence, this scheme withstands this attack.

4) USERS IMPERSONATION ATTACK:

Let us assume, a contender $\tilde{A}$ to be a certified consumer of an organization. Further, $\tilde{A}$ imitates the broadcasted communication, re-conveys it, and operates as if a relevant customer. On client side, the proposed scheme resists user impersonation attacks in the following grounds:

1) During initialization, tag and reader send their hello messages $Q_t,\ E_{K_{ts}}\ (TID_i||\ R_t\ ||\ H_t)$ and $Q_r,\ E_{K_{rs}}\ (RID_i||\ R_r||\ H_r)$ respectively to the server. The messages contain two different random nonce generated using random variables. It is infeasible to generate the random values from the random nonce due to rigidity of ECDLP. Alternatively, if the challenger $\tilde{A}$ wants to substitute the random information amid his own information but it can be simply traced by the server during the verification of message integrity using hash function (H_t and H_r). Moreover, to extract any secret information (random or hash random information), the $\tilde{A}$ must rupture the ECDH-based symmetric key $E_{K_{ts}}$ or $E_{K_{rs}}$ since; all the communicated messages are encrypted using the same. However, as it is previously stated compromising symmetric keys is hard due to the strength of ECC. Hence, message decryption is impossible.
2) Similarly, in the other case, tag sends the message $E_{SK}(KT_i||\ ta_i||\ T_2)$ to the reader where $ta_i = GH_i \oplus PRNG\ (J_i \,||\, KT_i \,||ID_g)$. If the challenger $\tilde{A}$ wants to amend any of the information such as ID_g, J_i or KT_i, it is impossible as it is generated as concatenated values using *PNRG* function, and each value are formed using ECC-based point multiplication or Zero-Knowledge protocol. On the other hand, GH_i is produced $GH_i = h(ID_g||\ SV_1)$ based on group ID and secret random value SV_1 selected by the server. Hence, cracking the values is impossible by the attacker. However, the overall message is encrypted by session key *SK* which is not feasible to decrypt by the attacker as *SK* is calculated as $SK = q_t.r_t.R_r = q_t.r_t.r_r.q_r.q_s.P$ containing private keys and random values of the tag and reader respectively. Hence, ECC-PDGPP proposal is competent to resist this attack.

5) SERVER-SIDE IMPERSONATION ATTACK:

In this attack, a challenger $\tilde{A}$ impersonates like a server recognizing two messages $E_{K_{ts}}(GH_i||\ w.\ ||\ p\ ||\ r_k\ ||TH_i||\ R_t\ ||\ R_r\ ||\ ID_g||\ \Delta T)$ and $E_{K_{rs}}(GH_i||\ RH_i||\ S_i\ ||\ R_t\ ||\ R_r\ ||\ J_i||\ r_g\ ||\ K_g\ ||ID_g||\ \Delta T)$are transmitted by the server the tag and reader correspondingly as like a response of the beginning demand. In this regard, Ã has to decrypt the communication first to obtain the information regarding secret keys and hashed information using symmetric keys $E_{K_{ts}}$and $E_{K_{rs}}$, random information and legitimate identities. But due to robustness of ECC, it is very rigid to rapture such keys. So, it is impossible to $\tilde{A}$ to ascertain such confidential information. Alternatively, in verification phase, the message $E_{K_{rs}}(GH_i||RH_i||CNF)$ is also forwarded by the server to reader where $GH_i = h(ID_g\ ||\ SV_1)$ and $RH_i = h(RID_i\ ||\ SV_3)$. Thus, the messages are encrypted with SK and worked out using ECDH scheme as $SK = q_t.r_t.r_r.q_r.q_s.P$ where r_t, an dr_p are the top secret random information and q_t, q_r and q_s are private keys. So, due to the rigidity of ECC scheme, it is too much hard to compromise by $\tilde{A}$. Therefore, ECC-PDGPP is very much resilient in opposition to server impersonation attack.

6) KNOWN SESSION SPECIFIC TEMPORARY ATTACK:

The session-generated key of ECC-PDGPP is worked out as $SK = q_t.r_t.r_r.q_r.q_s.P$ where r_t, and r_p are the top secret random information and q_t, q_r and q_s are private keys. Although any of the secret information such as r_t, or r_r are inadvertently disclosed to the challenger, due to the inadequacy of the private keys, the session key cannot be successfully computed. So, ECC-PDGPP is not vulnerable to this attack**.**

7) SESSION KEY COMPUTATION ATTACK:

To accomplish the information securely and swap over the same amid reader server and tag. ECC-PDGPP is designed in such a way that it preserves the secrecy of $SK = q_t.r_t.r_r.q_r.q_s.P$. This scheme utilizes ECDH-based session keys and due to the rigidity of ECDLP the session key cannot be compromised. Additionally, two random numbers (from both the reader and tag) and three private keys (from reader, tag and server), session key *SK* is computed. So, the challenger $\tilde{A}$ may not able to compromise the rigid key in polynomial time although any one of the secret parameters is unmasked to $\tilde{A}$. Hence, ECC-PDGPP prevents this type of attack.

8) PERFECT FORWARD SECRECY

In ECC-PDGPP, if the keys $E_{K_{ts}}$and $E_{K_{rs}}$are conciliated by the adversary $\tilde{A}$, still cannot be able to compromise the session key where $SK = q_t.r_t.r_r.q_r.q_s.P$. Although the contestant $\tilde{A}$ can somehow become successful for decrypting such messages by means of negotiated symmetric keys $E_{K_{ts}}$ as well as $E_{K_{rs}}$,the attacker still not be able to compute the session key due to the

use of random numbers (r_t and r_r) or secret private keys (q_t, q_r and q_s).

9) INFORMATION LEAKAGE:

Ã can deduce the messages as discussed earlier in initiation protocol those are substituted in vulnerable channel. However, all such messages are encrypted using symmetric keys $E_{K_{ts}}$ and $E_{K_{rs}}$ generated using ECDH. Moreover, the major marts of used messages are generated using random values (R_t, R_r) and ECDH scheme, hash random information (H_t, H_r), and one-way hash function. So, an attacker cannot be able to consume such diplomatic information from such messages. Moreover, in the grouping-proof collection and validation phase, all the messages are also encrypted using session key $SK = q_t.r_t.r_r.q_r.q_s.P$, generated using private keys (q_t, q_r, and q_s) and random information (r_t and r_r). So, unfeasible to evaluate due to the robustness of ECDH.

10) UNTRACEABILITY:

Suppose, a condition is considered where an antagonist $\tilde{A}$ can infer the messages that enclose Q_t, $E_{K_{ts}}$ $(TID_i || R_t || H_t)$ and Q_r, $E_{K_{rs}}$ $(RID_i || R_r || H_r)$ in a vulnerable channel. As those communications are encrypted by the contributory symmetric keys $E_{K_{ts}}$ and $E_{K_{rs}}$ that generated using ECDH, so the $\tilde{A}$ can't become successful in decrypting such communications. Alternatively, if the adversary somehow estimates the random information (R_t or R_r), s/he cannot get the anonymous identities of the user as those values are computed using ECDH-based point multiplication which is solid to counterfeit in polynomial time. Moreover, from the messages $E_{SK}(KT_i || ta_i || T_2)$ where $ta_i = GH_i \oplus PRNG(J_i || KT_i || ID_g)$ if $\tilde{A}$ desires to deduce the identity of the group ID_g still the adversary has to compute ta_i but it is a produced using random information and the concatenated values of ta_i created using the pseudorandom function $PRNG(J_i || KT_i || ID_g)$. Hence, ECC-PDGPP restricts such property of un-traceability.

VI. SIMULATION

In this section, well-known AVISPA *(Automated Verifications for Internet Security Protocol as well as Application)* is implemented to simulate ECC-PDGPP to ensure that ECC-PDGPP is protected against all relevant active and passive security attacks. AVISPA is a role-based simulator tool and denotes that every participant plays a specific role [44], [45], [48], [54], [57], [58], [59] and supports a language called *HLPSL* (*High-Level Protocol for Specification Language*). AVISPA mainly executes on a specification called *HLPSL* that is decoded into *HLPSL2IF*, a translator that uses a lower-level language and an intermediate Format (*IF*) that is contrasted to *HLPSL*. Using the AVISPA simulator, it is investigated for diverse security goals are satisfied or violated based on the output produced by different AVISPA backends either in SAFE or UNSAFE mode. There are four back ends [44], [45], [48], [54], [57], [58], [59] such as – (i) Attack Searcher founded on Constraint Logic (CL-At Se), (ii) Model Checker using On the Fly phrase (OFMC), (iii) Protocol for the Security Analysis methodology using Tree Automata (TA4SP) and (iv) Model Checker using State of the Art methodology (SATMC). The simulation result of the proposed scheme is depicted in Fig. 7 (Cl-AtSe backend) and Fig. 8 (OFMC backend) which show that the proposed scheme is 'SAFE'.

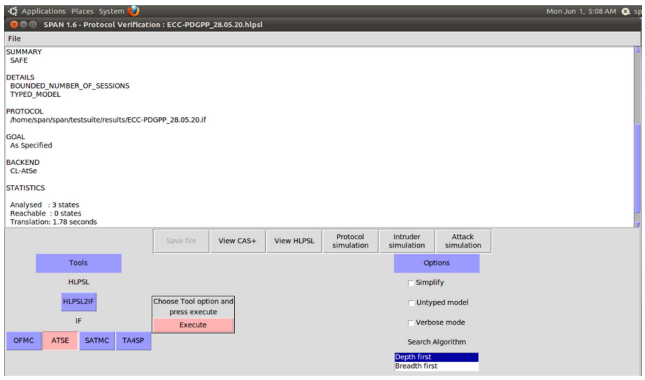

FIGURE 7. Result of AVISPA Simulation for Cl-At Se Backend.

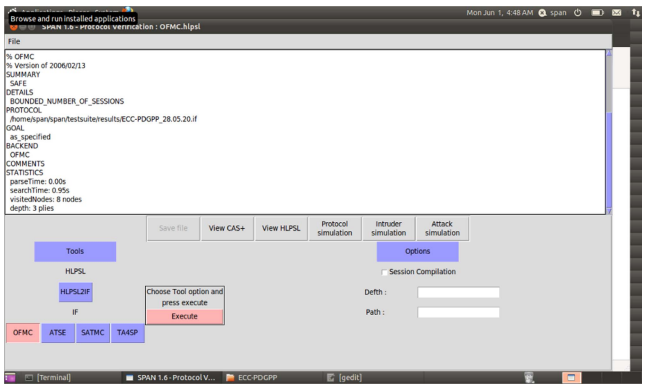

FIGURE 8. Result of AVISPA Simulation for OFMC Backend.

VII. PERFORMANCE ANALYSIS

Based on several metrics like communication overhead, computation overhead, number of communication messages, and storage overhead, the overall performance of ECC-PDGPP in terms of the aforementioned metrics is considered in this segment. The background system is accomplished using a platform that contains Intel Pentium Dual CPU E2200, 2048 MB of RAM, 2.20 GHz processor, and Ubuntu 17.04.1 LTS 32-bit operating system. We have compared ECC-PDGPP to evaluate the overall performance of this scheme with the zero-knowledge grouping-proof scheme proposed by Sunderaresan et al. [13], parallel dependency grouping-proof scheme by Cherneva and Trahan [16], serial dependency grouping-proof scheme proposed by Cherneva and Trahan [26] and recently proposed schemes by Li et al. [30] and Gong et al. [31].

The computations of different cryptographic operations are $T_{ECPM} = 2.226\ ms$, $T_{E/D(S)} = 3.85\ ms$, $T_h = 0.0046\ ms$, $T_{ECPA} = 0.0288\ ms$, $T_{EMod} = 3.85\ ms$ and $T_{Ran} = 0.539\ ms$ where T_{ECPM} is execution time for multiplication of points

TABLE 2. Comparison of Security Robustness

Security Feature	[16]	[18]	[13]	[30]	[15]	[18]	[20]	[21]	[17]	[31]	ECC-PDGPP
Resists Man-in-the-Middle Attack	✓	✓	×	✓	✓	✓	✓	✓	×	✓	✓
Resists DoS Attack	✓	✓	×	✓	×	×	×	×	✓	×	✓
Resists Replay Attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓
Resists Insider Attack	×	✓	✓	×	✓	✓	✓	✓	×	×	✓
Resists User Impersonation Attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resists Server Impersonation Attack	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Resists Offline Password Guessing Attack	×	×	×	×	✓	✓	✓	✓	✓	✓	✓
Resists Known Session Specific Temporary Attack	×	×	×	×	✓	✓	✓	✓	✓	✓	✓
Resists Session Key Computation Attack	×	×	×	×	✓	✓	✓	✓	✓	✓	✓
Resists Efficient Mutual Authentication	✓	✓	✓	✓	×	×	✓	✓	✓	✓	✓
Resists Non- Repudiation	✓	✓	×	✓	✓	✓	✓	✓	×	✓	✓
Resists Perfect Forward Secrecy	×	✓	✓	×	✓	✓	×	×	✓	✓	✓
Resists Un-traceability	✓	✓	✓	✓	✓	×	✓	×	✓	✓	✓
Resists Un-linkability/Anonymity	✓	×	×	×	✓	✓	✓	✓	✓	✓	✓
Resists Information leakage	✓	✓	✓	✓	×	×	✓	✓	✓	×	✓

TABLE 3. Comparison of Computation Overheads

Proposals	Scheme Overhead	Time in milliseconds(ms)
ECC-PDGPP	$\boldsymbol{12T_{Ran}+19T_{EMod}+3T_{E/D(S)}}$	**91.168**
Gong et al. [31]	$14T_{EMod}+7T_{E/D(S)}+7T_{ECPM}+10\,T_h$	96.478
Li et al. [30]	$24T_{EMod}+17T_{Ran}+4T_{E/D(S)}$	116.963
Cherneva and Trahan [16]	$9T_h+23T_{Ran}+34T_{EMod}$	150.009
Cherneva and Trahan [26]	$4T_h+40T_{Ran}+37T_{EMod}+6T_{E/D(S)}$	164.331
Sunderasan et al. [13]	$4T_h+4T_{E/D(S)}+30T_{Ran}+45T_{EMod}$	187.967

TABLE 4. Comparison of Communication Overheads

Schemes	Communication in bits	Number of message communication
ECC-PDGPP	**704 bits**	**4 messages**
Gong et al. [31]	3648 bits	8 messages
Li et al. [30]	4096 bits	8 messages
Cherneva and Trahan [16]	4928 bits	12 messages
Cherneva and Trahan [26]	3904 bits	9 messages
Sunderasan et al. [13]	5920 bits	18 messages

on elliptic curve, $T_{E/D(S)}$ is execution time for decryption/encryption using symmetric key, T_h is the execution time of hash operation, T_{ECPA} is the execution time of the point addition of different points on elliptic curve, T_{EMod} is the execution time of the modular exponential/XOR operations, T_{Ran} is the execution time of the selection of random numbers [33], [44], [59].On the other hand, it can also be computed based on the quantities of exchanged messages among the communicating parties. ECC-PDGPP is more proficient about computation, communication overhead and security robustness than other accessible schemes. In ECC-PDGPP, different entities are taken as number of bits for communication such as time stamps $(T_1, T_2, T_3, T_4, T_5)$ are extracted as 32 bits, identities of the communicating parties (TID_i, $ID_g$and RID_i) are considered as 64 bits, action performed for encryption using contributory session or symmetric keys (SK ,K_{ts} or K_{rs}) are regarded like 160 bits, random values (R_t, R_r and R_i) are extracted as 128 bits [33], [34], [35], [36], [37], [38], [39] and Pseudo Random Number Generators ($PRNG$) are regarded as 128 bits [40], [44], [59].

Based on the message communication, the overall bits transmitted in ECC-PDGPP is 704 bits which is not more than Sunderasan et al. scheme [13], parallel dependency grouping-proof scheme by Cherneva and Trahan [16], serial dependency grouping-proof scheme proposed by Cherneva and Trahan [26] and recently proposed schemes by Li et al. [30] and Gong et al. [31]. The comparison of security features, computation overheads and communication overheads with other related schemes are demonstrated in Tables 2–4 respectively. Table 2 shows that, unlike other schemes, the proposed scheme is unsusceptible to all possible active security threats; Table 3 demonstrates the proposed scheme incurs the lowest computation overhead (91.168 ms) compared to other schemes and Table 4 shows that the communication overheads of our scheme are 704 bits and 4 message which is under most considering the related schemes. Therefore, it can be concluded that the scheme is anonymous, robust, and efficient.

VIII. CONCLUSION

A flexible ECC-based secure grouping-proof scheme among the tag, reader, and cloud server is proposed for session management in IoT nodes. ECC-PDGPP provides secure data sharing among the tags, readers, and servers. On the other hand, ECC-PDGPP also resists security breaches and preserves a secure session for the participants of the IoT network under the grouping-proof activities and key management issues for resource-limited IoT devices. ECC-PDGPP also provides resistance against relevant cryptographic attacks since it utilizes a computationally hard ECDH algorithm. Moreover, ECC-PDGPP is formally verified using a widely recognized AVISPA simulator, Random Oracle Model, and BAN logic, and found well secure against existing security attacks. The performance analysis demonstrates the proposed ECC-PDGPP is efficient for resource-constrained IoT devices since it incurs low computation and communication overheads. Furthermore, our scheme also provides better solutions for ubiquitous ECC-based grouping-proof applications of IoT in compared to other relevant existing protocols.

REFERENCES

[1] A. Juels, "Yoking-proofs for RFID tags," in *Proc. IEEE Annu. Conf. Pervasive Comput. Commun. Workshops*, 2004, pp. 138–143,.

[2] J. Saito and K. Sakurai, "Grouping-proof for RFID tags," in *Proc. 19th Int. Conf. Adv. Inf. Netw. Appl.*, 2005, pp. 621–624.

[3] S. Piramuthu, "On existence proofs for multiple RFID tags," in *Proc. ACS/IEEE Int. Conf. Pervasive Serv.*, 2006, pp. 317–320.

[4] L. Bolotnyy and G. Robins, "Generalized yoking-proofs for a group of RFID tags," in *Proc. IEEE 3rd Annu. Int. Conf. Mobile Ubiquitous Syst.: Netw. Serv.*, 2006, pp. 1–4.

[5] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda, "Solving the simultaneous scanning problem anonymously: Clumping proofs for RFID tags," in *Proc. IEEE 3rd Int. Workshop Secur., Privacy Trust Pervasive Ubiquitous Comput.*, 2007, pp. 55–60.

[6] M. Burmester, B. De Medeiros, and R. Motta, "Provably secure grouping-proofs for RFID tags," in *Proc. Int. Conf. Smart Card Res. Adv. Appl.*, 2008, pp. 176–190.

[7] H. H. Huang and C. Y. Ku, "A RFID grouping-proof protocol for medication safety of inpatient," *J. Med. Syst.*, vol. 33, no. 6, 2009, Art. no. 467.

[8] I. Chatzigiannakis, A. Pyrgelis, P. G. Spirakis, and Y. C. Stamatiou, "Elliptic curve based zero-knowledge proofs and their applicability on resource constrained devices," in *Proc. IEEE 8th Int. Conf. Mobile Ad-Hoc Sensor Syst.*, 2011, pp. 715–720.

[9] A. Sardar, S. R. YV, and N. Rukma Rekha, "Zero-knowledge proof in secret sharing scheme using elliptic curve cryptography," in *Proc. Int. Conf. Comput. Commun. Syst.*, 2012, pp. 220–226,.

[10] D. M. Kuthe and A. J. Agrawal, "Implementation of blind digital signature using ECC and zero-knowledge protocol," *Int. J. Sci. Res. Pub.*, vol. 4, pp. 1–4, Sep. 2012.

[11] L. Ma, Y. Ge, and Y. Zhu, "Tiny ZKP: A lightweight authentication scheme based on zero-knowledge proof for wireless body area networks," *Wireless Pers. Commun.*, vol. 77, no. 2, pp. 1077–1090, 2013.

[12] S. Sundaresan, R. Doss, S. Piramuthu, and W. Zhou, "A robust grouping-proof protocol for RFID EPC C1G2 tags," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 6, pp. 961–975, Jun. 2014.

[13] S. Sundaresan, R. Doss, and W. Zhou, "Zero-knowledge grouping-proof protocol for RFID EPC C1G2 tags," *IEEE Trans. Comput.*, vol. 64, no. 10, pp. 2994–3008, Oct. 2015.

[14] S. Rostampour, N. Bagheri, M. Hosseinzadeh, and A. Khademzadeh, "A scalable and lightweight grouping-proof protocol for Internet of Things applications," *J. Supercomputing*, vol. 74, no. 1, pp. 71–86, 2017.

[15] Z. Shi, X. Zhang, and J. Liu, "The lightweight RFID grouping-proof protocols with identity authentication and forward security," *Wireless Commun. Mobile Comput.*, vol. 2021, 2020, Art. no. 8436917.

[16] V. Cherneva and J. L. Trahan, "A secure and efficient parallel-dependency RFID grouping-proof protocol," *IEEE J. Radio Freq. Identification*, vol. 4, no. 1, pp. 14–23, Mar. 2020.

[17] V. Cherneva and J. L. Trahan, "Grouping proofs for dynamic groups of RFID tags: A secure and scalable protocol," in *Proc. 10th Annu. Comput. Commun. Workshop Conf.*, 2020, pp. 0097–0103.

[18] P. Huang and H. Mu, "A high-security RFID grouping-proof protocol," *Int. J. Secur. Its Appl.*, vol. 9, no. 1, pp. 35–44, 2015.

[19] J. Shen, H. Tan, Y. Ren, Q. Liu, and B. Wang, "A practical RFID grouping authentication protocol in multiple-tag arrangement with adequate security assurance," in *Proc. IEEE 18th Int. Conf. Adv. Commun. Technol.*, 2016, pp. 693–699,.

[20] K. Hong-yan, "Analysis and improvement of ECC-based grouping-proof protocol for RFID," *Int. J. Control Automat.*, vol. 9, no. 7, pp. 343–352, 2016.

[21] L. Batina, Y. K. Lee, S. Seys, D. Singelée, and I. Verbauwhede, "Privacy-preserving ECC-based grouping proofs for RFID," in *Proc. Int. Conf. Inf. Secur.*, 2010, pp. 159–165.

[22] D. Z. Sun and Y. Mu, "Security of grouping-proof authentication protocol for distributed RFID systems," *IEEE Wireless Commun. Lett.*, vol. 7, no. 2, pp. 254–257, Jun. 2017.

[23] H. Liu, H. Ning, Y. Zhang, D. He, Q. Xiong, and L. T. Yang, "Grouping-proofs-based authentication protocol for distributed RFID systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 7, pp. 1321–1330, Jul. 2012.

[24] W. Zhang, S. Qin, S. Wang, L. Wu, and B. Yi, "A new scalable, lightweight grouping-proof protocol for RFID systems," *Wireless Pers. Commun.*, vol. 103, no. 1, pp. 133–143, 2018.

[25] V. Cherneva and J. L. Trahan, "Serial-dependency grouping-proof protocol for RFID EPC C1G2 Tags," in *Proc. IEEE 2018 Green Energy Smart Syst. Conf.*, 2018, pp. 1–6.

[26] V. Cherneva and J. L. Trahan, "Serial-dependency grouping-proof protocol for RFID EPC Gen2 tags," *IEEE J. Radio Freq. Identification*, vol. 4, no. 2, pp. 159–169, Jun. 2020.

[27] V. Cherneva and J. L. Trahan, "A secure and efficient parallel-dependency RFID grouping-proof protocol," in *Proc. IEEE 2019 Int. Conf. RFID*, 2019, pp. 1–8.

[28] S. R. Sahu and S. Pattniak, "A novel secure group RFID authentication protocol," *DogoRangsang Res. J., UGC Care Group I J.*, vol. 08, no. 04, pp. 94–103, 2021.

[29] M. Safkhani, S. Rostampour, Y. Bendavid, S. Sadeghi, and N. Bagheri, "Improving RFID/IoT-based generalized ultra-lightweight mutual authentication protocols," *J. Inf. Secur. Appl.*, vol. 67, 2022, Art. no. 103194.

[30] Y. Z. Li, D. W. Liu, and W. T. Zuo, "Tag group coexistence protocol for verifiable RFID system," *Int. J. Netw. Secur.*, vol. 24, no. 6, pp. 1056–1063, 2022.

[31] B. Gong, G. Zheng, M. Waqas, S. Tu, and S. Chen, "LCDMA: Lightweight cross-domain mutual identity authentication scheme for Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12590–12602, Jul. 2023.

[32] M. E. S. Saeed, Q. Y. Liu, G. Tian, B. Gao, and F. Li, "Remote authentication schemes for wireless body area networks based on the Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4926–4944, Jun. 2018.

[33] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *IEEE Commun. Surveys Tut.*, vol. 16, no. 2, pp. 1005–1023, Second Quarter 2013.

[34] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Comput. Netw.*, vol. 104, pp. 137–154, 2016.

[35] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Hoboken, NJ, USA: John Wiley & Sons, 2007.

[36] S. Sundaresan, R. Doss, and W. Zhou, "Zero-Knowledge grouping-proof protocol for RFID EPC C1G2 tags," *IEEE Trans. Comput.*, vol. 64, no. 10, pp. 2994–3008, Oct. 2015.

[37] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the Internet of Things," *Comput. Elect. Eng.*, vol. 37, no. 2, pp. 147–159, 2011.

[38] L. C. Silva, F. M. M. Neto, and J. L. J. Júnior, "MobiLE: Um ambiente multiagente de aprendizagem móvel baseado em algoritmo genético para apoiar a aprendizagem ubíqua," *Revista Brasileira de Informática na Educação*, vol. 21, no. 01, 2013, Art. no. 62.

[39] B. C. Villaverde, D. Pesch, R. D. P. Alberola, S. Fedor, and M. Boubekeur, "Constrained application protocol for low power embedded networks: A survey," in *Proc. IEEE 6th Int. Conf. Innov. Mobile Internet Serv. Ubiquitous Comput.*, 2012, pp. 702–707.

[40] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, 2001.

[41] S. Ray, G. P. Biswas, and M. Dasgupta, "Secure multi-purpose mobile-banking using elliptic curve cryptography," *Wireless Pers. Commun.*, vol. 9, no. 3, pp. 1331–1354, 2016.

[42] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology," *J. ACM*, vol. 51, no. 4, pp. 557–594, 2004.

[43] S. Challa et al., "An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 69, pp. 534–554, 2018.

[44] S. Majumder, S. Ray, D. Sadhukhan, M. K. Khan, and M. Dasgupta, "Ecc-coap: Elliptic curve cryptography-based constraint application protocol for Internet of Things," *Wireless Pers. Commun.*, vol. 116, no. 3, pp. 1867–1896, 2021.

[45] D. Rangwani, D. Sadhukhan, S. Ray, M. K. Khan, and M. Dasgupta, "An improved privacy preserving remote user authentication scheme for agricultural wireless sensor network," *Trans. Emerg. Telecommun. Technol.*, vol. 3, no. 3, 2021, Art. no. e4218.

[46] F. Sun, S. He, X. Zhang, F. Shen, Q. Li, and Y. He, "Tiny AKE: A more practicable and trustable scheme for authenticated key establishment in WSN," 2021, *arXiv:2104*.01907.

[47] M. Troncoso and B. Hale, "The bluetooth CYBORG: Analysis of the full human-machine passkey entry AKE protocol," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2021, pp. 1–6.

[48] D. Sadhukhan, S. Ray, M. S. Obaidat, and M. Dasgupta, "A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography," *J. Syst. Architecture*, vol. 114, 2021, Art. no. 101938.

[49] S. Majumder, S. Ray, C. Ghosh, and S. Datta, "Usage of Internet of Things in home automation systems: A review," in *Proc. Intern. Conf. Modelling, Simul. Optim.*, 2021, pp. 57–72.

[50] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *J. Supercomputing*, vol. 77, no. 2, pp. 1114–1151, 2021.
[51] U. Chatterjee, D. Sadhukhan, and S. Ray, "An improved authentication and key agreement protocol for smart healthcare system in the context of Internet of Things using elliptic curve cryptography," in *Proc. Int. Conf. IoT Inclusive Life*, 2020, pp. 11–22.
[52] S. Naskar, T. Zhang, G. Hancke, and M. Gidlund, "OTP-based symmetric group key establishment scheme for IoT networks," in *Proc. IEEE 47th Annu. Conf. Ind. Electron. Soc.*, 2021, pp. 1–8.
[53] G. Moad et al., "Living free radical polymerization with reversible addition–fragmentation chain transfer (the life of RAFT)," *Polym. Int.*, vol. 4, no. 9, pp. 993–1001, 2000.
[54] D. Sadhukhan, S. Ray, M. S. Obaidat, and M. Dasgupta, "A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography," *J. Syst. Architecture*, vol. 114, 2021, Art. no. 101938.
[55] M. S. Van Nguyen, T. T. T. Nguyen, and D. T. Do, "User grouping-based multiple access scheme for IoT network," *Telkomnika, Telecommunication Comput. Electron. Control*, vol. 19, no. 2, pp. 499–506, 2021.
[56] S. Majumder and S. Ray, "Usage of blockchain technology in e-voting system using private blockchain," in *Proc. Intell. Data Eng. Analytics*, 2022, pp. 51–61.
[57] S. Majumder, S. Ray, D. Sadhukhan, M. K. Khan, and M. Dasgupta, "Esotp: ECC-based secure object tracking protocol for IoT communication," *Int. J. Commun. Syst.*, vol. 35, no. 4, Nov. 2021, Art. no. e5026.
[58] S. Ray and G. P. Biswas, "Design of mobile public key infrastructure (M-PKI) using elliptic curve cryptography," *Int. J. Cryptogr. Inf. Secur.*, vol. 3, no. 1, pp. 25–37, 2013.
[59] S. Majumder, S. Ray, D. Sadhukhan, M. Dasgupta, A. K. Das, and Y. Park, "ECC-EXONUM-eVOTING: A novel signature-based e-voting scheme using blockchain and zero knowledge property," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 583–598, 2023.
[60] T. Li, Y. Liu, and J. Ning, "SDRLAP: A secure lightweight RFID mutual authentication protocol based on PUF with strong desynchronization resistance," *Peer-to-Peer Netw. Appl.*, vol. 16, no. 4, pp. 1652–1667, 2023.
[61] J. L. Trahan and V. Cherneva, "RT-OTP: A secure, EPC-compliant, ownership transfer protocol for an RFID tag," in *Proc. IEEE Green Energy Smart Syst. Conf.*, 2021, pp. 1–6.
[62] S. Majumder, S. Ray, C. Ghosh, and S. Datta, "Usage of Internet of Things in home automation systems: A review," in *Proc. Model., Simul. Optim.:CoMSO*, 2021, pp. 57–72.
[63] F. Xiao, "A lightweight secure search protocol for RFID tags," in *Proc. 2022 IEEE 2nd Int. Conf. Electron. Technol., Commun. Inf.*, 2022, pp. 114–118.
[64] F. M. Cao and X. P. He, "Lightweight RFID bidirectional authentication protocol based on improved hash function," *Int. J. Netw. Secur.*, vol. 26, no. 1, pp. 98–105, 2024.

SUMAN MAJUMDER received the B.Tech. degree in computer science engineering from the West Bengal University of Technology (currently known as Maulana Abul Kalam Azad University of Technology), Kolkata, West Bengal, India, in 2006, the M.Tech. degree in information technology from Jadavpur University, Kolkata, West Bengal, India, in 2011, and the Ph.D. degree on 2nd December, 2022, under the supervision of Dr. Sangram Ray, Associate Professor with the Department of Computer Science and Engineering, National Institute of Technology Sikkim, India under the Ministry of Human Resource Department, Govt. of India. He was an Associate System Engineer and Application Developer with IBM Indian and developed various live pilot projects for several Europian countries like Poland, Switzerland, Italy, U.K., and several Asian countries. He was also selected as a Postdoctoral Research Fellow with Nanyang Technological University, Singapore. His research interests include blockchain/distributed ledger/distributed applications, blockchain-security, blockchain based cross-chain bridge for crypto currency, Internet-of-Things, cryptography, information security, cybersecurity, and elliptic curve cryptography.

SANGRAM RAY (Senior Member, IEEE) received the M.Tech. and Ph.D. degrees from the Indian Institute of Technology (Indian School of Mines) Dhanbad, India. He has more than thirteen years of teaching and research experience, and more than eight years of administrative experience in various capacities including Dean, Head of the Department, Member of Board of Governors, Member of Senate, and Faculty In-charge Training & Placement Cell. He is currently an Associate Professor with the Department of Computer Science and Engineering, National Institute of Technology Sikkim, Sikkim, India. His research interests include cryptography and information security, elliptic curve cryptography, content centric network, Internet-of-Things, cyber security, and blockchain technology. He is also Supervising (sole) seven Ph.D. degree candidates and one Postdoctoral Fellow, and also two candidates were the recipient of Ph.D. degree, sponsored by Ministry of Electronics & IT, Govt. of India, under his sole supervision. He has authored more than 50 research papers in SCI-indexed international journals, conference of repute, and book chapters, and has delivered more than 50 keynote lectures/expert talks with International/National Conferences, Workshops, Seminars, Faculty Development Programs, and Short-term Courses. Dr. Ray has acted as the Member of Advisory Committee, Technical Committee, Program Committee, and Session Chairs with more than 200 International/National Conference, Seminars, and Workshops. He is also a Reviewer of more than 30 international and national journals published by IEEE, Springer, Elsevier, Wiley, CSI, IETE, MDPI, and Harvard. He has been granted external funding of more than 1 00 00 000 for R&D projects, and FDPs. He is the Chief Investigator (sole) of two R&D projects funded by Ministry of Science and Technology, Govt. of India and the Ministry of Electronics and Information Technology, Govt. of India, respectively. He is the Member of ACM and Life Member of CSI, ISTE, ISCA, IEI, IAENG, IACSIT, and CSTA.

DIPANWITA SADHUKHAN received the B.Tech. degree in information technology and the M.Tech. degree in computer science and engineering from the Maulana Abul Kalam Azad University of Technology, Kolkata, West Bengal, India, and the Ph.D. degree from the Department of Computer Science and Engineering, National Institute of Technology Sikkim, India under the Ministry of Education, Govt. of India. Her research interests include cryptography, information security, elliptic curve cryptography, Internet of Things, and network security.

MOU DASGUPTA (Senior Member, IEEE) received the M.Tech. degree from the Maulana Abul Kalam Azad University of Technology, Kolkata, West Bengal, India, and the Ph.D. degree from the Indian Institute of Technology (Indian School of Mines), Dhanbad, India. She has more than 10 years of teaching and research experience. She is currently an Assistant Professor with the Department of Computer Application, National Institute of Technology Raipur, India. Her research interests include cryptography and information security, elliptic curve cryptography, block chain technology, Internet-of-Things, and under water wireless sensor network. She is also Supervising (sole) two Ph.D. degree candidates and also one candidate was the recipient of the Ph.D. degree under her sole supervision. She has authored or coauthored more than 50 research papers in SCI-indexed international journals, conference of repute, and book chapters, and has delivered more than 20 keynote lectures/expert talks in International/National Conferences, Workshops, Seminars, Faculty Development Programs, and Short-term Courses. Dr. Dasgupta has acted as the Member of Advisory Committee, Technical Committee, Program Committee, and Session Chairs with several International/National Conference, Seminars, and Workshops. She is also a Reviewer of various International and National journals published by IEEE, Springer, Elsevier, Wiley, CSI, IETE, MDPI, and Harvard. She is also a Fellow Member of IETE, and Life Member of ISCA, IAENG, IACSIT, and CSTA.

ASHOK KUMAR DAS (Senior Member, IEEE) received a Ph.D. degree in computer science and engineering, an M.Tech. degree in computer science and data processing, and an M.Sc. degree in mathematics from IIT Kharagpur, India. He is currently a Full Professor with the Center for Security, Theory and Algorithmic Research, IIIT, Hyderabad, India, and also a visiting research professor with the Virginia Modeling, Analysis and Simulation Center, Old Dominion University, Suffolk, VA 23435, USA. His current research interests include cryptography, system and network security including security in smart grid, Internet of Things (IoT), Internet of Drones (IoD), Internet of Vehicles (IoV), Cyber-Physical Systems (CPS) and cloud computing, intrusion detection, blockchain, AI/ML security, and post-quantum cryptography. He has authored over 420 papers in international journals and conferences in the above areas, including over 355 reputed journal papers. He was a recipient of the Institute Silver Medal from IIT Kharagpur. He has been listed in the Web of Science (Clarivate) Highly Cited Researcher 2022 and 2023 in recognition of his exceptional research performance. He was/is on the editorial board of IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE SYSTEMS JOURNAL, *Journal of Network and Computer Applications* (Elsevier), *Computer Communications* (Elsevier), *Journal of Cloud Computing* (Springer), *Cyber Security and Applications* (Elsevier), *IET Communications, KSII Transactions on Internet and Information Systems*, and *International Journal of Internet Technology and Secured Transactions* (Inderscience). He also served as one of the Technical Program Committee Chairs of the first International Congress on Blockchain and Applications (BLOCKCHAIN'19), Avila, Spain, June 2019, International Conference on Applied Soft Computing and Communication Networks (ACN'20), October 2020, Chennai, India, second International Congress on Blockchain and Applications (BLOCKCHAIN'20), L'Aquila, Italy, October 2020, and International Conference on Applied Soft Computing and Communication Networks (ACN'23), December 2023, Bangalore, India. His Google Scholar H-index is 87 and i10-index is 262 with over 21 800 citations.

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