PDCM-IoD: A Lightweight PUF-Based Drone Access Control Mechanism for Internet of Drones

Shehzad Ashraf Chaudhry, *Senior Member, IEEE*, Azeem Irshad, Matloub Hussain, Bander A. Alzahrani, Ashok Kumar Das, *Senior Member, IEEE*, and Muhammad Nasir Mumtaz Bhutta

***Abstract*—The growing number of uncrewed aerial vehicles (UAVs) or drones in low altitude airspace has opened a multitude of frontiers in diverse applications such as smart city, disaster management, logistics, and surveillance operations. Nonetheless, the open and dynamic communication landscape leads the Internet of Drones (IoD) environment to many security threats, including forgery, unauthorized access, or physical drone hijacking attacks. One of the pressing challenges is to ensure perfect forward secrecy using symmetric crypto-primitives. Most of the conventional access control schemes rely on costly public key cryptosystems that might not be suitable for a constrained environment. We can spot many lightweight key agreement mechanisms for the IoD environment; however, regrettably, security loopholes render those inappropriate for deployment. In this article, we propose a lightweight access control mechanism for IoD environment leveraging a physically unclonable functions (PUF) based on barrel shifter (BS) architectures. The commutative properties of BS-oriented PUF (BS-PUF) have been exploited to ensure perfect forward secrecy in PDCM-IoD. Moreover, it ensures privacy, revocation of rogue users' identity, and resistance to known attacks, including physical drone capture threats and forgery attacks. It significantly helps to reduce computational overheads in comparison with other IoD-based schemes. The security features are rigorously analyzed using the real-or-random (RoR)-based random oracle model. Overall, the PDCM-IoD supports a 19.52% increase number of security features. The performance evaluation depicts that PDCM-IoD is highly suitable for an IoD-based resource-deficient ecosystem.**

Received 30 August 2025; revised 28 October 2025; accepted 11 November 2025. Date of publication 14 November 2025; date of current version 8 January 2026. This work was supported by the Deanship of Scientific Research (DSR) at King Abdulaziz University, Jeddah, Saudi Arabia, under Grant RG-3-611-41. The work of Shehzad Ashraf Chaudhry was supported by Abu Dhabi University's Office of Research and Sponsored Programs under Grant 19300906. *(Corresponding author: Muhammad Nasir Mumtaz Bhutta.)*

Shehzad Ashraf Chaudhry is with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates, and also with the Department of Software Engineering, Faculty of Engineering and Architecture, Nisantasi University, 34398 Istanbul, Türkiye.

Azeem Irshad is with the Faculty of Computer Science, GGC Asghar Mall Rawalpindi, Punjab Higher Education Department, Lahore 54000, Pakistan.

Matloub Hussain is with the College of Business Administration (COBA), University of Sharjah, Sharjah, United Arab Emirates.

Bander A. Alzahrani is with the Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia.

Ashok Kumar Das is with the Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500032, India, and also with the Department of Computer Science and Engineering, College of Informatics, Korea University, Seongbuk-gu, Seoul 02841, South Korea.

Muhammad Nasir Mumtaz Bhutta is with the Department of Computer Science and Information Technology, College of Engineering, Abu Dhabi University, Abu Dhabi, United Arab Emirates (e-mail: muhammad.bhutta@adu.ac.ae).

Digital Object Identifier 10.1109/JIOT.2025.3632929

***Index Terms*—Attacks, authentication, Internet of Drones (IoD), physically unclonable function, privacy protection.**

NOMENCLATURE

GCMS	Ground control and monitoring station.
U_i, D_j	ith user and jth drone.
ID_u, ID_{D_j}	Identities of U_i and D_j.
PUF_G/PUF_U PUF_D	PUF chips for GCMS, U_i, and D_j, respectively.
PW_u	Password of U_i.
CRP	Challenge-response pair.
$\mathcal{A}$	Malicious adversary.
$L_t\{\}$	List maintained by GCMS for non-revoked entities.
$\oplus$, $\|$, $h(\cdot)$	XOR, concatenation, and one-way hash function.

I. INTRODUCTION

DRONES, also termed as uncrewed aerial vehicles (UAVs), are programmed for long automated flights without aviator. Drones have limited battery, storage, and processing capabilities. The generation of economically effective microcontroller engineering has amplified the pace of drone-oriented regulation and monitoring systems [1]. A network of drones, called as Internet of Drones (IoD), collaborates in the accomplishment of a mission or the provision of coordinated services by exchanging control information. The numerous applications can be witnessed from military to civil use cases, such as modern warfare and surveillance, rescue and disaster projects, smart agriculture, smart transport monitoring, smart logistics, crowd monitoring, smart monitoring of ecologically sensitive geographical areas, and combating forest fires [2]. The IoD architecture relies inherently on the communication principles of the Internet of Things (IoT). IoT assists in remote communication and enhanced interactivity for drones in the IoD network, where direct optical transmission seems to be unfeasible. The interconnected architecture of IoD offers a multitude of online services to remote users with augmented features [3]. Drones, in the permitted air space, could be regulated by dependable administrators with the help of mobile gadgets. The IoD brings convenience for humans; however, it needs to meet the security and privacy challenges faced by drone-based practical deployments [4]. The IoD environment confronts many cybersecurity concerns due to its open

2327-4662 © 2025 IEEE. All rights reserved, including rights for text and data mining, and training of artificial intelligence and similar technologies. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

nature. There is always risk that the malevolent entity may eavesdrop the messages and attempt to delete, block, modify, or replay the same message toward other entities of the system to initiate man-in-the-middle (MiTM) attack, replay, stolen verifier attack, impersonation, ephemeral secret leakage (ESL) attack, and so on [5], [6], [7], [8]. Preventive security techniques could be adopted to mitigate the involved risks. The IoD networks with a fragile communication system, having inadequate resilience, are susceptible to numerous risks. Thus, to ensure protection of information as well as devices in the IoD system, a resilient communication setup capable of safeguarding the aforementioned threats must be deployed [9].

Drones are mostly deployed in antagonistic and hostile environments where security lapses could have catastrophic ramifications. Ensuring resilient and trustworthy communication for an IoD-based ecosystem is indispensable for the sensitive nature of operations [10]. Nonetheless, traditional authentication models adopt public key infrastructures (PKIs), rendering the IoD networks unsuitable due to heavy computational latencies and storage requirements [11]. More recently, we can witness many low-cost access control mechanisms for IoD frameworks. Those schemes, however, suffer from many physical compromise threats. Later, physically unclonable functions (PUF)-based circuits have emerged as promising hardware-oriented security primitives specifically designed to assist the device in maintaining its biometric fingerprint without storing any secret in its memory [12]. Alternatively, the PUF not only assures that the device carries its unique identity but also averts the requirement for maintaining repositories of user-based verifiers, making it an exceedingly attractive option for an IoD-based environment. The barrel shifter PUF [29], a combinational circuit capable of implementing multiple-bit shifts within a single cycle, offers distinctive benefits for its commutative computations that can be exploited in generating a mutually agreed secret key with the use of a unique challenge-response pair (CRP) in an authentication protocol. In this article, we suggest a novel drone-based access control mechanism (PDCM-IoD) with the help of barrel shifter PUF.

A. Contribution

With the increasing number of drones in the IoD-based network, ensuring efficient and secure key management has become an acute challenge. Most of the conventional access control schemes are vulnerable to privacy and physical drone threats, besides incurring added computational overheads, which could undermine network confidentiality and affect mission integrity. To address these concerns, the PDCM-IoD suggests a low-cost and hardware-assisted authentication technique leveraging exclusive features of a PUF to ensure efficient and secure drone authentication in an IoT-enabled drone-based ecosystem. The salient features of PDCM-IoD are summarized as follows.

1) A novel user-to-drone access control exchange mechanism (PDCM-IoD) is suggested for an IoD-based setting. The successful mutual authentication between the user and drone is facilitated with the assistance of a trusted online entity for negotiating a commonly agreed session key.
2) The PDCM-IoD incorporates barrel shifter PUF and lightweight symmetric primitives to enhance privacy fortification and resistance against known threats.
3) The PDCM-IoD helps to reduce computational and communication overheads for better adaptability in a constrained IoD-based ecosystem.
4) The PDCM-IoD, besides supporting privacy and perfect forward secrecy, may effectively thwart known threats, including MiTM, denial of service (DoS), impersonation, and physical drone capture threats. In addition, it can revoke any rogue user's identity from its repository maintained for the revocation list.
5) The PDCM-IoD demonstrates security using a real-or-random (RoR)-based rigorous random oracle model. Detailed security analysis and experimental evaluations suggest that the proposed scheme offers computational and communicational efficiencies as compared to previous studies.

B. Study Layout

The layout of this study is mentioned as follows. Section II presented up-to-date literature work on drone-based access control techniques. Section III illustrates preliminary facts narrating the PUF description, network model, and threat model. Section IV suggests the proposed work, comprising subsections. Section V presents an informal discussion along with and RoR-model-based formal security analysis. Section VI illustrates performance evaluation details concerning comparative studies. Finally, it presents a concluded summary.

II. Related Work

Drones require traversing through open and insecure wireless domains, rendering them exposed to several security threats, including privacy. Thus, a resilient authentication scheme might play a significant role in countering unauthorized access.

In this connection, Srinivas et al. [13] presented a low-cost key agreement scheme for an IoD system. However, it requires servers to store drone-related credentials, which makes the scheme vulnerable to forgery and drone capture threats. Alladi et al. [14] suggested a key agreement scheme for UAV–UAV and UAV-ground server. However, there might be a privacy failure due to a single ground server managing all information regarding drones. Moreover, the incorrect design of the PUF configuration also fails to convey the real information. Later, Ali et al. [15] introduced a biometric low-cost key exchange technique for drones; however, the scheme was prone to physical capture and impersonation attacks. Bansal and Sikdar [16] presented a key agreement protocol for a dynamic fleet of drones. Wu et al. [17] suggested a biometric authentication protocol that enables encryption for personal information; however, it could not resist a physical drone compromise threat. Li et al. [18] presented a bilinear pairing-based UAV authentication protocol; however, it was susceptible to a physical drone compromise threat. Yu et al. [19] demonstrated a low-cost PUF authentication model for a drone network. Nonetheless, the scheme was not immune to device capture

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

threats. Zhang et al. [20] introduced another low-cost drone authentication model with improved efficiency; however, it could not handle physical compromise and intrusions for drones that lead to information disclosure. Chandran and Vipin [21] presented a PUF-oriented low-cost access control scheme for multidrone usage employing symmetric key operations. Tian et al. [22] propounded a PUF-oriented drone access control scheme for multidomain scenarios; nonetheless, each ground station maintains its own information database, which augments the chances of privacy breach and stolen verifier threats for stakeholders. Later, Karmegam et al. [23] suggested a blockchain-based drone-assisted access control scheme with respect to multiple domains. Nonetheless, the scheme was not protected for drone-based physical capture threats. Ever [24] put forward a bilinear pairing-assisted authentication method for a mobile sink-based IoD system. Yet, the technique does not fulfill forward secrecy, and was vulnerable to physical drone capture and masquerading threats. Then, Nikooghadam et al. [25] put forward a key agreement mechanism for drone-assisted smart cities; nevertheless, the scheme was unable to resist impersonation and drone-based physical capture attacks. Then, Chaudhry et al. [26] designed a certificate-aided key agreement mechanism for an IoD environment; however, it was not protected from ESL threat as well and failed to preserve the unlinkability feature. Then, Li et al. [27] introduced an access control method for an IoT system by using elliptic curve cryptography (ECC) primitives; however, it was costly for computations due to PKI encryptions. Later, Hussain et al. [28] presented a lightweight drone access control scheme for smart city surveillance; however, it was vulnerable to impersonation attack and physical drone capture attack. Onward, Sharma et al. [29] presented a PUF-oriented access control technique for an IoD network by employing lightweight symmetric primitives. Thereafter, Park et al. [30] demonstrated a PUF-aided key agreement technique for an IoD network; nevertheless, the scheme was prone to a MiTM threat. Then, Chaudhry et al. [31] presented a low-cost key agreement method for drones; however, it does not provide anonymity to the subscribers. Then, Zhang et al. [32] introduced another lightweight PUF-oriented authentication method for the IoD system. Nevertheless, it was not protected from replay and Dos attacks. Lee et al. [33] suggested a barrel shifter (BS) PUF-based access control technique for an IoD system. The scheme was low-cost due to the utilization of symmetric primitives; however, the scheme has scalability issues and was not adaptable for drone replacements. Shui and Xie [42] presented a low-cost PUF-based key agreement scheme for an IoT-enabled ecosystem using BS-PUF. However, the scheme does not support perfect forward secrecy for the involved participants or devices. In addition, it is vulnerable to session-specific ESL threats as it does not support session key secrecy if ephemeral secrets are inadvertently exposed to the adversary. Besides PUF and other access control techniques, several evolving directions have lately been explored to reinforce IoD security. Blockchain-based authentication protocol designs by Shahidinejad and Abawajy [43], Harbi et al. [44], and Huang et al. [45] employ distributed ledgers to facilitate auditability, identity management, and tamper-resistant logging of drone-based communication exchanges. Although these techniques reduce reliance on a single centralized and trusted authority, they incur high communication and computational overheads. Also, we can witness another related direction based on AI-driven anomaly and intrusion detection, where deep learning (DL) and machine learning (ML) models are trained to determine awkward flight patterns or anomalies related to communication. The solutions presented by Bakhsh et al. [46] and Saba et al. [47] facilitate threat prediction in addition to dynamic authentication, yet suffer from many privacy concerns and resource constraints. More recently, de Jesus Sousa and Gondim [34] designed a new multifactor authentication-based technique for the IoD system; however, the scheme was not resilient against a Dos threat.

Several access control protocols have been designed for IoD to ensure secure interaction, yet most suffer from problems like privacy concerns, replay, impersonation, and physical capture threats. While recent low-cost and PUF-enabled techniques reduced cost with enhanced efficiency, they still lack forward secrecy and resilience to ESL threats. A review as some of the existing works is also given in Table I. Thus, a more resilient and privacy-preserving access control framework is required for the IoD ecosystem.

III. Preliminaries

This section narrates preliminary details of PUF, network model, and adversary model as given in the following.

A. Physical Unclonable Function

The PUF can help in the unique identification of any service, device, or chip, just like a biometric fingerprint [8]. This chip is embodied in a device and is practically unmanageable to clone through the fabrication process. It obviates the need to store the secrets in its memory, unlike a smart card, which provides it resilience during physical compromise of the device. It is immensely sensitive to environmental variations and would malfunction if any attempt at physical tampering is made. The malevolent controls and impositions on the part of the adversary may bring about perceptible perturbations, making the chip useless for future use. The PUF function $\mathrm{PUF}_{fn} : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$, where l_1 and l_2 show the length of characters used either as input or output into the device.

B. BS Physical Unclonable Function

Guo et al. [35] presented an encryption hardware underpinning invertible and commutative behavior as shown in the following.

1) Invertibility: Assume an input θ and secret key σ, then $\mathrm{PUF}_f(\sigma, \theta) = \omega \rightarrow \mathrm{PUF}_f^{-1}(\sigma, \omega) = \theta$, where PUF_f^{-1} exhibits a PUF-aided invertible function.

2) Commutativity: Assume two BS-PUF chips, i.e., PUF_u and PUF_v, with input θ, $\mathrm{PUF}_u\ [\mathrm{PUF}_v\ (\theta)] = \mathrm{PUF}_v\ [\mathrm{PUF}_u\ (\theta)]$ always holds true.

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

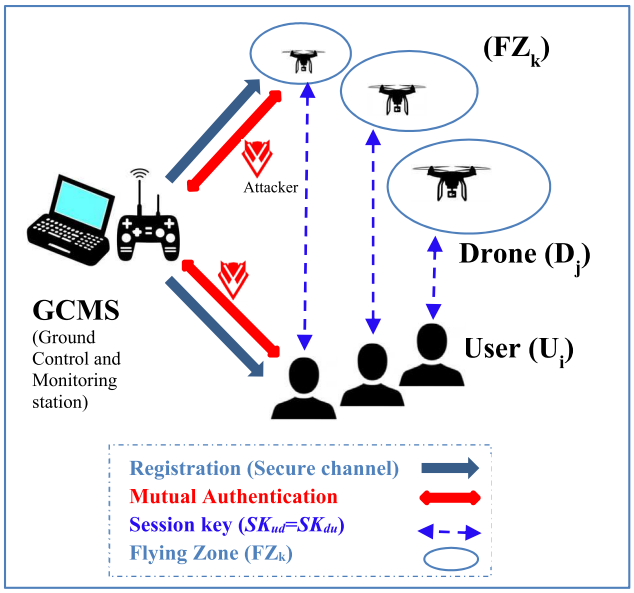

Fig. 1. Network architecture.

C. Security Requirements

The proposed scheme must consider the following security requirements to ensure efficiency and resilience of the scheme against known threats.

1) Anonymity and Unlinkability: The participating entities should remain anonymous and unlinkable with the use of nonidentifiable dynamic pseudonyms.

2) Resilient to Physical Capture and Tampering: The secrets must be stored safely in the memory of IoT-enabled drones to thwart any possible attack by the adversary.

3) DoS Attack: The protocol must employ low-cost prechecks so that repeated malicious attempts can be continuously defeated.

4) Desynchronization Attack: The participating entities should not become desynchronized at any level with the intrusion of adversaries.

5) Perfect Forward Secrecy: Session keys should remain safe even if the long-term secrets are exposed to the adversary.

6) MiTM Threat: The adversary needs to be debarred from initiating any replay, modification, or MiTM-based intrusions.

7) Malfunctioning Drone Replacement: The protocol picks the identity of the operational drone inducted in the field, and gets it verified through the central server, and is not bound with a single drone identity initially assigned.

D. Network Model

The network model for PDCM-IoD consists of three participating members: 1) user (U_i), 2) GCMS, and 3) drone (D_j), as depicted in Fig. 1. In this architecture, the GCMS enrolls all users U_i and drones D_j specified for various flying zones FZ_k. In the login and authentication procedure, U_i initiates an authentication query request toward GCMS for a specific FZ_k. GCMS assigns a certain D_j for any specific FZ_k and submits a request to that D_j for verifying U_i. Ultimately, a session key SK is mutually converged among U_i, D_j, and GCMS. These participating members are detailed as follows.

1) *User (U_i)* : U_i gets itself registered through GCMS on a confidential channel and is issued with secret credentials, which may be later employed to get authenticated through GCMS in the login and authentication phase. The user is deployed with BS-PUF, gaining a commutative advantage during session key generation in PDCM-IoD.
2) GCMS: The GCMS, being a controlling authority, is responsible for registering users and drones, besides authenticating the same entities in the IoD network. The GCMS allocates a drone for a single FZ_k at a time. The GCMS also engages the BS-PUF circuit to validate U_i and D_j entities and facilitate the construction of mutually agreed session keys.
3) *Drone (D_j)*: The D_j is registered through GCMS along with the issuance of secret parameters. A single drone is assumed to be deployed in any specific FZ_k for the provision of designated services. In addition, it is also implanted with BS-PUF circuits for ensuring protection from physical compromise and counterfeit procedures initiated by an adversary. The mutually built SK between U_i and D_j can help in the provision of related services.

E. Threat Model

A threat model in cryptography is critical since it assists the developers in anticipating and mitigating potential threats. By considering a worst case scenario, in which the adversary $\mathcal{A}$ could have massive capabilities, the resilience of any cryptographic protocol can be thoroughly assessed and reinforced [36]. The PDCM-IoD considers two threat models with varying capabilities, i.e., Dolev–Yao (DY) model [37] and Canetti–Krawczyk (CK) model [38]. These models undertake malicious capabilities of adversaries, serving as a benchmark to strengthen the designed schemes. The DY model is a widely accepted model utilized for designing security applications. It undertakes that $\mathcal{A}$ could intercept, delete, replay, and block the message by controlling the open channel. Then, the adversary may initiate MiTM attacks. The CK model, being an extension of the DY-threat model, assumes added capabilities of the adversary, comprising the compromise of temporary session-based random nonces.

IV. Proposed Scheme

This study suggests a novel user-to-drone access control exchange mechanism (PDCM-IoD) for an IoD-based environment. The successful mutual authentication between the user and the drone is mediated with the help of a trusted online entity, GCMS, for negotiating a commonly agreed session key. The details of the PDCM-IoD are stated as follows.

A. System Initialization

In this phase, the GCMS, a trusted entity, assumes the BS-PUF circuit PUF_G not only for registering all entities but also helps them attain mutual authentication in the login and authentication phase. In addition, GCMS maintains a CRP repository along with a revocation list of malicious user identities.

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

Fig. 2. Registration of drone (D_j).

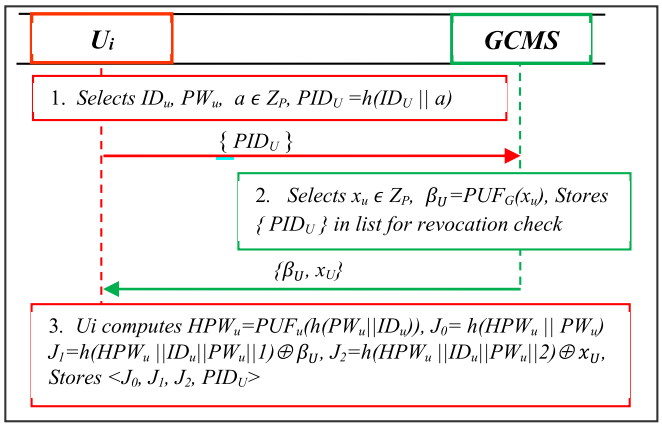

Fig. 3. Registration of user (U_i).

The $\mathcal{CRP}$ repository is characterized by a function, $\mathcal{CRP}$: $I \rightarrow \mathcal{C} \times R$, where the drone identity is mapped to a unique CRP pair.

B. Drone Registration Phase

The drone is registered employing the following steps.

1) Initially, the drone D_j selects its identity ID_{D_j}, generates $x_d \epsilon Z_P$, and computes $\beta_d = \mathrm{PUF}_d(x_d)$. Then, it submits the registration request $\{\mathrm{ID}_{D_j}, x_d, \beta_d\}$ to GCMS as shown in Fig. 2.
2) The GCMS stores CRP parameters in its $\mathcal{CRP}$ repository.

C. User Registration Phase

The user is enrolled through GCMS by adopting the following procedure.

1) Primarily, U_i selects its identity ID_u and password PW_u.Then, it generates a random nonce $a \epsilon Z_P$ and calculates $\mathrm{PID}_U = h(\mathrm{ID}_U||a)$ and sends the message $\{\mathrm{PID}_U\}$ to GCMS.
2) The GCMS, after receiving a request, generates $x_u \epsilon Z_P$ and computes $\beta_U = \mathrm{PUF}_G(x_u)$. Then, it stores $\{\mathrm{PID}_U\}$ in its list for revocation check, and sends the message $\{\beta_U, x_U\}$ to U_i.
3) Next, U_i computes $\mathrm{HPW}_u = \mathrm{PUF}_u[h(PW_u|| \mathrm{ID}_u)]$, $J_0 = h(\mathrm{HPW}_u|| \mathrm{PW}_u)$, $J_1 = h(\mathrm{HPW}_u|| \mathrm{ID}_u|| \mathrm{PW}_u||1) \oplus \beta_U$, $J_2 = h(\mathrm{HPW}_u|| \mathrm{ID}_u|| \mathrm{PW}_u|| 2) \oplus x_U$, and stores $< J_0, J_1, J_2, \mathrm{PID}_U >$, as shown in Fig. 3.

D. Mutual Authentication Phase

The login and authentication procedure of this scheme comprises the subsequent steps.

1) Initially, U_i inputs its identity ID_u, password PW_u, and computes $\mathrm{HPW}_u = \mathrm{PUF}_u\ [h(\mathrm{PW}_u||\mathrm{ID}_u)]$, $J'_0 = h(\mathrm{HPW}_u|| \mathrm{PW}_u)$, and verifies $J'_0? = J_0$.If it is not true, the login request is aborted. Otherwise, it further computes $\beta_U = h(\mathrm{HPW}_u|| \mathrm{ID}_u|| PW_u||1) \oplus J_1$, $x_U = h(\mathrm{HPW}_u||\mathrm{ID}_u|| \mathrm{PW}_u||2) \oplus J_2$, $\alpha_u = \mathrm{PUF}_u(x_U), \beta'_U = \mathrm{PUF}_u(\beta_U)$, $A_1 = h(\alpha_u||\beta'_U||T_1)$, $A_2 = h(\beta'_U||T_1||1) \oplus \mathrm{ID}_{D_j}$,and $A_3 = h(\beta'_U||T_1||2) \oplus (x_U||\mathrm{PID}_U)$. Then, it senses the flying zone FZloc_i and chooses the sensed D_j identity ID_{D_j}. Then, it submits the message $M_1 = \{A_1, A_2, A_3, \alpha_u, T_1\}$ to GCMS.
2) The GCMS verifies $T_1 - T_c < \Delta T$, and computes $\alpha'_u = \mathrm{PUF}_G(\alpha_u)$, $A'_1 = h(\alpha_u||\alpha'_u||T_1)$, and $(x_U||\mathrm{PID}_U) = h\left(\beta'_U \mathbf{t} ||T_1|| 2\right)) \oplus A_3$. Then, it checks its revocation list. If PID_U exists in the database, then it verifies $A_1? = A'_1$. If it does not hold true, the GCMS aborts. On the other hand, computes $\mathrm{ID}_{D_j} = h(\alpha'_u||T_1||1) \oplus A_2$. Then, it recovers the CRP (x_d, β_d) for a particular drone-oriented PUF_{D_j} from $\mathcal{CRP}$ repository using ID_{D_j}, i.e., $(x_d, \beta_d) = \mathcal{CRP}(\mathrm{ID}_{D_j})$. Then, it computes $\alpha_d = \mathrm{PUF}_G(x_d), \beta'_d = \mathrm{PUF}_G(\beta_d)$, $B_1 = h(\alpha_u||\alpha_d||\beta'_d||T_2||1) \oplus x_U$, and $B_2 = h(\alpha_u||\alpha_d||x_U||\beta'_d||T_2)$. Then, it sends message $M_2 = \{B_1, B_2, \alpha_d, \alpha_u, T_2\}$ to D_j for verification.
3) D_j, after verifying $T_2 - \mathrm{Tc} < \Delta T$ for message M_2, computes $\alpha'_d = \mathrm{PUF}_d(\alpha_d), x_U = h(\alpha_u||\alpha'_d||\alpha_d||T_2||\ 1) \oplus B_1$, $B'_2 = h(\alpha_u||\alpha_d||x_U||\alpha_d||T_2)$, and verify $B_2\ ? = B_2$. If it is true, it further calculates $\gamma = \mathrm{PUF}_D(x_U)$ and $sk_{du} = \mathrm{PUF}_D(\alpha_u)$. Then, it generates $x_d^{\mathrm{new}} \epsilon Z_P$ and computes $\beta_d^{\mathrm{new}} = \mathrm{PUF}_d(x_d^{\mathrm{new}})$, $C_1 = h(sk_{du}||\alpha_u)$, $C_2 = h(\alpha'_d||T_2||1) \oplus \beta_d^{\mathrm{new}}$, $C_3 = h(\alpha'_d||T_2||2) \oplus \mathrm{x}_d^{\mathrm{new}}$, $C_4 = h(\alpha'_d||T_2||3) \oplus \gamma$, and $C_5 = h(\beta_d^{\mathrm{new}}||x_d^{\mathrm{new}}||\gamma||\alpha'_d)$. Next, it submits $M_3 = \{C_1, C_2, C_3, C_4, C_5\}$ to GCMS as shown in Fig. 4.
4) The GCMS, after receiving M_3, computes $\beta_d^{\mathrm{new}} = h(\beta'_d||T_2||1) \oplus C_2$, $x_d^{\mathrm{new}} = h(\beta'_d||T_2||2) \oplus C_3, \gamma = h(\beta'_d||T_2||3) \oplus C_4$, $C'_5 = h(\beta_d^{\mathrm{new}}||x_d^{\mathrm{new}}||\gamma||\beta'_d)$, and verifies $C_5? = C_5$. If it is true, a random integer is defined as $x_u^{\mathrm{new}} \epsilon Z_P$. Then, it computes $\beta_U^{\mathrm{new}} = \mathrm{PUF}_G(x_u^{\mathrm{new}})$, $B_3 = h(\alpha'_u||T_1||1) \oplus \beta_u^{\mathrm{new}}$, $B_4 = h(\alpha'_u||T_1||2) \oplus x_u^{\mathrm{new}}$, $B_5 = h(\alpha'_u||T_1||3) \oplus \gamma$, $B_6 = h(\beta_u^{\mathrm{new}}||x_u^{\mathrm{new}}||\alpha'_u||\gamma||T_1)$, and sends message $M_4 = \{C_1, B_3, B_4, B_5, B_6\}$ to U_i. It also updates the message parameters β_d^{new} and x_d^{new} to ensure unlinkability of messages across various sessions of the same entities.
5) U_i, upon the receipt of M_4, computes $\beta_u^{\mathrm{new}} = h(\beta'_u||T_1||1) \oplus B_3$, $x_u^{\mathrm{new}} = h(\beta'_u||T_1||2) \oplus B_4, \gamma = h(\beta'_u||T_1||3) \oplus B_5$, $B_6 = h(\beta_u^{\mathrm{new}}||x_u^{\mathrm{new}}||\beta'_u||\gamma||T_1)$, and verifies $B_6\ ? = B_6$. If it holds valid, further computes $sk_{ud} = \mathrm{PUF}_u(\gamma)$ and $C_1 = h(sk_{ud}||\alpha_u)$, and again verifies $C_1\ ? = C_1$. If it is true, it updates the parameters β_u^{new} and x_u^{new} in its memory to avoid the unlinkability feature.

V. Security Analysis

This section illustrates informal and formal security analysis as demonstrated below:

A. Informal Security Analysis

1) Mutual Authentication: In PDCM-IoD, GCMS verifies $A_1\ ? = A_1'$ on the basis of transmitted communication messages from U_i. If it is valid, GCMS authenticates U_i. Since it knows

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

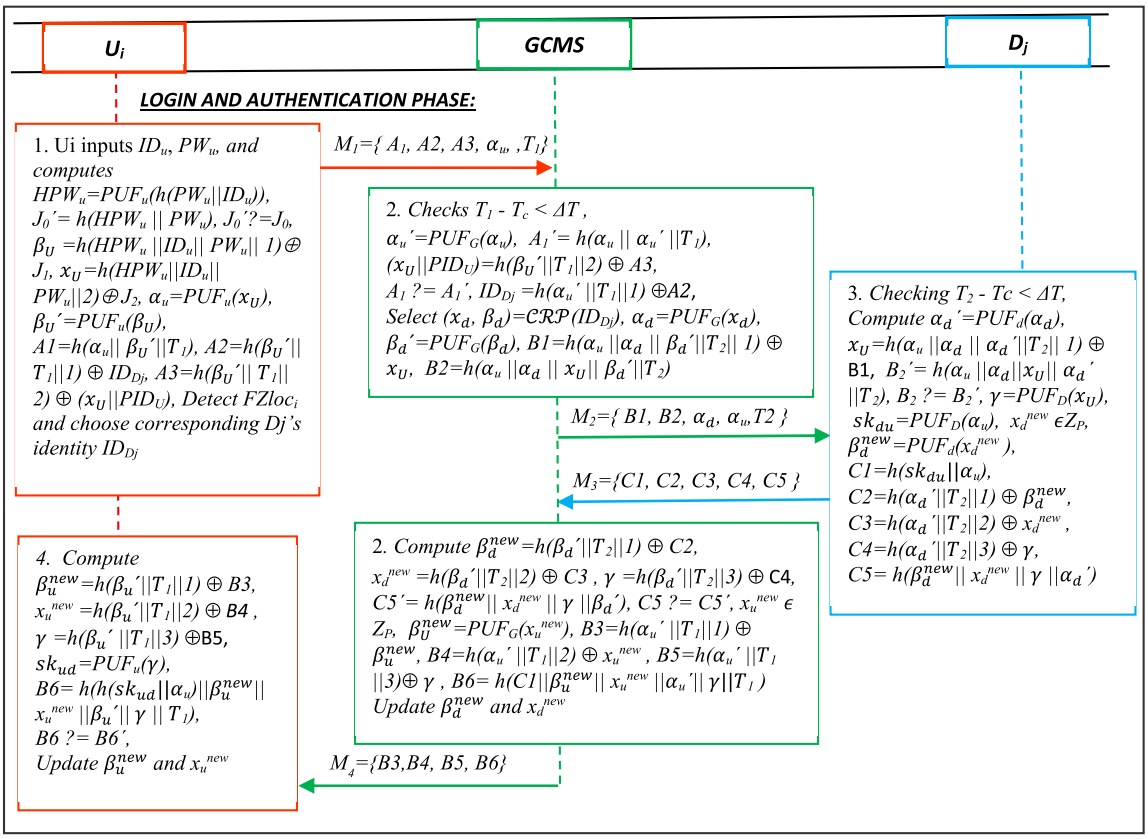

Fig. 4. Proposed scheme (PDCM-IoD).

that $\alpha_u' \approx \beta_U'$ and a valid A_1 cannot be produced by any outsider other than a valid entity registered with GCMS. Likewise, GCMS authenticates D_j on the basis of verification for $C_5 ? = C_5'$, in which β_d' is the parameter that GCMS knows C_5 cannot be produced without the help of a legally registered D_j. U_i authenticates GCMS by checking $B_6 ? = B_6'$ since the parameter β_u' can only be produced by a valid GCMS, which warrants the fact that the involved GCMS and D_j are legitimate entities. Likewise, D_j authenticates GCMS by checking the validity of $B_2 ? = B_2'$, which endorses the fact that the shared parameter $\alpha_d' \approx \beta_d'$ used in the construction of B_2 can only be produced by a valid GCMS entity. Thus, all entities support mutual authentication in PDCM-IoD.

2) Anonymity and Unlinkability: The PDCM-IoD is anonymous as well as unlinkable on the part of a malicious adversary since the user entity is not submitting its original identity in the open communication messages. The scheme employs CRP-based commutative outcomes from both PUF circuits of involved participating entities to ensure mutual authenticity between the two participants. A unilateral PUF-based outcome $\text{PUF}_a(\partial)$ for any integer ∂ is submitted as a challenge by the challenger entity to the verifying entity, which may be treated as a pseudo-identity of the challenger entity. The verifying entity takes the respective PUF-based outcome PUF_b $[\text{PUF}_a(\partial)]$ for the received parameter $\text{PUF}_a(\partial)$, which acts as the commutative outcome, and is verified as the shared parameter between both entities. If it matched, the verifying entity authenticates the challenging entity. Moreover, our scheme does not carry any identical parameter that remains the same and distinguishable across various sessions of the same participating entities, which ensures unlinkability for the proposed scheme.

3) Replay Attack: The PDCM-IoD makes use of fresh timestamps, T1 and T2, in the first two messages, M1 and M2, which enables the protocol to attain resilience against any replay threat that may be launched by the attacker. Thus, PDCM-IoD can detect any forged message fabricated by the adversary.

4) Impersonation Attack: If $\mathcal{A}$ attempts to masquerade as any valid participant with the submission of forged messages toward another legal entity, the latter may detect and foil that attempt by performing the crucial checks and verifications. As mentioned in the mutual authentication phase, the verifications, $A_1 ? = A_1'$, $B_2 ? = B_2'$, $C_5 ? = C_5'$, and $B_6 ? = B_6'$, are performed by GCMS, D_j, GCMS, and U_i, respectively. The shared parameters such as $\alpha_u' \approx \beta_U'$ as well as $\alpha_d \approx \beta_d$ among U_i, GCMS, and D_j form the basis of mutually agreed session key, i.e., $sk_{ud} = sk_{du}$ that refrains the adversary from intruding into the communication exchange among legal participants.

5) Drone Physical Capture Attack: The PDCM-IoD is resilient against drone-based physical capture threats. Even if the attacker approaches the drone equipment, the former will not be able to access the key α_d' shared between D_j and GCMS, for which $\mathcal{A}$ must access the PUF circuit of either of the two entities. However, it is a proven fact that the PUF remains physically unclonable or inaccessible due to its inherent design

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

of fabrication, even if the drone is stolen by the attacker. Also, without approaching the PUF, $\mathcal{A}$ could never recover the shared key, which can only be produced in a commutative manner.

6) Session-Specific Ephemeral Secrets Leakage Attack: The resistance to the ESL threat specifies resilience of the session key in case temporary keys are revealed to the adversary. According to the assumed eCK adversary model, even if the adversary gets access to short-term ephemeral secrets such as x_u, $\mathcal{A}$ may not be able to compute the respective session key $sk_{ud} = sk_{du}$, without getting access to the device's embedded PUF circuits. Thus, PDCM-IoD remains impervious to session-specific ESL threats, as the adversary is unable to compute the session key from the inadvertently revealed short-term secrets.

7) Perfect Forward Secrecy: The perfect forward secrecy maintains that if the long-term private key of any participating legal entity is revealed to the adversary, the previous session keys remain protected. In PDCM-IoD, GCMS employs only the PUF_G circuit and $\mathcal{CRP}$ repository to register and facilitate the mutual authentication process between U_i and the corresponding drones D_j. It is a known fact that the PUF circuits held by these entities, acting as the biometric key for GSR, cannot be replicated or cloned by an adversary in case the entity is compromised by the adversary. While the constructed session key for PDCM-IoD cannot be produced without engaging the respective PUF_G, it can be concluded that perfect forward secrecy is ensured in PDCM-IoD.

8) Stolen CRP Attack: The PDCM-IoD ensures resistance to the stolen verifier threat even if the $\mathcal{CRP}$ repository is stolen by any internal attacker. As discussed before, the session key cannot be developed without engaging the respective PUF_G held by various entities in the system. We can infer that our scheme supports resilience against the stolen CRP threat.

B. Formal Security Analysis

The PDCM-IoD is formally evaluated using a random oracle model based on the RoR model [38]. The adversary $\mathcal{A}$ is permitted to initiate several queries, including test, execute, reveal, send, and hash queries. $\mathcal{A}$ could use the test query to guess the concealed bit c. For this purpose, it makes use of an unbiased coin $c \in \{0, 1\}$ for determining the outcome, which may return the original key, or otherwise, it returns a random string. In case the bit is guessed correctly, the adversary wins this game [39], which substantiates the fact that $\mathcal{A}$ correctly distinguishes the legitimate session key from a random string.

The $\text{Adv}_{\mathcal{A}}^{\text{PDCM-IoD}}$ characterizes the benefit of the adversary in winning the game for PDCM-IoD. The PDCM-IoD remains resilient as long as $\text{Adv}_{\mathcal{A}}^{\text{PDCM-IoD}}$ is negligible.

Commutative Property of PUF:

Presumably, $\text{PUF}_{\bowtie}(\cdot)$ and $\text{PUF}_{\bowtie}(\cdot)$ exhibit commutative behavior since it yields a uniform outcome when used in a commutative combination in either way. Given $\text{PUF}_{\bowtie}(x)$ and $\text{PUF}_{\bowtie}(x)$, it is not feasible to compute $\text{PUF}_{\bowtie}(\text{PUF}_{\bowtie}(x))$ or $\text{PUF}_{\bowtie}(\text{PUF}_{\bowtie}(x))$ without retrieving $\text{PUF}_{\bowtie}(\cdot)$ and $\text{PUF}_{\bowtie}(\cdot)$, where x is a positive integer. The attacker's benefit in compromising the commutative behavior of the BS-PUF could be represented as $\text{Adv}_{\mathcal{A},\text{CP}}^{\text{PDCM-IoD}}$, which is negligible.

TABLE I
TABULAR DESCRIPTION OF SUMMARIZED RELATED WORK

Protocol	*Features*	*Operations*	*Drawbacks*	*Year*
Chaudhry *et al.* [26]	GCACS-IoD: A certificate-based authentication method for IoD	ECC	Emphemeral secret leakage and spoofing threat	2021
Li *et al.* [27]	Anonymous efficient access control for IoD	Hash	Stolen device factors threat	2022
Hussain *et al.* [28]	Lightweight drone access scheme for smart city surveilance.	Hash	Physical drone capture and impersonation attack	2022
Sharma *et al.* [29]	PSECAS: PUF-enabled key management for IoD	Hash, PUF	Stolen device parameters and impersonation threat	2023
Park *et al.* [30]	PUF-aided key management protocol for IoD	Hash, FE	Man-In-The-Middle attack	2023
Chaudhry *et al.* [31]	A lightweight access control scheme for IoD.	Hash, PUF	Man-In-The-Middle attack, session key insecurity	2023
Zhang *et al.* [32]	A PUF-aided key agreement technique for IoD.	Hash, PUF	Replay and Denial of Service (DoS) threats	2024
Lee *et al.* [33]	PUF-aided privacy preserving key management protocol for IoD	Hash, PUF	Inability to support dynamic replacement of malfunctioning drones	2024
Shui *et al.* [42]	A lightweight PUF based authentication scheme for IoT devices	Hash, PUF	Ephemeral secrets leakage threat, No perfect forward secrecy, Lacking session key security	2024
Sousa and Gondim [34]	Multi-server authenticated key agreement scheme for IoD	ECC, FE	Susceptible to DoS threat	2025

Communication Model:

The participating members in PDCM-IoD, i.e., U_i and D_j, come into mutual authentication and generate a session key SK with the help of GCMS. These members engage in multiple distinct instances of the joint execution for protocol P, termed as oracles. The $\prod_{\bowtie}^{U_i}$ acting as U_i instance assumes there lies a PUF-based commutative secret $\alpha'_u \approx \beta'_U$ shared with GCMS, while the D_j instance assumes another commutative secret $\alpha'_d \approx \beta'_d$ as shared with GCMS. To model the actual threat, this communication framework makes use of various queries such as Hash(·), Send(·), Reveal(·), Test(·), and Execute(·), as shown in Table II.

Security Proofs:

Theorem 1 exhibits that PDCM-IoD establishes a resilient session key given the assumption based on the commutative property of BS-PUF and a cryptographically secure hash operation.

Theorem 1: Assuming $\text{Adv}_{\mathcal{A},\text{CP}}^{\text{PDCM-IoD}}$ as the probabilistic polynomial time adversary $\mathcal{A}$ advantage in compromising the assumption based on the commutative property of BS-PUF. The probability of the adversary compromising the session key SK of PDCM-IoD. The benefit of the adversary for winning the game can be bounded by the following equation:

$$\text{Adv}_{\mathcal{A}}^{\text{PDCM-IoD}}(\delta_e, \delta_t, \delta_s, \delta_h) \leq \frac{(\delta_h)^2}{2^{l-1}} + 2.\text{Adv}_{\mathcal{A},\text{CP}}^{\text{PDCM-IoD}}(\delta_e, \delta_s) \tag{1}$$

where δ_s, δ_t, δ_e, and δ_h indicate the number of queries for *send*, *test*, *execute*, and *hash* oracles, respectively. Here, l is the bit-length of security parameters such as identity, hash, or random string. Alternatively, l determines the resistance of the

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

TABLE II
QUERIES WITH SEMANTICS

Queries	Semantics
Execute (U_i^{α}, D_j^{β} and $GCMS^{\gamma}$)	$\mathcal{A}$ makes use of this query to overhear publicly available messages exchanged among U_i, D_j and *GCMS*.
Reveal (U_i^{α}, D_j^{β})	$\mathcal{A}$ makes use of this *Reveal* query for divulging *SK* as generated mutually by U_i and D_j.
Send (U_i^{α}, $\mathrm{M_{sg}}$)	This query embodies an active attack by $\mathcal{A}$ towards U_i.
Corrupt (U_i^{α})	$\mathcal{A}$ makes use of this query to reveal the secrets as stored in memory of D_j.
Hash (M)	The attacker makes use of *Hash* query to list all collisions in H_t.
Test (U_i^{α})	The Test query is utilized for verifying the integrity of estimated *SK*. For this purpose, $\mathcal{A}$ makes use of an unbiased coin c to check the findings of experiment in the following way: • c=0: the estimated SK generated between U_i^{α} and D_j^{β} isn't fresh, which terms it a random string of similar length. • c=1: the estimated SK is fresh and legitimate. • c=⊥: the estimated SK cannot be constructed, or the oracle query is not effective.

PDCM-IoD in the guessing of threats, collisions, or statistical distinguishing.

Proof: We utilize a sequence of games G_n ($0 \leq n \leq 3$) and analyze the probability of the adversary's success, i.e., $\mathrm{Wins}_{\mathcal{A}}^{G_n}$ for various events E_n ($0 \leq n \leq 3$).

Game G_0: This game represents the execution of the real protocol under threat against $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{PDCM-IoD}}$ involving the participating members U_i and D_j. By the definition of semantic security, we have

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{PDCM-IoD}}(t) = \left|2.Pr\left[\mathrm{Wins}_{\mathcal{A}}^{G_{n0}}\right] - 1\right|. \tag{2}$$

Game G_1: This game entertains added send and test oracle queries in game G_0 regarding the flows containing $\mathrm{PUF}_{\bowtie}(\varphi)$ and $\mathrm{PUF}_{\bowtie}(\varphi)$, and responding to the queries in PDCM-IoD, respectively. Presumably, (A, B, C) = ($\mathrm{PUF}_{\bowtie}(\varphi), \mathrm{PUF}_{\bowtie}(\varphi), \mathrm{PUF}_{\bowtie}(\mathrm{PUF}_{\bowtie}(\varphi))$ indicates a commutative-PUF triplet. The simulator S models the oracle queries for all sessions by using the same (A, B, C) triplet, and classical random self-reducibility as per the assumption related to commutative-PUF [29]. The simulator S models the oracle queries related to all sessions by using (A, B, C) along with the classical random self-reducibility property based on commutative-PUF. First, S initializes parameter setup and then responds to the oracle's queries for PDCM-IoD. Afterward, test oracles could be responded to in a better way. By employing the bridge step, we can say G_0 is equivalent to G1, i.e.,

$$Pr\left[\mathrm{Wins}_{\mathcal{A}}^{G_1}\right] = Pr\left[\mathrm{Wins}_{\mathcal{A}}^{G_0}\right]. \tag{3}$$

Game G_2: At the end of game G2, the challenger C could gain a negligible benefit by compromising the security of the session for PDCM-IoD. This game models all of the abovementioned oracles in G1, with the exception that all rules are computed with the use of a random triplet (A, B, C) in place of a commutative-PUF triplet. An assumed challenger $\mathcal{A}_C$ could attempt to break the commutative-PUF assumption. Likewise, $\mathcal{A}_B$ could attempt to compromise the resilience of PDCM-IoD to recover SK. For this purpose, $\mathcal{A}_C$ could use various oracle queries, such as corrupt, execute, test, and send queries that may either return a real session key or a random string based on the flipping of an unbiased coin c. The outcome of $\mathcal{A}_C$ is largely the same as the outcome of G1, with the exception of (A, B, C) as input. In the case, $\mathcal{A}_B$ is able to distinguish the factual SK from the random string, it generates an outcome with the guessed bit c, and wins the game only if $c = c$ holds

$$\Pr\left[\mathrm{Wins}_{\mathcal{A}}^{G_2}\right] - Pr\left[\mathrm{Wins}_{\mathcal{A}}^{G_1}\right] \leq \mathrm{Adv}_{\mathcal{A},\,\mathrm{CP}}^{\mathrm{PDCM-IoD}}(\mathcal{A}_C). \tag{4}$$

Game G_3: The game G_3 employs similar oracles as used in game G_2, except for the use of table list H_t for modeling hash oracle queries. That is to say, these are alike games with the exception that it also checks possible collisions by consulting the table H_t. Hence, by employing the birthday paradox [40], we have

$$Pr\left[\mathrm{Wins}_{\mathcal{A}}^{G_3}\right] = Pr\left[\mathrm{Wins}_{\mathcal{A}}^{G_2}\right] \leq \frac{(\delta_h)^2}{2^l}. \tag{5}$$

With the modeling of the oracle queries, $\mathcal{A}_c$ must guess the factor c by engaging the *test* query to win G3. Hence, $Pr[\mathrm{Wins}_{\mathcal{A}}^{3}]$ shows the adversary's benefit in the estimation of c with the help of the following equation:

$$Pr\left[\mathrm{Wins}_{\mathcal{A}}^{G_3}\right] = \frac{1}{2}. \tag{6}$$

By employing the difference Lemma [39], we infer

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{PDCM-IoD}}(\mathcal{A}_B) \leq \frac{(\delta_h)^2}{2^{l-1}} + 2.\mathrm{Adv}_{\mathcal{A},\mathrm{CP}}^{\mathrm{PDCM-IoD}}(\mathcal{A}_C).$$

■

VI. PERFORMANCE EVALUATION

In this section, we evaluate the contributed scheme against a few state-of-the-art drone-based authentication protocols, with a focus on computational, communicational, and security functionalities. The comparative analysis is evaluated on the basis of findings from techniques [25], [27], [28], [29], [30], [31], [32], [33], [34].

The comparison of security functionalities for schemes [25], [27], [28], [29], [30], [31], [32], [33], [34] is exhibited in Table III. According to this table, we can see that [25] is vulnerable to impersonation attack, drone capture threat, stolen verifier, and desynchronization attack. The scheme [27] is not protected from a stolen device attack. The scheme [28] is prone to impersonation and drone capture attacks. The scheme [29] is prone to impersonation and stolen device attacks. The scheme [30] does not provide protection from a MiTM attack. Scheme [31] does not comply with anonymity and unlinkability features. The scheme [32] is prone to replay and denial-of-service (DoS) attacks, and does not support session key secrecy. The scheme [33] does not support replacement for malfunctioning drones since drones are wireless, movable

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

TABLE III
THREAT RESISTANCE ATTRIBUTES AND COMPARISON

	[25]	[27]	[28]	[29]	[30]	[31]	[32]	[33]	[34]	PDCM - IoD
TRA1	□	□	□	□	□	■	□	□	□	□
TRA2	□	□	□	□	□	□	□	□	■	□
TRA3	■	□	■	■	□	□	□	□	□	□
TRA4	■	□	■	□	□	□	□	□	□	□
TRA5	□	□	□	□	■	□	□	□	□	□
TRA6	□	□	□	□	□	□	□	□	□	□
TRA7	□	□	□	□	□	□	■	□	□	□
TRA8	□	□	□	□	□	□	■	□	□	□
TRA9	■	■	□	■	□	□	□	□	□	□
TRA10	□	□	□	□	□	□	■	□	■	□
TRA11	□	□	□	□	□	□	□	■	□	□
TRA12	■	□	□	□	□	□	□	□	□	□

TRA1: Unlinkability and anonymity, TRA2: Mutual authentication support, TRA3: Safe against impersonation threat, TRA4: Safe against drone capture threat, TRA5: Safe against Man-In-The-Middle attack, TRA6: Sustains perfect forward secrecy, TRA7: Sustains session key agreement, TRA8: Safe against replay attack, TRA9: Safe against stolen device attack, TRA10: Safe against Denial of Service attack, TRA11: Sustains malfunctioning drone replacement , TRA12: Safe against De − synchronization attack, □: Security Trait supported, ■: Security Trait not supported

TABLE IV
EXPERIMENTAL EVALUATION OF COSTS

Operations	U_i	*GCMS*	D_j
T_h	0.017	0.008	0.013
T_a	0.024	0.007	0.016
T_{PUF}	0.078	0.005	0.014
T_S	0.035	0.013	0.017
T_{PM}	6.227	0.991	4.809
T_{fe}	0.099	-	0.088

entities, and tend to change their respective locations. The scheme [34] is vulnerable to a DoS-based threat. Moreover, it does not warrant mutual authentication.

To evaluate the computational performance of user, server, and drones in an IoD-based setting, let T_h be the timing latency for hash operation, let T_a be the timing latency for point addition operation, let T_{PUF} be the timing for PUF operation, let T_{PM} be the timing latency for ECC point multiplication operation, let T_S be the timing latency for symmetric key operation, and let T_{fe} be the timing latency for fuzzy extractor operation. These computational metrics determine the overall performance of the PDCM-IoD since these are the crypto-primitives that are nonnegligible for consuming more processing time as compared to other negligible operations, such as exclusive-OR (XOR). As a test bench, we employed Core[1] i5-6300HQ processor @ 2.40 GHz, 16-GB RAM, Windows 10 64-bit for simulating GCMS to get execution time as depicted in Table III. Likewise, for modeling the user and drone, we used a Raspberry Pi 4B, 64-bit ARM Cortex-A72 CPU with 1.5 GHz and 2 GB of LPDDR4 SDRA, to get to the execution time as shown in Table IV. The computational overhead of schemes [25], [27], [28], [29], [30], [31], [32], [33], [34] is shown in Table V, which shows that the protocols [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30] and proposed scheme take computational cost as $19T_h + 4T_{PM}$, $27T_h, T_{fe} + 2T_S + 31T_h$, $2T_{PUF} + 24T_h$, $2T_{fe} + 32T_h$, $30T_h$, $2T_{PUF} + 20T_h$, $12T_{PUF} + 22T_h, T_{fe} + 3T_{PM} + 4T_a + 12T_h$, and $12T_{PUF} + 31T_h$. The computational latencies of [25], [27], [28], [29], [30], [31], [32], [33], and [34] and the proposed scheme amount to 21.47, 0.365, 0.566, 0.42, 0.592, 0.401, 0.406, 0.654, 16.24, and 0.723 ms.

To evaluate the efficiency of communication, the size of each message and the total number of exchanged messages are considered. For examining the communication overhead of [25], [27], [28], [29], [30], [31], [32], [33], and [34] and PDCM-IoD, we assume that bit sizes of each communicated message primitive such as user's identity, hash operation, random nonce, PUF challenge in CRP, ECC-based scalar point, and timestamp take 160, 256, 160, 160, 320, and 32 bits, respectively. The communication cost of [25], [27], [28], [29], [30], [31], [32], [33], and [34] is computed as 340, 396, 396, 368, 304, 308, 364, 492, 240, and 488. It can be witnessed that PDCM-IoD bears a lower communication cost than [33], while other schemes have a lower communication cost comparatively. However, these schemes are susceptible to many security threats despite low communication cost as shown in Table V. In this study, we can witness that PDCM-IoD overcomes most of these attacks due to judicious use of BS-PUF with comparably low computational overhead. Overall, the PDCM-IoD supports a 19.52% increase number of security features. Although PDCM incurs slightly higher communication costs due to extra communicational exchanges, this tradeoff is justified by the scheme's lower computational cost and improved overall security.

VII. CONCLUSION

This study aims to provide a lightweight and secure communication framework for users, drones, and GCMS. A novel BS-PUF-based drone access control technique PDCM-IoD is introduced for the IoD system. The use of symmetric key-based operations along with commutative features of PUF in the design of PDCM-IoD assures attaining mutual authenticity among participants. Moreover, the unique design of the proposed technique also helps in gaining anonymity, unlinkability, conditional revocation for legal but malicious users, and resistance to other known attacks, including physical drone compromise threats. The suggested scheme is

[1]Trademarked.

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

TABLE V
COMPUTATIONAL COSTS

	U_i	GCMS	D_j	Total Computational cost (msec.)	Comm. Bits Exchanged
[25]	$6T_h+2T_{PM}$	$8T_h$	$5T_h+2T_{PM}$	$19T_h+4T_{PM}\approx 21.47$	2720
[27]	$11T_h$	$6T_h$	$10T_h$	$27T_h\approx 0.365$	3168
[28]	$T_{fe}+15T_h$	$2T_S+9T_h$	$7T_h$	$T_{fe}+2T_S+31T_h\approx 0.566$	3168
[29]	$8T_h$	$10T_h$	$2T_{PUF}+6T_h$	$2T_{PUF}+24T_h\approx 0.420$	2944
[30]	$T_{fe}+11T_h$	$11T_h$	$T_{fe}+10T_h$	$2T_{fe}+32T_h\approx 0.592$	2432
[31]	$14T_h$	$9T_h$	$7T_h$	$30T_h\approx 0.401$	2464
[32]	$8T_h$	$6T_h$	$2T_{PUF}+6T_h$	$2T_{PUF}+20T_h\approx 0.406$	2912
[33]	$10T_h+4T_{PUF}$	$9T_h+5T_{PUF}$	$3T_h+3T_{PUF}$	$12T_{PUF}+22T_h\approx 0.654$	3936
[34]	$T_{fe}+1T_{PM}+1T_a+7T_h$	$2T_a+2T_h$	$2T_{PM}+1T_a+3T_h$	$T_{fe}+3T_{PM}+4T_a+12T_h\approx 16.24$	1924
PDCM-IoD	$11T_h+4T_{PUF}$	$13T_h+4T_{PUF}$	$4T_{PUF}+7T_h$	$12T_{PUF}+31T_h\approx 0.723$	3904

comparable to contemporary models in terms of communication, computational overheads, and security features. The RoR model-assisted formal security analysis and performance assessment demonstrates that PDCM-IoD could meet the test of time for next-generation IoD networks concerning industrial applications.

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest to report regarding the present study.

ACKNOWLEDGMENT

The authors would like to thank the Abu Dhabi University's Office of Research and Sponsored Programs for sponsoring this endeavor.

REFERENCES

[1] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in UAV communication networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1123–1152, 2nd Quart., 2016.

[2] Y.-J. Chen and L.-C. Wang, "Privacy protection for Internet of Drones: A network coding approach," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1719–1730, Apr. 2019.

[3] W. Yang, S. Wang, X. Yin, X. Wang, and J. Hu, "A review on security issues and solutions of the Internet of Drones," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 96–110, 2022.

[4] A. Irshad, S. A. Chaudhry, A. Ghani, and M. Bilal, "A secure blockchain-oriented data delivery and collection scheme for 5G-enabled IoD environment," *Comput. Netw.*, vol. 195, Aug. 2021, Art. no. 108219.

[5] S. A. Chaudhry, A. Irshad, B. A. Alzahrani, A. Alhindi, M. Shariq, and A. K. Das, "TS-PAID: A two-stage PUF-based lightweight authentication protocol for Internet of Drones," *IEEE Access*, vol. 13, pp. 1458–1469, 2025.

[6] B. A. Alzahrani and A. Irshad, "An improved IoT/RFID-enabled object tracking and authentication scheme for smart logistics," *Wireless Pers. Commun.*, vol. 129, no. 1, pp. 399–422, Mar. 2023.

[7] A. Irshad, M. Farooq, K. Mahmood, G. A. Mallah, and S. A. Chaudhry, "DAC-MD: A privacy preserving drone-access control scheme for last mile delivery," *Trans. Emerg. Telecommun. Technol.*, vol. 35, no. 3, Mar. 2024, Art. no. e4958.

[8] A. A. Alshdadi and A. Irshad, "PDAC-SL: A PUF-enabled drone access control technique for smart logistics," *Alexandria Eng. J.*, vol. 107, pp. 747–756, Apr. 2024.

[9] Y. Mekdad et al., "A survey on security and privacy issues of UAVs," *Comput. Netw.*, vol. 224, Apr. 2023, Art. no. 109626.

[10] C. Lin, D. He, N. Kumar, 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.

[11] A. Irshad, B. A. Alzahrani, A. Albeshri, K. Alsubhi, A. Nayyar, and S. A. Chaudhry, "SPAKE-DC: A secure PUF enabled authenticated key exchange for 5G-based drone communications," *IEEE Trans. Veh. Technol.*, vol. 73, no. 4, pp. 5770–5780, Apr. 2024.

[12] 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.

[13] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of Drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.

[14] T. Alladi, Naren, G. Bansal, V. Chamola, and M. Guizani, "SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 15068–15077, Dec. 2020.

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

[16] G. Bansal and B. Sikdar, "S-MAPS: Scalable mutual authentication protocol for dynamic UAV swarms," *IEEE Trans. Veh. Technol.*, vol. 70, no. 11, pp. 12088–12100, Nov. 2021.

[17] T. Wu, X. Guo, Y. Chen, S. Kumari, and C. Chen, "Amassing the security: An enhanced authentication protocol for drone communications over 5G networks," *Drones*, vol. 6, no. 1, p. 10, Dec. 2021.

[18] T. Li et al., "Energy-efficient and secure communication toward UAV networks," *IEEE Internet Things J.*, vol. 9, no. 12, pp. 10061–10076, Jun. 2022.

[19] S. Yu, A. K. Das, Y. Park, and P. Lorenz, "SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for Internet of Drones in smart city environments," *IEEE Trans. Veh. Technol.*, vol. 71, no. 10, pp. 10374–10388, Oct. 2022.

[20] S. Zhang, Y. Liu, Z. Han, and Z. Yang, "A lightweight authentication protocol for UAVs based on ECC scheme," *Drones*, vol. 7, no. 5, p. 315, May 2023.

[21] I. Chandran and K. Vipin, "A PUF secured lightweight mutual authentication protocol for multi-UAV networks," *Comput. Netw.*, vol. 253, Nov. 2024, Art. no. 110717.

[22] C. Tian, Q. Jiang, T. Li, J. Zhang, N. Xi, and J. Ma, "Reliable PUF-based mutual authentication protocol for UAVs towards multi-domain environment," *Comput. Netw.*, vol. 218, Dec. 2022, Art. no. 109421.

[23] A. Karmegam, A. Tomar, and S. Tripathi, "Blockchain-based cross-domain authentication in a multi-domain Internet of Drones environment," *J. Supercomput.*, vol. 80, no. 19, pp. 27095–27122, Dec. 2024.

[24] Y. K. Ever, "A secure authentication scheme framework for mobile-sinks used in the Internet of Drones applications," *Comput. Commun.*, vol. 155, pp. 143–149, Apr. 2020.

[25] M. Nikooghadam, H. Amintoosi, S. H. Islam, and M. F. Moghadam, "A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance," *J. Syst. Archit.*, vol. 115, pp. 1–16, May 2021.

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.

[26] S. A. Chaudhry et al., "GCACS-IoD: A certificate-based generic access control scheme for Internet of Drones," *Comput. Netw.*, vol. 191, May 2021, Art. no. 107999.
[27] C.-T. Li, C.-Y. Weng, C.-L. Chen, C.-C. Lee, Y.-Y. Deng, and A. L. Imoize, "An efficient authenticated key agreement scheme supporting privacy-preservation for Internet of Drones communications," *Sensors*, vol. 22, no. 23, p. 9534, Dec. 2022.
[28] S. Hussain, K. Mahmood, M. K. Khan, C.-M. Chen, B. A. Alzahrani, and S. A. Chaudhry, "Designing secure and lightweight user access to drone for smart city surveillance," *Comput. Standards Interface*, vol. 80, Mar. 2022, Art. no. 103566.
[29] M. Sharma, B. Narwal, R. Anand, A. K. Mohapatra, and R. Yadav, "PSECAS: A physical unclonable function based secure authentication scheme for Internet of Drones," *Comput. Electr. Eng.*, vol. 108, May 2023, Art. no. 108662.
[30] Y. Park, D. Ryu, D. Kwon, and Y. Park, "Provably secure mutual authentication and key agreement scheme using PUF in Internet of Drones deployments," *Sensors*, vol. 23, no. 4, p. 2034, Feb. 2023.
[31] D. Chaudhary, T. Soni, K. L. Vasudev, and K. Saleem, "A modified lightweight authenticated key agreement protocol for Internet of Drones," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100669, doi: 10.1016/j.iot.2022.100669.
[32] Z. Zhang et al., "PRLAP-IoD: A PUF-based robust and lightweight authentication protocol for Internet of Drones," *Comput. Netw.*, vol. 238, Jan. 2024, Art. no. 110118.
[33] T.-F. Lee, X. Ye, and W.-J. Huang, "Lightweight privacy-preserving authenticated key agreements using physically unclonable functions for Internet of Drones," *J. Inf. Secur. Appl.*, vol. 87, Dec. 2024, Art. no. 103915.
[34] M. de Jesus Sousa and P. R. L. Gondim, "A multi-factor user authentication protocol for the Internet of Drones environment," *Peer-Peer Netw. Appl.*, vol. 18, no. 2, pp. 1–22, Mar. 2025.
[35] Y. Guo, T. Dee, and A. Tyagi, "Barrel shifter physical unclonable function based encryption," *Cryptography*, vol. 2, no. 3, p. 22, Aug. 2018.
[36] S. A. Chaudhry et al., "A physical capture resistant authentication scheme for the Internet of Drones," *IEEE Commun. Standards Mag.*, vol. 5, no. 4, pp. 62–67, Dec. 2021.
[37] D. Dolev and A. C. Yao, "On the security of public key protocols, (PDF)," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 2, pp. 198–208, Feb. 1983.
[38] R. Canetti, O. Goldreich, and S. Halevi, "The random Oracle methodology, revisited," *J. ACM*, vol. 51, no. 4, pp. 557–594,Jul. 2004.
[39] O. Millwood, J. Miskelly, B. Yang, P. Gope, E. B. Kavun, and C. Lin, "PUF-phenotype: A robust and noise-resilient approach to aid group-based authentication with DRAM-PUFs using machine learning," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2451–2465,2023.
[40] M. Tanveer, A. U. Khan, N. Kumar, and M. M. Hassan, "RAMP-IoD: A robust authenticated key management protocol for the Internet of Drones," *IEEE Internet Things J.*, vol. 9, no. 2, pp. 1339–1353, Jan. 2022.
[41] Q. Xie and H. Wang, "PUF-based secure and efficient anonymous authentication protocol for UAV towards cross-domain environments," *Drones*, vol. 9, no. 4, p. 260, Mar. 2025.
[42] D. Shui and Y. Xie, "A PUF-based lightweight mutual authentication scheme for IoT devices," in *Proc. Int. Conf. Frontiers Cyber Security*. Singapore: Springer, Jul. 2024, pp. 180–200.
[43] A. Shahidinejad and J. H. Abawajy, "Anonymous blockchain-assisted authentication protocols for secure cross-domain IoD communications," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 3, pp. 2661–2674, May 2024.
[44] Y. Harbi, Z. Aliouat, S. Harous, and A. M. Gueroui, "Lightweight blockchain-based remote user authentication for fog-enabled IoT deployment," *Comput. Commun.*, vol. 221, pp. 90–105, May 2024.
[45] K. Huang, H. Hu, and C. Lin, "BAKAS-UAV: A secure blockchain-assisted authentication and key agreement scheme for unmanned aerial vehicles networks," *IEEE Internet Things J.*, vol. 11, no. 22, pp. 36858–36883, Nov. 2024.
[46] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing IoT network security through deep learning-powered intrusion detection system," *Internet Things*, vol. 24, Dec. 2023, Art. no. 100936.
[47] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Comput. Electr. Eng.*, vol. 99, Apr. 2022, Art. no. 107810.

Authorized licensed use limited to: Abu Dhabi University. Downloaded on February 12,2026 at 07:04:16 UTC from IEEE Xplore. Restrictions apply.