IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 30, 2021, accepted June 10, 2021, date of publication June 14, 2021, date of current version June 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3089009

Securing Internet of Drones With Identity-Based Proxy Signcryption

MUHAMMAD ASGHAR KHAN[1], HABIB SHAH[2], SAJJAD UR REHMAN[3], (Member, IEEE), NEERAJ KUMAR[4,5,6], (Senior Member, IEEE), ROZAIDA GHAZALI[7], DANISH SHEHZAD[8], AND INSAF ULLAH[1]

[1]Hamdard Institute of Engineering and Technology, Hamdard University, Islamabad 44000, Pakistan
[2]Department of Computer Science, College of Computer Science, King Khalid University, Abha 62529, Saudi Arabia
[3]Department of Electrical Engineering, Namal Institute, Mainwali 42250, Pakistan
[4]Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala 147004, India
[5]Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan
[6]School of Computer Science, University of Petroleum and Energy Studies, Dehradun 222001, India
[7]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Batu Pahat 86400, Malaysia
[8]Department of Computer Science, National University of Computer and Emerging Sciences, Chiniot-Faislabad Campus, Islamabad 35400, Pakistan

Corresponding author: Insaf Ullah (insafktk@gmail.com)

This work was supported by the Deanship of Scientific Research at King Khalid University, Abha, Saudi Arabia, through the Research Groups Program under Grant R.G.P.1/365/42.

ABSTRACT Internet of Drones (IoD) is a decentralized networking architecture that makes use of the internet for uniting drones to enter controlled airspace in a coordinated manner. On the one hand, this new clan of interconnected drones has ushered in a new era of real-world applications; Small drones, on the other hand, are generally not designed with security in mind, making them exposed to fundamental security and privacy concerns. Limited computing capabilities, along with communication over an open wireless channel, exacerbate these challenges, making the IoD unfeasible for secure operations. In this article, we propose an identity-based proxy signcryption scheme to address these issues. During data transfer between drones and to the cloud server, the proposed scheme supports outsourcing decryption and member revocation. The proposed scheme is based on the notion of Hyper Elliptic Curve Cryptography (HECC), which improves network computation efficiency. We use formal security analysis with the Random Oracle Model (ROM) to evaluate security toughness. The performance analysis of the proposed scheme has also been reviewed in terms of computation and communication costs with the relevant existing schemes. The results obtained from both the security and performance analyses affirm the superiority of the proposed scheme.

INDEX TERMS Internet of drones, proxy signcryption, security, privacy, edge computing, HECC, random oracle model.

I. INTRODUCTION

Internet of Drones (IoD) is a network of interconnected drones that uses the Internet of Things (IoT) framework to provide users with real-time data access. They are equipped with all of the necessary electronic gadgets to execute their task effectively, including a communication module for relaying data to GS, sensors to collect data, memory to store the data gathered by the sensor, as well as computational and power resources [1]–[3]. Additionally, the key characteristics of drones, such as agility, low cost, and ease of deployment, make IoD an excellent choice for a number of military and civilian applications.

Although the IoD network has many advantages, it also has many vulnerabilities that must be tackled, the most significant of which are security and privacy issues [4]–[6]. Since the IoD networks are typically deployed for real-time applications in which users want to acquire real-time data from drones that are linked to a specified zone. As a result, there is high chances of security attacks, resulting in colossal damage to the information exchange operations within the network [7], [8]. An attacker or intruder may gain access to the keys and intercept communications. To access keys, the attacker may exploit a vulnerability in the IoD network and its application platforms. The attacker may fabricate

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Khurram Khan.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

or modify this information, leading to misdirection of the receivers. Since IoD access control is such an important parameter, security issues regarding access and authorization should be highlighted [9]–[12]. This implies that data in transit must be secured for confidentiality, integrity, and authenticity [13]–[18].

In general, the energy, sensing, communication and computing capabilities of drones in an IoD network are minimal. As a consequence, drones are experiencing difficulties performing resource-intensive applications on time. For example. IoD can be used in remote areas to assist IoT devices in capturing massive amounts of data. Data gathered from the same platform may be too large to be processed by the same drones doing the same mission. Fortunately, the Fifth Generation (5G) wireless cellular network offers Multi-access Edge Computing (MEC) facility, which will help overcome this barrier [19], [20]. As an outcome, MEC will alleviate resource-constrained drones from heavy computational activities while embedded in an IoD environment and utilizing a 5G cellular network [21], [22]. Instead, computationally expensive operations will be offloaded to the cloud server for further processing. Furthermore, when the drone-cells relay the data, the available data may be temporarily stored for retrieval by either the drones or the ground devices. Thus, the MEC paves the way for a wide range of applications that specifically require a real-time response.

The data transfer from drones to a cloud server is subjected to various cyber physical attacks by hackers, resulting in the leakage of confidential information. To address these problems, an identity-based proxy signcryption (IDPS) scheme may be used, which allows for outsourcing decryption and member revocation. Drone users may regard the edge node device as a proxy signer in the IoD network, allowing it to perform proxy signcryption on transmitted data to ensure data privacy and security. Finally, the ciphertext is offloaded to the Cloud Server by the proxy signcryptor (CS). The cloud service provides outsourcing decryption after the data visitor sends a download ciphertext request to CS, and the data receiver obtains the plaintext with just a few estimates. When an unauthorized user attempts to enter data, the user identity value ID is added to a list of revocations, and the unauthorized user is identified.

Some computationally tough schemes, such as Rivest–Shamir–Adleman (RSA), bilinear pairing, and Elliptic Curve Cryptosystems (ECC), have been used to test the security and efficiency of the IDPS scheme in the literature. RSA proposes a large factorization-based approach that uses a 1024-bit large key. Furthermore, high pairing and map-to-point feature computations afflict bilinear pairing. Furthermore, ECC is distinguished by its smaller key size of 160 bits. However, in the IoD setting, a 160-bit key is still not a viable choice for drones. As a result, a more advanced version of the ECC, hyperelliptic curve cryptography (HECC), was proposed. The HECC uses an 80-bit key and guarantees the elliptic curve, bilinear pairing, and RSA security features. Therefore, it is an excellent choice for the IoD network.

Based on the above discussions, the authors propose an identity-based proxy signcryption scheme for IoD in this article. The proposed scheme is based on the HECC, which reduces power consumption while increasing network computation efficiency, making it suitable for a wide variety of devices, including sensors and drones. The following are some of the significant contributions of our research work that set it apart from its counterpart work in this paper:

- We propose an identity-based proxy signcryption for IoD network by incorporating the concepts of ID-based signcryption and proxy signature schemes.
- In the IoD setting, the scheme facilitates member revocation and outsourced decryption, making it a safer and more effective option.
- The proposed scheme employs the HECC concept for encryption and signature verification, while the Random Oracle Model (ROM) ensures security endurance.
- Finally, a comparison with the other schemes reveals that the proposed scheme is better in terms of both computational and communication costs.

The remainder of the article is organized as follows. Related work is presented in Section II. The preliminaries are provided in Section III. The network model and syntax are presented in section IV. The proposed scheme is defined in Section V. Part VI is dedicated to security analysis. Performance compassion is discussed in Section VII. The concluding thoughts can be found in section VIII.

II. RELATED WORK

In 1996, Mambo *et al.*[23] became the first to present the idea of proxy signature. The proxy signature scheme is based on the idea that the original signer delegated signing authority to the proxy signer, and the proxy signer then issues a valid signature on the side of original signer. Proxy signcryption is a combination of the proxy signature concept and the signcryption algorithm. In 2004, Li and Chen [24] proposed an ID-based proxy signcryption scheme. Wang *et al.*[25], on the other hand, determined that Li and Chen [24] scheme did not adhere to the rigorous requirements of high unforgeability and forward security. A year later, in 2005, Wang and Cao [26] provided an effective IDPS scheme without a secure channel. Wang and Cao [26] used bilinear pairing to create an identity-based proxy signature and proxy signcryption in the same year. Bilinear pairing was also used in the proposed scheme, which is a computationally intensive process. Swapna *et al.*[27] suggested a bilinear pairings-based ID-based proxy signcryption (ID-PSC) scheme. This scheme is public-verifiable, forward secure, and much more effective in terms of computational overhead.

Yu *et al.*[28] built an identity-based proxy signcryption scheme using the universally composable (UC) paradigm (IBPSP). Using the random oracle model, the author proved that their protocol possesses semantic security under the gap bilinear Dife-Hellman and computational Dife-Hellman assumptions. Furthermore, in [29] an

TABLE 1. Notation table.

No	Notation	Explanations
1	$\mathcal{HYEC}$	hyper elliptic curve of genius greater or equals to 2
2	∂	security parameter having $\partial \geqslant 2^{80}$
3	PKG	private key generator
4	β and α	master public and private key of PKG
5	n	large prime number belonging to $\mathcal{HYEC}$ having value be $n \geqslant 2^{80}$
6	$\mathcal{H}^1, \mathcal{H}^2, \mathcal{H}^3, \mathcal{H}^3$	cryptographic hash functions with the property of irreversibility
7	OA, PA, and RA	original actor, proxy actor, and receiver actor
8	Υ^{OA}, Ω^{OA}	public and private key of original actor
9	Υ^{PA}, Ω^{PA}	public and private key of proxy actor
10	Υ^{RA}, Ω^{RA}	public and private key of receiver actor
11	m^w	warrant message generated by original actor
12	ID^{OA}, ID^{PA}, ID^{RA}	identity of original actor, proxy actor, and receiver actor
13	$\mathcal{C}$	cipher text generated by proxy actor
14	$\oplus$	used for scrambling and decryptions
15	φ	represents the signed delegated text from original actor
16	ψ	represents the proxy signcryption ciphertext from proxy actor
17	$\mathcal{K}$	represents the scrambling and decryptions key
18	$\mathcal{D}$	Devisor of $\mathcal{HYEC}$
19	ξ	Advantages of adversary/opponent
20	$\mathcal{O}$	Represents opponent

identity-based signcryption mechanism to safeguard the cloud delegation process. The proxy agent uses a proxy key to produce encrypted messages and uploads the encrypted messages to the CSP, where it can be read and checked later. The scheme proposed in [29] was also based on bilinear pairing and therefore failed to meet the requirement for drones. A novel identity-based proxy signcryption (IBPS) approach employing ECC is presented in [30] to decrease the intensive mathematical operations involved in bilinear pairing approach. Finally, Yang *et al.*[31] offered an identity-based proxy signcryption scheme for drones that allows member revocation and outsourced decryption, claiming that their scheme is simpler and more reliable than previous schemes. Our work basically supplements the work done by Yang *et al*. [31]. The adaption of HECC, which requires an 80-bit key size and is far lower than that required by ECC and bilinear pairing, is a clear advantage of our scheme.

III. PRELIMINARIES

This section includes formal definitions as well as the notions used in the proposed scheme in table form.

Definition 1: Assume an arbitrary value $(\mathcal{D}, \mathcal{N}.\mathcal{D})$, attacker job is to extract the unknown values $(\mathcal{N})$; said to be a Hyper Elliptic Curve Discrete Logarithm Problem (HECDP).

Definition 2: Assume an arbitrary value $(\mathcal{D}, \mathcal{N}.\mathcal{D}, \mathcal{P}.\mathcal{D})$, attacker job is to extract the unknown values $(\mathcal{N}, \mathcal{P})$; said to be a Hyper Elliptic Curve Diffie-Hellman problem (HCDHPM).

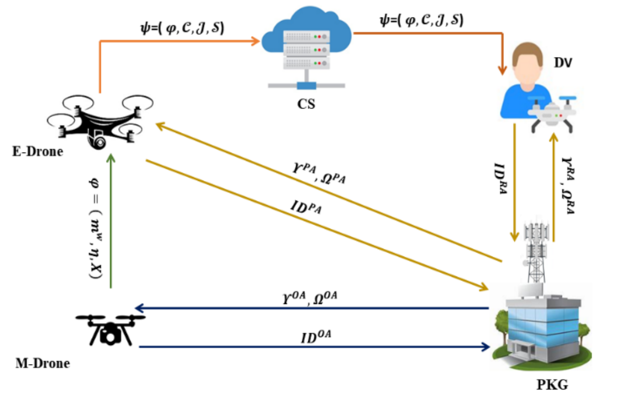

FIGURE 1. Network model of the proposed scheme.

IV. NETWORK MODEL AND SYNATX

In this section, we will define the network model and syntax of the proposed scheme.

A. NETWORK MODEL

The proposed network model, as shown in Fig. 1, is made up of two types of drones: member Drones (M-Drones) and edge Drones (E-Drones). M-Drones are in charge of completing monitoring tasks in their designated zones. On the other hand, Edge Drones (E-Drones) are in charge of gathering and offloading M-Drone data to Cloud Servers (CS) with multi-access edge computing capabilities. The E-Drone is equipped with 5G and Wi-Fi wireless technologies in order to connect it to the CS and offer a hotspot service to the M-Drones. The M-Drones communicate with one another using Wi-Fi. The main purpose for using a hybridized system is to take use of the best aspects of both technologies. The following are the main entities that execute the proposed algorithm:

- **Private Key Generator (PKG):** A trustworthy authority that uses identity information of the user to generate their private key.
- **Member Drone (M-Drone):** An entity (Original Actor) wishes to entrust its signcryption authority to a proxy signcryptor (E-Drone).
- **Edge Drone (E-Drone):** An entity (Proxy Actor) that, on behalf of the E-Drone, produces a signcrypted message and uploads it to a trusted cloud service provider (CSP) for further processing and storage using special information known as a "proxy key."
- **Cloud Server (CS):** An entity, who sends the signcrypted ciphertext to authorized users and provides storage and high processing facilities.
- **Data Visitor (DV):** An entity (Receiver Actor) that can retrieve data from the IoD network via the Internet at any time and from any location, restore the message content, and check its validity.

B. SYNTAX

The five algorithms that make up the proposed scheme syntax are Setup, Extract, Delegation Generation, Proxy

Signcryption, and Proxy Un-signcryption. The descriptions for each step are listed below:

- **Setup:** PKG computes β and $\mathcal{X}$ after taking the security parameter 1^{∂} as an input during the setup phase, and then publishes $\mathcal{X}$ in the network.
- **Extract:**For the identity ID^i, PKG calculates σ^i and Ω^i. The PKG then sends public and private key as (Y^i, Ω^i) using a secure channel to an actor with identity ID^i.
- **Delegation Generation:** The original actor **(**OA**),** computes η and X. Then, it transmits φ to proxy actor (PA).
- **Proxy Signcryption:** Upon receiving $\varphi = (m^w, \eta, X)$, PA performs the computational steps for verification of φ and generation of $\mathcal{C}, \mathcal{J}, \mathcal{S}$.
- **Proxy Un-Signcryption:** Upon receiving $\psi = (\varphi, \mathcal{C}, \mathcal{J}, \mathcal{S})$, RA performs the computational steps for verification of ψ and decryption of $\mathcal{C}$.

V. PROPOSED SCHEME

The five algorithms of the proposed scheme are described in detail in this section, which are made through the following computational steps:

- **Setup:** Given 1^{∂} as $\mathcal{HYEC}$ security parameter, PKG choose $\alpha \in \{1, 2, 3, \ldots, n\}$ randomly and compute $\beta = \alpha.\mathcal{D}$, where $\mathcal{D}$ is the devisor on $\mathcal{HYEC}$. Then the PKG set $\mathcal{X} = \{\beta, \mathcal{D}, \mathcal{HYEC}, n \gtrsim 2^{80}, \mathcal{H}^1, \mathcal{H}^2, \mathcal{H}^3, \mathcal{H}^3\}$ as a set of system parameters, where $\mathcal{H}^1, \mathcal{H}^2, \mathcal{H}^3, \mathcal{H}^3$ are the cryptographic hash functions with the property of irreversibility. Moreover, PKG publishes $\mathcal{X}$ in the IoD network.
- **Extract:**For the identity ID^i, PKG calculates $Y^i = \gamma^i.\mathcal{D}$, $\sigma^i = \mathcal{H}^1(ID^i, Y^i)$, and $\Omega^i = \gamma^i + \sigma^i.\alpha$, where $\gamma^i \in \{1, 2, 3, \ldots, n\}$. The PKG then sends the public and private keys as (Y^i, Ω^i) using a secure channel to an actor with identity ID^i.
- **Delegation Generation:** Here, original actor (OA**),** computes $\eta = \Phi.\mathcal{D}$ and $X = \Phi + \delta.\ \Omega^{OA}$, where $\Phi \in \{1, 2, 3, \ldots, n\}$ and $\delta = \mathcal{H}^2(ID^{OA}, ID^{PA}, Y^{OA}, Y^{PA}, m^w, \eta)$. Then, it transmits $\varphi = (m^w, \eta, X)$ to proxy actor (PA).
- **Proxy Signcryption:**Upon receiving $\varphi = (m^w, \eta, X)$, PA performs the following steps for verification of φ and generation of proxy signcryption ciphertext $\psi = (\varphi, \mathcal{C}, \mathcal{J}, \mathcal{S})$.
  1. Accomplish $\delta = \mathcal{H}^2(ID^{OA}, ID^{PA}, Y^{OA}, Y^{PA}, m^w, \eta)$ and compare $X.\mathcal{D} = \eta + \delta(\sigma^{OA}.\beta + Y^{OA})$, if it is satisfied then it performs proxy signcryption process
  2. Compute $\mathcal{J} = \mathcal{G}.\mathcal{D}$ and $\mathcal{V} = \mathcal{G}.\left(\sigma^{RA}.\beta + Y^{RA}\right)$, where $\mathcal{G} \in \{1, 2, 3, \ldots, n\}$
  3. Calculate $\mathcal{C} = \mathcal{M} \oplus \mathcal{K}$, where $\mathcal{K} = \mathcal{H}^3(\mathcal{V}, \mathcal{J}, ID^{OA}, ID^{PA}, ID^{RA}, Y^{OA}, Y^{PA}, Y^{RA})$.
  4. Compute $\mathcal{S} = \mathcal{G} + \mathcal{U}.\ \Omega^{PA}$, where $\mathcal{U} = \mathcal{H}^4(\mathcal{M}, \varphi, \mathcal{V}, \mathcal{J}, ID^{OA}, ID^{PA}, ID^{RA}, Y^{OA}, Y^{PA}, Y^{RA})$
  5. Send $\psi = (\varphi, \mathcal{C}, \mathcal{J}, \mathcal{S})$ to receiver actor (RA).
- **Proxy Un-signcryption:**Upon receiving $\psi = (\varphi, \mathcal{C}, \mathcal{J}, \mathcal{S})$, RA perform the following steps for verification of ψ and decryption of $\mathcal{C}$.
  1. Compute $\mathcal{V} = \Omega^{RA}.\mathcal{J}$ and $\mathcal{K} = \mathcal{H}^3(\mathcal{V}, \mathcal{J}, ID^{OA}, ID^{PA}, ID^{RA}, Y^{OA}, Y^{PA}, Y^{RA})$
  2. Decrypt $\mathcal{M} = \mathcal{C} \oplus \mathcal{K}$ and compute $\mathcal{U} = \mathcal{H}^4(\mathcal{M}, \varphi, \mathcal{V}, \mathcal{J}, ID^{OA}, ID^{PA}, ID^{RA}, Y^{OA}, Y^{PA}, Y^{RA})$
  3. Checking whether $\mathcal{S}.\mathcal{D} = \mathcal{J} + \mathcal{U}(\sigma^{PA}.\beta + Y^{PA})$ is hold.

A. CORRECTNESS ANALYSIS

PA can verify $\varphi = (m^w, \eta, X)$ using $X.\mathcal{D} = \eta + \delta\left(\sigma^{OA}.\beta + Y^{OA}\right)$, and the process is carried out as follows:

$X.\mathcal{D} = \eta + \delta\left(\sigma^{OA}.\beta + Y^{OA}\right) = X.\mathcal{D} = \mathcal{D}.(\Phi + \delta.\ \Omega^{OA}) = (\Phi.\mathcal{D} + \delta.\ \Omega^{OA}\mathcal{D}) = (\eta + \delta.\left(\gamma^{OA} + \sigma^{OA}.\alpha\right).\mathcal{D}) = (\eta + \delta.\left(\gamma^{OA}.\mathcal{D} + \sigma^{OA}.\alpha.\mathcal{D}\right)) = (\eta + \delta.\left(Y^{OA} + \sigma^{OA}.\beta\right)) = \eta + \delta\left(\sigma^{OA}.\beta + Y^{OA}\right)$ proved

RA can recover $\mathcal{K}$ and $\mathcal{M}$ using $\mathcal{V} = \Omega^{RA}.\mathcal{J}$, and verify $\psi = (\varphi, \mathcal{C}, \mathcal{J}, \mathcal{S})$, using $X\mathcal{S}.\mathcal{D} = \mathcal{J} + \mathcal{U}(\sigma^{PA}.\beta + Y^{PA})$, the process is carried out as follows:

It first recovers $\mathcal{V} = \Omega^{RA}.\mathcal{J} = \mathcal{G}.\left(\sigma^{RA}.\beta + Y^{RA}\right) = \mathcal{G}.\left(\sigma^{RA}.\alpha.\mathcal{D} + \gamma^{RA}.\mathcal{D}\right) = \mathcal{G}.\mathcal{D}\left(\sigma^{RA}.\alpha + \gamma^{RA}\right) = \mathcal{G}.\mathcal{D}\left(\Omega^{RA}\right) = \mathcal{J}\left(\Omega^{RA}\right) = \Omega^{RA}.\mathcal{J}$ proved

Then it verifies $\mathcal{S}.\mathcal{D} = \mathcal{J} + \mathcal{U}(\sigma^{PA}.\beta + Y^{PA})$

$$\mathcal{S}.\mathcal{D} = (\mathcal{G} + \mathcal{U}.\ \Omega^{PA}).\mathcal{D} = (\mathcal{G}.\mathcal{D} + \mathcal{U}.\ \Omega^{PA}.\mathcal{D})$$
$$= (\mathcal{J} + \mathcal{U}.\ \Omega^{PA}.\mathcal{D}) = (\mathcal{J} + \mathcal{U}(\gamma^{PA} + \sigma^{PA}.\alpha).\mathcal{D})$$
$$= \mathcal{J} + \mathcal{U}(\gamma^{PA}.\mathcal{D} + \sigma^{PA}.\alpha.\mathcal{D}) \text{ proved}$$
$$= \mathcal{J} + \mathcal{U}(Y^{PA} + \sigma^{PA}.\beta) \text{ hence proved.}$$

VI. SECURITY ANALYSIS

A. DEFINITIONS

This phase comprises the definitions of two games e.g., indistinguishability against adaptive selected scrambled text attacks (IAA-IDPSC-SSA) and existential forgery for adaptive selected plaintext attacks (EF-IDPSC-SPA) regarding confidentiality and unforgeability of a proposed identity based signcryption scheme. The following Game 1 and Game 2 present that how the proposed scheme provides confidentiality and unforgeability when it plays between the polynomial time opponent $\mathcal{O}$ and its helper $\mathcal{Q}$.

Game 1: The opponent $\mathcal{O}$ and helper $\mathcal{Q}$ can play this game to solve HCDHPM.

Setup: Helper $\mathcal{Q}$ set $\mathcal{X}$ as a set of system parameters, and send $\mathcal{X}$ to opponent $\mathcal{O}$.

Queries: *In this stage,* opponent $\mathcal{O}$ enquiring for the following queries such as $\mathcal{H}^i$ queries, extract queries that further includes public and private key queries (q^{PB}, q^{PR}), delegation generation queries (q^{DG}), and proxy signcryption queries (q^{PS}).

$\mathcal{H}^i$ **Queries:**The opponent $\mathcal{O}$ enquired for the hash value, $\mathcal{Q}$ responds with requested value, when it is exists in the list (LH^i), otherwise $\mathcal{Q}$ responds with the randomly chosen value.

Extract Queries: When opponent $\mathcal{O}$ enquired for (q^{PB}, q^{PR}), $\mathcal{Q}$ responded with the public and private key by calling Extract algorithm.

Delegation Generation Queries: If opponent $\mathcal{O}$ submit ID^{OA}, $\mathcal{Q}$ responds with φ using Delegation Generation algorithm to opponent $\mathcal{O}$.

Proxy Signcryption Queries: If opponent $\mathcal{O}$ enquired and give $\mathcal{M}$ along with ID^{OA}, ID^{PA}, and ID^{RA}, $\mathcal{Q}$ responds with ψ.

Proxy Un-Signcryption Queries: If opponent $\mathcal{O}$ give ψ, $\mathcal{Q}$ responded in a normal way by calling Proxy Un-signcryption algorithm.

Challenge: If opponent $\mathcal{O}$ give $\mathcal{M}^1$ and $\mathcal{M}^2$ along with ID^{RA}, ID^{PA}, $\mathcal{Q}$ pick $g \in \{0,1\}$ responds with ψ=($\varphi, \mathcal{C}, \mathcal{J}, \mathcal{S}$) to opponent $\mathcal{O}$.

Then opponent $\mathcal{O}$ can continue with$\mathcal{H}^i$ queries, extract queries public key queries (q^{PB}), delegation generation queries (q^{DG}), proxy signcryption queries (q^{PS}), and proxy un-signcryption queries.

Guess: opponent $\mathcal{O}$ output $g^{/}$ and compare if $g^{/} = g$, then $\mathcal{O}$ succeeded.

Game 2: The opponent $\mathcal{O}$ and helper $\mathcal{Q}$ can play this game to solve HECDP.

Setup: Helper $\mathcal{Q}$ send $\mathcal{X}$ to opponent $\mathcal{O}$.

Queries: In this stage, opponent $\mathcal{O}$ enquiring for $\mathcal{H}^i$ queries, extract queries that further includes public and private key queries (q^{PB}, q^{PR}), delegation generation queries (q^{DG}), and proxy signcryption queries (q^{PS}) same as *Game 1*.

Forgery*:* Opponent $\mathcal{O}$, outputs will be entertained in the following two cases.

Case 1:Helper $\mathcal{Q}$ can get two delegation signatures X and X^*. So, it can get the private key as $\Omega^{OA} = \frac{X+X^*}{(\delta^*-\delta)}$, if it gets then it means that opponent $\mathcal{O}$ is successful.

Case 2: helper $\mathcal{Q}$ can get two delegation signatures $\mathcal{S}$ and $\mathcal{S}^*$, So, it can get the private key as $\Omega^{PA} = \frac{\mathcal{S}+\mathcal{S}^*}{(\mathcal{U}^*-\mathcal{U})}$, if it gets then it means that opponent $\mathcal{O}$ is successful.

From the process we can define three events that are E^1: the helper $\mathcal{Q}$ successful in queries,E^2: the helper $\mathcal{Q}$ successful in *Proxy Un-Signcryption Queries*, and E^3 $ID^{PA} = ID^*$.

B. PROOFS

This section includes the proofs of two games that are indistinguishability against adaptive selected scrambled text attacks (IAA-IDPSC-SSA) and existential forgery for adaptive selected plaintext attacks (EF-IDPSC-SPA) regarding confidentiality and unforgeability of the proposed scheme. The following Game 1 and Game 2 present that how the proposed scheme provides confidentiality and unforgeability when it plays between the polynomial-time opponent $\mathcal{O}$ and its helper $\mathcal{Q}$.

Game 1: Using ROM**,** if in IAA-IDPSC-SSA opponent $\mathcal{O}$ has the capability to two genuine scrambled texts during this Game with the acceptable advantage ξ, and enquiring at utmost $\mathcal{H}^i$ queries, extract queries that further includes public and private key queries (q^{PB}, q^{PR}), delegation generation queries (q^{DG}), and proxy signcryption queries (q^{PS}), then helper $\mathcal{Q}$ can solve HCDHPM with the benefits of $\xi^* \succeq \xi\left(1-\frac{q^{PR}}{q^{PB}}\right)\left(1-\frac{1}{2^{\partial}}\right).\frac{1}{q^{PB}-q^{PR}}$.

Proof: Assume that the helper $\mathcal{Q}$ obtains an arbitrary HCDHPM instance ($\mathcal{D}, \mathcal{N}.\mathcal{D}, \mathcal{P}.\mathcal{D}$), then $\mathcal{Q}$ jobs is to extract the unknown values ($\mathcal{N}, \mathcal{P}$).

Setup: Helper $\mathcal{Q}$ set $\mathcal{X} = \{\beta,\ \mathcal{D},\ \mathcal{HYEC},\ n \succcurlyeq 2^{80}, \mathcal{H}^1, \mathcal{H}^2, \mathcal{H}^3, \mathcal{H}^4\}$ as a set of system parameters, send $\mathcal{X}$ to opponent $\mathcal{O}$.

Queries: *In this stage* opponent $\mathcal{O}$ enquiring for the following queries

$\mathcal{H}^1$ **Queries:** The opponent $\mathcal{O}$ enquired for the triple(ID^i, Y^i, σ^i), $\mathcal{Q}$ responds with σ^i, when it is exists in the list (LH^1), otherwise $\mathcal{Q}$ responds with σ^i, where σ^i is the randomly chosen value and includes (ID^i, Y^i, σ^i) to LH^1.

$\mathcal{H}^2$ **Queries:** The opponent $\mathcal{O}$ enquired for (ID^i, Y^i, m^w, η, δ), $\mathcal{Q}$ responds with δ, when it is exists in the list (LH^2), otherwise $\mathcal{Q}$ responds with δ, where δ is the randomly chosen value and includes (ID^i, Y^i, m^w, η, δ) to LH^2.

$\mathcal{H}^3$ **Queries:** The opponent $\mathcal{O}$ enquired for ($\mathcal{V}$, $\mathcal{J}$,ID^i, $Y^i, \mathcal{K}$), $\mathcal{Q}$ responds with $\mathcal{K}$, when it is exists in the list (LH^3), otherwise $\mathcal{Q}$ responds with $\mathcal{K}$, where $\mathcal{K}$ is the randomly chosen value and includes ($\mathcal{V}$, $\mathcal{J}$,ID^i, $Y^i, \mathcal{K}$) to LH^3.

$\mathcal{H}^4$ **Queries:** The opponent $\mathcal{O}$ enquired for ($\mathcal{M}$,φ, $\mathcal{U}, \mathcal{V}$, $\mathcal{J}$,ID^i, Y^i), $\mathcal{Q}$ responds with $\mathcal{U}$, when it is exists in the list (LH^4), otherwise $\mathcal{Q}$ responds with $\mathcal{U}$, where $\mathcal{U}$ is the randomly chosen value and includes ($\mathcal{M}$,$\varphi, \mathcal{U}, \mathcal{V}$, $\mathcal{J}$,ID^i, Y^i) to LH^4.

Extract Queries: It further divided in public and private key queries (q^{PB}, q^{PR}), when opponent $\mathcal{O}$ enquired for q^{PB}, if $ID^i = ID^j$, $\mathcal{Q}$ set Y^j= $\mathcal{N}.\mathcal{D}$, otherwise it processes $Y^i = \gamma^i.\mathcal{D}$, where $\gamma^i \in \{1, 2, 3, \ldots, n\}$ and responded to opponent $\mathcal{O}$. Then update L^{PB} accordingly. Further, when opponent $\mathcal{O}$ enquired for q^{PR}, if $ID^i = ID^*$, $\mathcal{Q}$ aborts executions, otherwise it set $\Omega^i = \gamma^i + \sigma^i.\alpha$ and responded to opponent $\mathcal{O}$. Then update q^{PR} accordingly.

Delegation Generation Queries: If opponent $\mathcal{O}$ enquired for q^{DG}, if $ID^{OA} = ID^*$, $\mathcal{Q}$ responds with φ using Delegation Generation algorithm to opponent $\mathcal{O}$, otherwise it responded in the following way. It Compute $\eta = X + \delta(\sigma^{OA}.\beta + Y^{OA})$, where δ, $X \in \{1, 2, 3, \ldots, n\}$, set $\varphi = (m^w, \eta, X)$ and responds to opponent $\mathcal{O}$.

Proxy Signcryption Queries: If opponent $\mathcal{O}$ enquired and give $\mathcal{M}$ along with ID^{OA}, ID^{PA}, and ID^{RA}, if $ID^{PA} = ID^*$, $\mathcal{Q}$ responds as it compute $\mathcal{J} = \mathcal{G}.\mathcal{D}$ and $\mathcal{V} = \mathcal{G}.\left(\sigma^{RA}.\beta + Y^{RA}\right)$, where $\mathcal{G} \in \{1, 2, 3, \ldots, n\}$, calculate $\mathcal{C} = \mathcal{M} \oplus \mathcal{K}$, where $\mathcal{K} \in \{1, 2, 3, \ldots, n\}$, compute $\mathcal{S}$= $\mathcal{G} + \mathcal{U}.\Omega^{PA}$, where $\mathcal{U} \in \{1, 2, 3, \ldots, n\}$, and send ψ^*=($\varphi, \mathcal{C}, \mathcal{J}, \mathcal{S}$) to opponent $\mathcal{O}$. Otherwise, it responded in a normal way by calling proxy signcryption algorithm.

Proxy Un-Signcryption Queries: If opponent $\mathcal{O}$ enquired, if $ID^{RA} \neq ID^*$, $\mathcal{Q}$ responded in a normal way by calling Proxy Un-signcryption algorithm.

Challenge: If opponent $\mathcal{O}$ give $\mathcal{M}^1$ and $\mathcal{M}^2$ along with ID^{RA}, ID^{PA}, if $ID^{PA} = ID^*$, $\mathcal{Q}$ pick $g \in$ 0,1responds

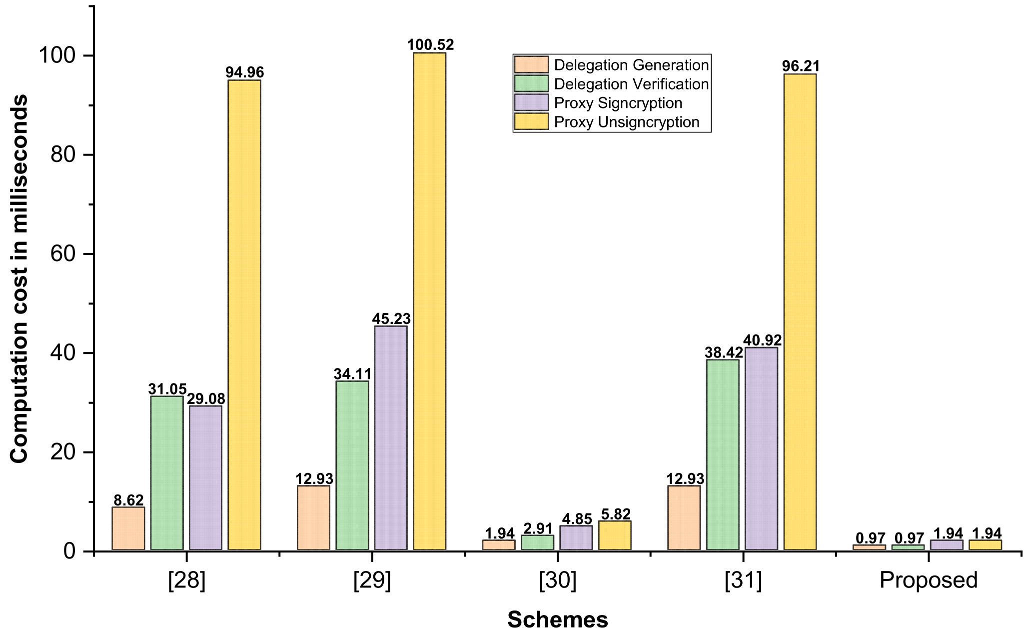

FIGURE 2. Comparison of computation cost (in ms).

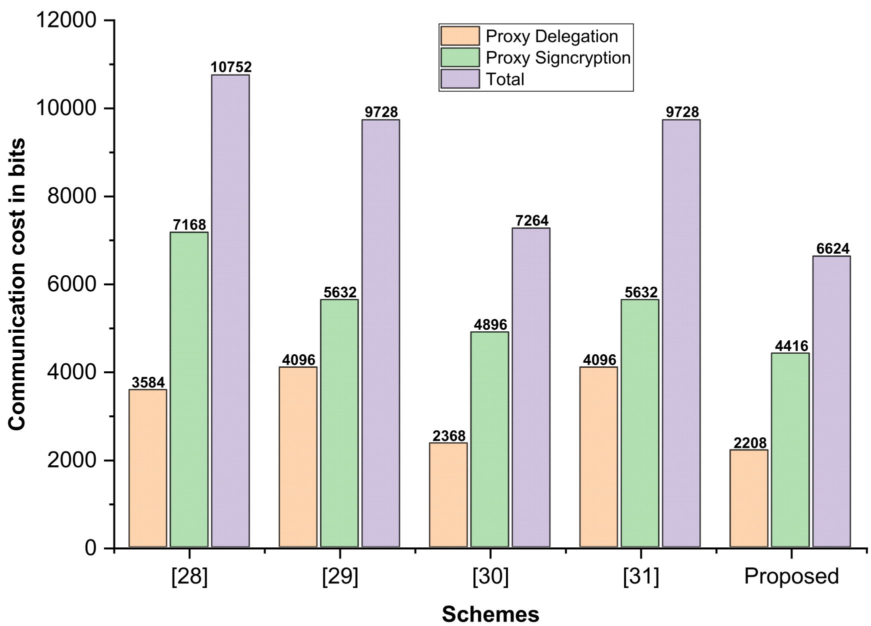

FIGURE 3. Comparison of communication cost (in bits).

as, it compute $\mathcal{J} = \mathcal{P}.\mathcal{D}$ and $\mathcal{V} = \mathcal{P}.\left(\sigma^{RA}.\beta + Y^{RA}\right)$, where $\mathcal{P} \in \{1, 2, 3, \ldots, n\}$, calculate $\mathcal{C} = \mathcal{M} \oplus \mathcal{K}$, where $\mathcal{K} \in \{1, 2, 3, \ldots, n\}$, compute $\mathcal{S} = \mathcal{P} + \mathcal{U}.\ \Omega^{PA}$, where $\mathcal{U} \in \{1, 2, 3, \ldots, n\}$, and send ψ=($\varphi, \mathcal{C}, \mathcal{J}, \mathcal{S}$) to opponent $\mathcal{O}$. Then opponent $\mathcal{O}$ can continue with$\mathcal{H}^i$ queries, extract queries public key queries (q^{PB}), delegation generation queries (q^{DG}), proxy signcryption queries (q^{PS}), and proxy un-signcryption queries.

Guess: opponent $\mathcal{O}$ output $g^{/}$ and compare if $g^{/} = g$, then $\mathcal{O}$ succeeded and find the solution for HCDHPM instance $(\mathcal{D}, \mathcal{N}.\mathcal{D}, \mathcal{P}.\mathcal{D})$, otherwise $\mathcal{O}$ failed.

From the process, we can define three events that are E^1: the helper $\mathcal{Q}$ successful in q^{PR} and its probability as $\left(1 - \frac{q^{PR}}{q^{PB}}\right)$, E^2: the helper $\mathcal{Q}$ successful in *Proxy Un-Signcryption Queries* and its probability as$\left(1 - \frac{1}{2^{\partial}}\right)$, and E^3: the helper $\mathcal{Q}$ successful in *Challenge* step and its probability as$\frac{1}{q^{PB} - q^{PR}}$. So, we have the collective probability as$\xi^* \succeq \xi \left(1 - \frac{q^{PR}}{q^{PB}}\right)\left(1 - \frac{1}{2^{\partial}}\right) \cdot \frac{1}{q^{PB} - q^{PR}}$.

Game 2: Using ROM, if the opponent $\mathcal{O}$has the capability to existential forgery for adaptive selected plaintext

TABLE 2. Computational cost.

Schemes	Delegation Generation	Delegation Verifications	Proxy Signcryption	Proxy Unsigncryption
Yu et al. [28]	2 BPBM	2 BP+ 1E	1 BP+ 1E + 3 BPBM	6BP+ 1E + 1 BPBM
Hundera et al. [29]	3 BPBM	2 BP+ 1BPBM	2 BP+ 2E + 3 BPBM	6 BP+ 2E + 2 BPBM
Guo et al. [30]	2 ESM	3 ESM	5 ESM	6 ESM
Yang et al. [31]	3 BPBM	2 BPBM +2 BP	2 BP+ 2E + 2 BPBM	6 BP+ 2E + 1 BPBM
Proposed	2 HSM	2 HSM	4 HSM	4 HSM

Note: BPBM= bilinear pairing-based multiplications, E= exponentiations, BP= bilinear pairing, ESM= elliptic curve devisor scalar multiplications and HSM= hyper elliptic curve devisor scalar multiplications

TABLE 3. Computational cost in millisecond.

Schemes	Delegation Generation	Delegation Verification	Proxy Signcryption	Proxy Unsigncryption
Yu et al. [28]	8.62	31.05	29.08	94.96
Hundera et al. [29]	12.93	34.11	45.23	100.52
Guo et al. [30]	1.94	2.91	4.85	5.82
Yang et al. [31]	12.93	38.42	40.92	96.21
Proposed	0.97	0.97	1.94	1.94

TABLE 4. Communication cost.

Schemes	Proxy Delegation	Proxy Signcryption	Total
Yu et al. [28]	1|M|+ 1|G|+ 1|$\mathcal{H}$|	2|M|+ 3|G|	3|M|+ 4|G|+ 1|$\mathcal{H}$|
Hundera et al. [29]	|M|+ 2|G|	2|M|+ 1|G|+ 1|$\mathcal{H}$|	3|M|+ 3|G|+ 1|$\mathcal{H}$|
Guo et al. [30]	|M|+ 2|q|	2|M|+ 5|q|	3|M|+ 7|q|
Yang et al. [31]	|M|+ 2|G|	2|M|+ 1|G|+ 1|$\mathcal{H}$|	3|M|+ 3|G|+ 1|$\mathcal{H}$|
Proposed	|M|+ 2|n|	2|M|+ 4|n|	3|M|+ 6|n|

TABLE 5. Communication cost in bits.

Schemes	Proxy Delegation	Proxy Signcryption	Total
Yu et al. [28]	3584	7168	10752
Hundera et al. [29]	4096	5632	9728
Guo et al. [30]	2368	4896	7264
Yang et al. [31]	4096	5632	9728
Proposed	2208	4416	6624

attacks (EF-IDPSC-SPA) during this Game with the acceptable advantage ξ, and enquiring at utmost $\mathcal{H}^i$queries, extract queries that further includes public and private key queries (q^{PB}, q^{PR}), delegation generation queries (q^{DG}), and proxy signcryption queries (q^{PS}), then helper $\mathcal{Q}$ can solve HECDP with the benefits of $\xi^* \geq \xi \left(1-\frac{q^{PR}}{q^{PB}}\right)\left(1-\frac{1}{2^{\partial}}\right)\cdot\frac{1}{q^{PB}-q^{PR}}$.

Proof: Assume that the helper $\mathcal{Q}$ obtains an arbitrary HECDP instance ($\mathcal{D}$, $\Omega^{OA}.\mathcal{D}$, $\Omega^{PA}.\mathcal{D}$), then $\mathcal{Q}$jobs is to extract the unknown values (Ω^{OA}, Ω^{PA}).

Setup: Helper $\mathcal{Q}$ send $\mathcal{X}$ to opponent $\mathcal{O}$.

Queries: In this stage opponent $\mathcal{O}$ enquiring for $\mathcal{H}^i$queries, extract queries that further includes public and private key queries (q^{PB}, q^{PR}), delegation generation queries (q^{DG}), and proxy signcryption queries (q^{PS}) same as *Game 1*.

Forgery: Opponent $\mathcal{O}$, outputs will be entertained in the following two cases.

Case 1: Helper $\mathcal{Q}$ can get two delegation signatures $X = \mathcal{P}+\delta.\ \Omega^{OA}$ and $X^*= \mathcal{P}+\delta^*.\ \Omega^{OA}$, so we have $X-\mathcal{P}-\delta.\ \Omega^{OA} - (X^*-\mathcal{P}-\delta^*.\ \Omega^{OA})= X-\mathcal{P}-\delta.\ \Omega^{OA} - X^*+\mathcal{P}+\delta^*.\ \Omega^{OA})= X+X^* = \delta^*.\ \Omega^{OA}-\delta.\ \Omega^{OA}= X+X^* = (\delta^*-\delta)\ \Omega^{OA}$. So, it can get the private key as $\Omega^{OA} = \frac{X+X^*}{(\delta^*-\delta)}$.

Case 2: Helper $\mathcal{Q}$ can get two delegation signatures $\mathcal{S} = \mathcal{G} + \mathcal{U}.\ \Omega^{PA}$ and $\mathcal{S}^*= \mathcal{G}+\mathcal{U}^*.\ \Omega^{PA}$, so we have $\mathcal{S}-\mathcal{G}-\mathcal{U}.\ \Omega^{PA} - (\mathcal{S}^*-\mathcal{G}-\mathcal{U}^*.\ \Omega^{PA})= \mathcal{S}-\mathcal{G}-\mathcal{U}.\ \Omega^{PA} - \mathcal{S}^*+\mathcal{G}+\mathcal{U}^*.\ \Omega^{PA})= \mathcal{S}+\mathcal{S}^* = \mathcal{U}^*.\ \Omega^{PA}-\mathcal{U}.\ \Omega^{PA}= \mathcal{S}+\mathcal{S}^* = (\delta^*-\delta)\ \Omega^{PA}$. So, it can get the private key as $\Omega^{PA} = \frac{\mathcal{S}+\mathcal{S}^*}{(\mathcal{U}^*-\mathcal{U})}$.

From the process, we can define three events that are E^1: the helper $\mathcal{Q}$ successful in queries and its probability as $\left(1-\frac{q^{PR}}{q^{PB}}\right)$,$E^2$: the helper $\mathcal{Q}$ successful

TABLE 6. Variables.

S. No	Variable	Value in bits
1	|M|	2048 bits
2	|G|	1024 bits
3	|q|	160 bits
4	$\|\mathcal{H}\|$	512 bits
5	|n|	80 bits

Note: M= plaintext, G = bilinear pairing bits, q = elliptic curve bits, $\mathcal{H}$= hash function and n =hyperelliptic curve

in *Proxy Un-Signcryption Queries* and its probability as$\left(1-\frac{1}{2^{\partial}}\right)$, and $E^3\ ID^{PA} = ID^*$ and its probability as$\frac{1}{q^{PB}-q^{PR}}$. So, we have the collective probability as$\xi^* \succeq \xi\left(1-\frac{q^{PR}}{q^{PB}}\right)\left(1-\frac{1}{2^{\partial}}\right)\cdot\frac{1}{q^{PB}-q^{PR}}$.

VII. PERFORMANCE COMPARISON

In this section, the proposed scheme is contrasted to the schemes proposed by Yu *et al.* [28], Hundera *et al.* [29], Guo and Deng [30], and Yang *et al.* [31] in terms of computation and communication costs. Table 2, Table 3 and Figure 2 provide the details of the cost comparison for computation, while Table 4, Table 5 and Figure 3 show the cost comparison for communication. Table 6 lists the variables that were used to calculate communication costs. A single ESM takes 0.97 milliseconds to process; bilinear pairing takes 14.90 milliseconds; BPBM takes 4.31 milliseconds; and E takes 1.25 milliseconds [32]. The HSM is assumed to be 0.48 milliseconds [33,34]. The computational performance is measured using the Multi-precision Integer and Rational Arithmetic C Library (MIRACL) [35]. To evaluate the effectiveness of the proposed scheme, the MIRACLE library is used to test the runtime of basic cryptographic operations up to 1000 times. The simulation results are obtained using a machine that meets the following specifications: Windows 7 Home Basic 64-bit Operating System [32], Intel Core i7- 4510U CPU @ 2.0 GHz, 8 GB RAM.

VIII. CONCLUSION

In this article, we proposed an identity-based proxy signcryption scheme for the IoD network. To effectively address the issue of data security and privacy during the transmission of data from drones to a cloud server, the proposed scheme advocates outsourcing decryption and member revocation. To assess the security toughness of the proposed scheme, we used formal security analysis technique i.e., the Random Oracle Model (ROM). In addition, the scheme is contrasted to its counterpart scheme in terms of computation and communication costs. The findings of the efficiency evaluation support the supremacy of the proposed scheme. In the future, we plan to propose a novel architecture in which the E-Drone acts as a cloud edge processing node for all the M-Drones, reducing the time it takes to transmit massive volumes of data to the cloud server.

REFERENCES

[1] M. A. Khan, A. Safi, I. M. Qureshi, and I. U. Khan, "Flying ad-hoc networks (FANETs): A review of communication architectures, and routing protocols," in *Proc. 1st Int. Conf. Latest Trends Electr. Eng. Comput. Technol. (INTELLECT)*, Nov. 2017, pp. 1–9.

[2] F. Noor, M. A. Khan, A. Al-Zahrani, I. Ullah, and K. A. Al-Dhlan, "A review on communications perspective of flying ad-hoc networks: Key enabling wireless technologies, applications, challenges and open research topics," *Drones*, vol. 4, no. 4, p. 65, Sep. 2020.

[3] M. A. Khan, I. M. Qureshi, I. U. Khan, A. Nasim, U. Javed, and W. Khan, "On the performance of flying ad-hoc networks (FANETs) with directional antennas," in *Proc. 5th Int. Multi-Topic ICT Conf. (IMTIC)*, Apr. 2018, pp. 1–8.

[4] M. Gharibi, R. Boutaba, and S. L. Waslander, "Internet of drones," *IEEE Access*, vol. 4, pp. 1148–1162, 2016.

[5] M. Singh, G. S. Aujla, and R. S. Bali, "ODOB: One drone one block-based lightweight blockchain architecture for Internet of drones," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Jul. 2020, pp. 249–254.

[6] M. Yahuza, M. Y. I. Idris, I. B. Ahmedy, A. W. A. Wahab, T. Nandy, N. M. Noor, and A. Bala, "Internet of drones security and privacy issues: Taxonomy and open challenges," *IEEE Access*, vol. 9, pp. 57243–57270, 2021.

[7] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks,"' *Sensors*, vol. 10, no. 3, pp. 2450–2459, Mar. 2010.

[8] S.-J. Horng, S.-F. Tzeng, Y. Pan, P. Fan, X. Wang, T. Li, and M. K. Khan, "B-SPECS+: Batch verification for secure pseudonymous authentication in VANET," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1860–1875, Nov. 2013.

[9] 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.*, vol. 6, no. 2, pp. 3572–3584, Apr. 2019.

[10] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, "Amassing the security: An ECC-based authentication scheme for Internet of drones," *IEEE Syst. J.*, early access, Mar. 1, 2021, doi: 10.1109/JSYST.2021.3057047.

[11] G. Choudhary, V. Sharma, T. Gupta, J. Kim, and I. You, "Internet of drones (IoD): Threats, vulnerability, and security perspectives," 2018, *arXiv:1808.00203*. [Online]. Available: http://arxiv.org/abs/1808.00203

[12] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of drones," *Comput. Commun.*, vol. 154, pp. 455–464, Mar. 2020.

[13] V. Odelu, A. K. Das, M. K. Khan, K.-K.-R. Choo, and M. Jo, "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts," *IEEE Access*, vol. 5, pp. 3273–3283, 2017.

[14] S.-F. Tzeng, S.-J. Horng, T. Li, X. Wang, P.-H. Huang, and M. K. Khan, "Enhancing security and privacy for identity-based batch verification scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3235–3248, Apr. 2017.

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

[16] S. Aggarwal and N. Kumar, "Path planning techniques for unmanned aerial vehicles: A review, solutions, and challenges," *Comput. Commun.*, vol. 149, pp. 270–299, Jan. 2020.
[17] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, "Certificateless public key authenticated encryption with keyword search for industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3618–3627, Aug. 2018.
[18] D. He, N. Kumar, N. Chilamkurti, and J.-H. Lee, "Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol," *J. Med. Syst.*, vol. 38, no. 10, pp. 1–6, Oct. 2014.
[19] Y. K. Tun, Y. M. Park, N. H. Tran, W. Saad, S. R. Pandey, and C. S. Hong, "Energy-efficient resource management in UAV-assisted mobile edge computing," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 249–253, Jan. 2021.
[20] P. Zhou, K. Shen, N. Kumar, Y. Zhang, M. M. Hassan, and K. Hwang, "Communication-efficient offloading for mobile edge computing in 5G heterogeneous networks," *IEEE Internet Things J.*, early access, Oct. 6, 2020, doi: 10.1109/JIOT.2020.3029166.
[21] M. A. Khan, I. M. Qureshi, I. Ullah, S. Khan, F. Khanzada, and F. Noor, "An efficient and provably secure certificateless blind signature scheme for flying ad-hoc network based on multi-access edge computing," *Electronics*, vol. 9, no. 1, p. 30, Dec. 2019.
[22] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi, F. Khanzada, H. Khattak, and M. A. Aziz, "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Inf. Syst.*, vol. 2020, pp. 1–15, Jul. 2020.
[23] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 79, no. 9, pp. 1338–1354, 1996.
[24] X. Li and K. Chen, "Identity based proxy-signcryption scheme from pairings," in *Proc. IEEE Int. Conf. Services Comput. (SCC)*, Sep. 2004, pp. 494–497.
[25] M. Wang, H. Li, and Z. Liu, "Efficient identity based proxy-signcryption schemes with forward security and public verifiability," in *Proc. ICCNMC*, in Lecture Notes in Computer Science, vol. 3619. Springer-Verlag, 2005, pp. 982–991.
[26] Q. Wang and Z. Cao, "Efficient ID-based proxy signature and proxy signcryption form bilinear pairings," in *Proc. Int. Conf. Comput. Inf. Sci.* Springer, 2005, pp. 167–172.
[27] G. Swapna, P. V. S. S. N. Gopal, T. Gowri, and P. V. Reddy, "An efficient ID-based proxy signcryption scheme," *Int. J. Inf. Netw. Secur.*, vol. 1, no. 3, pp. 200–206, Jul. 2012.
[28] H. Yu, Z. Wang, J. Li, and X. Gao, "Identity-based proxy signcryption protocol with universal composability," *Secur. Commun. Netw.*, vol. 2018, pp. 1–11, Dec. 2018.
[29] N. W. Hundera, Q. Mei, H. Xiong, and D. M. Geressu, "A secure and efficient identity-based proxy signcryption in cloud data sharing," *KSII Trans. Internet Inf. Syst.*, vol. 14, no. 1, pp. 455–472, 2020, doi: 10.3837/tiis.2020.01.025.
[30] H. Guo and L. Deng, "An identity based proxy signcryption scheme without pairings," *Int. J. Netw. Secur.*, vol. 22, no. 4, pp. 561–568, 2020.
[31] X. Yang, W. Xi, N. Ren, J. Wang, and M. Li, "Support outsourcing unsigncryption and member revocation identity-based proxy signcryption scheme with drone environment," *J. Phys., Conf. Ser.*, vol. 1828, no. 1, Feb. 2021, Art. no. 012119.
[32] C. Zhou, Z. Zhao, W. Zhou, and Y. Mei, "Certificateless key-insulated generalized signcryption scheme without bilinear pairings," *Secur. Commun. Netw.*, vol. 2017, pp. 1–17, Aug. 2017.
[33] M. A. Khan, I. Ullah, N. Kumar, O. S. Oubbati, I. M. Qureshi, F. Noor, and F. U. Khanzada, "An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4839–4851, May 2021, doi: 10.1109/TVT.2021.3055895.
[34] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi, F. U. Khanzada, and N. U. Amin, "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.
[35] Shamus Sofware. *MIRACL Library*. [Online]. Available: http://github.com/miracl/

MUHAMMAD ASGHAR KHAN received the Ph.D. degree in electronic engineering from the School of Engineering and Applied Sciences (SEAS), ISRA University, Islamabad. He is currently the Director-ORIC with the Department of Electrical Engineering, Hamdard University, Islamabad. He has more than 40 technical research articles in leading journals, such as the IEEE Transactions on Vehicular Technology, IEEE Transactions on Industrial Informatics, the IEEE Internet of Things Journal, and conferences. His main research interests include drones/UAVs, the IoT, e-health with a focus on networks, platforms, security, and applications and services. He is a reviewer for various journals published by IEEE, Elsevier, MDPI, and EURASIP. He has served as a guest editor for a number of international journals.

HABIB SHAH received the Ph.D. degree from the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, in 2013. He is currently an Assistant Professor with the Department of Computer Science, College of Computer Science, King Khalid University, Saudi Arabia. He has successfully published more than 42 articles in various international SCI and Scopus journals and conference proceedings. His research interests include artificial intelligence, learning algorithms, data mining techniques, time series analysis, numerical optimization, and latest research topics of computer science areas. He is an editorial board member, a guest editor, and a reviewer for various journals and conferences. He has served as a program committee member and a co-organizer for numerous international conferences/workshops. He is working on three research projects of KKU and KSA.

SAJJAD UR REHMAN (Member, IEEE) received the B.Sc. degree in electronics engineering from Iqra University, Karachi, Pakistan, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from King Saud University, Riyadh, Saudi Arabia, in 2018. He worked as a Lecturer with the Department of Electronics Engineering, Iqra University, Peshawar Campus, from 2007 to 2008. He worked as a Researcher with the Electrical Engineering Department, King Saud University, from 2008 to 2019. He worked as an Associate Professor with the Qurtuba University of Science and IT, D. I. Khan, Pakistan, from May 2019 to October 2019. He is currently an Associate Professor with Namal Institute, Mianwali, Pakistan. His research interests include the Internet of Things (IoT), advanced technologies in wireless communications, reconfigurable antennas and filter designing, and MIMO antennas. His awards and honors include the Kind Saud University College of Engineering Excellent Research Award, in 2012, 2015, and 2017. In 2013, he was awarded the General Prize by the Deanship of Graduate Studies, King Saud University, for his outstanding research performance.

NEERAJ KUMAR (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra, India. He is currently an Associate Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He is working with the Department of Computer Science and Information Engineering, Asia University, Taiwan, and the School of Computer Science, University of Petroleum and Energy Studies, Dehradun. He has more than 300 technical research articles in leading journals, such as the IEEE Transactions on Industrial Informatics, the IEEE Transactions on Industrial Electronics, the IEEE Transactions on Dependable and Secure Computing, the IEEE Transactions on Intelligent Transportation Systems, the IEEE TWPS, the IEEE Systems Journal, the *IEEE Communications Magazine*, the *IEEE Wireless Communications Magazine (WCMAG)*, the *IEEE Network Magazine (NETMAG)*, and conferences. His research is supported by DST, TCS, and UGC. He has guided many students leading to M.E. and Ph.D. His research interests include mobile computing, parallel/distributed computing, multiagent systems, service-oriented computing, routing and security issues in mobile *ad hoc*, and sensor and mesh networks. He is a TPC member/a technical committee member of various conferences and organized various workshops in ICC and GLOBOCOM conferences. He was a recipient of the Best Papers Award from IEEE Systems Journal, in 2018, and IEEE ICC, in 2018.

ROZAIDA GHAZALI received the B.Sc. degree (Hons.) in computer science from Universiti Sains Malaysia, in 1997, the M.Sc. degree in computer science from Universiti Teknologi Malaysia, in 2003, and the Ph.D. degree in higher order neural networks from the School of Computing and Mathematical Sciences, Liverpool John Moores University, U.K., in 2007. In 2001, she was an Academic Staff at UTHM. She is currently a Professor with the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia. She has successfully supervised a number of Ph.D. and master students and published more than 150 articles in various international journals and conference proceedings. Her research interests include deep learning algorithms, higher-order neural networks, swarm intelligence, optimization, and data mining. She has served as the conference chair and a technical committee for numerous international conferences. She acts as a reviewer for various journals and conferences.

DANISH SHEHZAD received the B.S. degree from COMSATS University, in 2010, the M.S. degree in computer sciences from Hazara University, Pakistan, in 2014, and the Ph.D. degree in computer engineering from Kadir Has University, Turkey, in 2019. He is currently working as an Assistant Professor with the Department of Computer Science, FAST National University of Computer and Emerging Sciences. He has teaching and research experience of over eight years. In the past, he worked as a researcher on the brain-inspired run-time system for a very large-scale brain simulation (BiRTS) project funded by the Scientific and Technological Research Council of Turkey. He worked as a Senior Researcher on a joint venture between Kadir Has University and Selcuk University, Turkey, for the automatic detection of various diseases through medical image processing. He is an active reviewer in various international journals and has published his research work in well-reputed international journals and conferences.

INSAF ULLAH received the master's degree in computer sciences from the Department of Information Technology, Hazara University Mansehra, Pakistan. He is currently pursuing the Ph.D. degree in computer sciences with the Department of Information Technology. He is a Lecturer with the Department of Computer Sciences, Hamdard University, Islamabad. His research interest includes network security for resource constrained devices. He is an active reviewer in various international journals and has published his research work in well-reputed international journals and conferences.