IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 27 February 2024, accepted 19 March 2024, date of publication 27 March 2024, date of current version 2 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3382579

RESEARCH ARTICLE

PSLAPS-IoD: A Provable Secure and Lightweight Authentication Protocol for Securing Internet-of-Drones (IoD) Environment

FAHAD ALGARNI[1] **AND SAEED ULLAH JAN**[2]
[1]Faculty of Computing and Information Science, Department of Computer Science, University of Bisha, Bisha 14174, Saudi Arabia
[2]Higher Education Department of Khyber Pakhtunkhwa, Government College Wari (Dir Upper), Wari, Khyber Pakhtunkhwa 18200, Pakistan

Corresponding author: Fahad Algarni (fahad.alqarni@ub.edu.sa)

This work was supported by the Deanship of Graduate Studies and Scientific Research at the University of Bisha through the Fast-Track Research Support Program.

ABSTRACT The infrastructureless architecture for Internet-of-Drones (IoD) environment regulates drones in airspace for performing tactical tasks. Synergy is crucial for IoD participants; otherwise, complex task completion is impossible because IoD is a newer area that has gained more attention for domestic and commercial usage. However, wireless communication in the IoD environment is prone to numerous threats; security and privacy are among the top challenges. If all the participating entities of IoD become securely authenticated, then information broadcasting will never be confronted by a strong adversary. Therefore, in this research article, we have designed a robust and lightweight security mechanism based on a fuzzy extractor and the MD5 (Message Digest 5) method to authenticate all IoD participants and ensure secure communication. The security analysis of the proposed biometric-based authentication mechanism has been formally verified through a simulation toolkit ProVerif and Random-Oracle Model (ROM) and informally through propositions. The performance metrics of the proposed protocol have been measured by considering communication and computation costs. The result obtained from the security and performance analysis sections shows that the secrecy, reachability, and confidentiality of the session secret key are, of course, ensuring secure information communication for the IoD environment. When comparing it with prior works, the result demonstrated that it can be strongly recommended for practical implementation in the IoD environment.

INDEX TERMS Authentication, MD5, security, confidentiality, IoD, privacy, fuzzy extractor, attacks.

I. INTRODUCTION

Unmanned aerial vehicles (UAVs), commonly known as drones, offer unique characteristics such as mobility, ease of deployment and maintenance, and the ability to measure various quantities anywhere, at any time. A drone can affordably collect and send data (such as pictures or videos) and analyze the necessary parts to make intelligent decisions [1]. The network of drones—now called the Internet of Drones (IoD)—facilitates the coordination of drones in the airspace and has the same characteristics as IoT [2]. The IoD is frequently referred to as a layered network control architecture that provides navigation services and coordinates drone access to regulate it in the airspace [3]. Due to its apparent benefits (mobility, portability, and automation), the IoD has recently gained popularity in both industry and academia. Drones have been used in various industries, including agriculture, air traffic control, and the military. Drones are used in the IoD environment's flying domains, where they communicate with each other and with the ground station server (GSS) for transmitting data intelligently [4].

Similarly, with the global expansion of the drone business model, commercial UAVs provide numerous benefits to the business community, and a sizable number of drone accidents

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

© 2024 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

are recorded each week. A suitable mitigation technique is required to efficiently recognize and detect UAV dangers in their earliest stages to prevent such events [5]. These security techniques also give the operator enough time to set up the necessary equipment to countermeasure such incidents/attacks. It is also crucial to consider the potentially risky applications for such a sensitive IoD environment. In actuality, the increasing growth of UAVs results in various weaknesses in both their physical and cyber components [6]. As the UAV deployment geography expands, governments are becoming increasingly concerned about the security and privacy essences of it in the national airspace. Additionally, the majority of commercial UAVs in use today lack security features like intrusion detection systems [7].

As discussed, the use of drones is becoming ubiquitous, leading to an increase in many attacks on systems. For instance, attackers may target drones' radio connections to prevent the system from communicating with mobile users' (MUs) devices. Attackers can intercept when a drone sends information or establishes communication with the GSS or MU and steals command and control signals for malicious deeds. The adversary can also operate the drone directly using the data they have collected/captured from the open channel. Also, attackers can remotely hijack drones by taking advantage of flaws in the drone software. Adversaries can manipulate GPS signals for disreputable purposes when malicious software programs on drones influence them [5]. As these signals are synchronized with GSS, the intelligent command and control must be carefully managed and controlled because they are transmitted by autonomous drones across multiple channels with changing transmission ratios. Therefore, the IoD systems must be able to identify the security of wireless communication channels and shared data [6].

Despite developing a wide range of potential solutions for drone transmissions involving sensitive and essential data, security is still a top issue for the IoD environment. Effective cyber-attacks on UAVs have been seen all over the world. Real-world cyber-attacks against civilian UAVs are now considered a national security issue. UAV security concerns have sparked a meaningful conversation among governments and organizations in the public and private sectors following their integration into the country's airspace. The range of current cyber-attacks shows that UAVs are vulnerable at various levels from a security perspective. The widespread use of drones for civilian purposes benefits hostile actors. They actively endanger people's safety by utilizing the flaws of various commercial drones [8].

With the rapid invention, modification, and manufacturing of embedded sensors, the fast-processing speed of the Central Processing Unit (CPU), and the universal connectivity of wireless networks, drones have been used for different purposes to advance our lifestyles like infrastructure inspection, fire and wildlife surveillance, cinematography, and agriculture-land monitoring [9]. Also, UAVs should be incorporated into the national airspace for sensitive installations like chemical and nuclear power plants and monitor the privacy of public users. However, these various drone applications can provide security and privacy challenges as most UAVs have cameras on board, which could reveal sensitive information about human activities. To that purpose, the absence of adequate security measures that can ensure the traditional trinity, like the CIA (Confidentiality, Integrity and Availability), makes cyber-attacks possible against UAVs [10]. Therefore, we must examine UAVs from a security and privacy perspective, which can only be solved by designing a robust and flawless authentication protocol.

A. MOTIVATIONS

The wireless communication in IoD is prone to several threats, including Denial-of-Service(DoS) insider, replay, side-channel, impersonation, man-in-the-middle (MITM), password guessing, and traceability attacks, which, in turn, can create security and privacy issues. These issues must be appropriately addressed to make communication secure among all the participants in the IoD environment. To do so, secure authentication is much needed to ensure secure communication in the IoD environment. Also, a lightweight authentication scheme can deliver efficient services to such a resource-constrained technology due to UAVs' limited flight time and low battery power. Therefore, a lightweight and robust security cryptographic technique is needed to design a robust authentication scheme. All these things motivated us to design a security framework for securely authenticating all the entities in the IoD environment, which, in turn, can ensure secure communication.

B. PROBLEM STATEMENT

Nowadays, drone communication continuously faces security and privacy issues and challenges; robust authentication of all the participating entities is necessary for secure broadcasting to be achieved. Communication mostly occurs in a hostile environment; security and privacy are significant features of IoD; if the IoD participants have not been authenticated properly, an attacker harms the system. In this regard, researchers have proposed numerous authentication schemes (discussed in the literature survey section of the article) over the last decades; however, their schemes are either suffer from impersonation, traceability, offline password-guessing, stolen verifiers, forgery, known-key, Ephemeral Secret Leakage (ESL), brute-force, and side-channel attacks or consumes more hardware cycles and expand the exchange message by presenting lengthy bits. Also, the third part key generation (PKG) can easily be compromised, and the issue of implicit key escrow is usually generated on the user's computer. Therefore, in this article, we have proposed a provable, secure and lightweight authentication protocol and named it PSLAPS-IoD for securing the Internet-of-Drones (IoD) Environment. The other common issues and challenges faced by IoD are described as follows:

- GPS Spoofing/Jamming – The Attacker might align fake signals on the actual signal due to low frequency and limited bandwidth and, in turn, hack the system for spoofing attacks.
- An attacker can quickly launch attacks on IEEE 802.11 and IEEE 802.15 ports.
- The drone captures photos/videos that contain hidden information like coordinates, resolution, manufacturer data, and recording and shooting time, exposing to the privileged users that cause harm to the system.
- The broken communication session needs a robust authentication scheme to handle the heterogeneous networking nature of IoD, which is the need of the day as IoD lacks fixed network topology.
- Hackers use frequency interference for malicious deeds and take control of the whole IoD system.
- A de-authentication attack is expected in which the attacker changes the system's synchrony, and the legal drone sends its message to the attacker instead of the ground station server (GSS).

C. OBJECTIVES

Different cryptographic techniques are discussed by researchers from time to time in the literature. Each method has its own merits as well as demerits. However, a few of them are lightweight and provide secure authentication; minimum computation resources are required and take less memory space, but they are not effective as they are limited in terms of functionality. Therefore, the main objectives of this research were as follows:

- To design an efficient security framework for securely authenticating the IoD participants; this, in turn, can ensure the information broadcasting of the IoD environment.
- To design a secure framework so that it can work in any drone, from small to very large.
- To design a security framework that can resist all known threats.
- The drone, when sending the shooting videos/audio/pictures/etc., will never be open to anyone, even the person sitting in the ground station server (GSS).
- To analyze the security of the proposed framework using the random oracle model (ROM) and pragmatic illustrations/propositions.
- To simulate the proposed security protocol using a programming verification toolkit ProVerif2.03.
- To analyze the proposed protocol for performance metrics by considering communication and computation costs.
- To comparatively analyze the proposed protocol for performance metrics and security functionalities.

D. CONTRIBUTIONS

This research aimed to secure information communication for drone technology by reliably authenticating each entity. Because the different cryptographic techniques discussed by numerous researchers from time to time in the literature are posed with multiple vulnerabilities, each method has its own merits and demerits. But a few are lightweight and provide secure authentication; minimum computation resources are required and take less memory space. However, they are posed to insider, impersonation, physical capture, and MITM attacks; therefore, to cope with these vulnerabilities, the main contributions of this research work are as follows:

- A lightweight and secure protocol has been designed for IoD in which we have used a cryptographic hash function, XOR operations, and concatenation function for protecting secret keys and securing the exchange of keys among all IoD participants while communicating.
- The proposed security mechanism is robust because when the adversary possesses the hash values, it is still difficult for them to crack the key.
- All the parameters in the proposed protocol are safe. This claim is scrutinized using a widely accepted method, the ROM analysis.
- Key secrecy, integrity, reachability, and authorization have been confirmed by simulating the proposed protocol through a programming toolkit called ProVerif.
- The proposed protocol performance and security balancing strategies have been achieved, which is a difficult task, as these two functionalities contradict each other, and the change in one inversely affects the other.

E. SIGNIFICANCE

All the efforts of the researchers will be helpful in various walks of life, as explained as follows:

- The framework can be used for small UAVs operationalized in electronic media, cinematography, and search-and-rescue purposes in the civilian domain.
- The framework will be fast and secure for a drone used in infrastructure inspection, agricultural land monitoring, and wildlife surveillance.
- The scheme, if installed in UAVs, can effectively be utilized for package delivery and weather forecasting purposes.
- The robust mechanism might be used for drones deployed for heat-sensing, sidewalk-monitoring with the help of smart objects, and car parking control.
- The said technique can be used for drones operationalized for strategic purposes like reconnaissance and attacking drones, traffic, extensive damage investigation after earthquakes/floods, forest-fire monitoring, and troop movements.

F. TECHNOLOGICAL INNOVATIONS

Drones are becoming increasingly popular, which has sparked an exciting discussion on how best to employ them. This argument has mostly focused on their frequent usage in fighting and espionage, emphasizing their use in the civilian domain. Drone technology involves drones' design principles, flight time, capabilities, and applications. These innovations have significantly improved drone performance, functionality, and versatility across various domains. Upon designing a drone, the following major aspects need to be taken into consideration:

1. Without compromising functionalities, drones should be designed to be smaller, lighter, portable, and suitable for various applications.
2. Power efficiency allows drones to stay for a longer time in the airspace and longer mission delivery.
3. To enhance the stability and precision of drones, the company must consider gyroscopes, accelerometers, and GPS for precise navigation and control.
4. To improve a drone's capability, sensors, high-resolution cameras, LiDAR (Light Detection and Ranging), thermal imaging, and multispectral sensors can be equipped flawlessly so that they can easily be deployed for various applications, including aerial photography, mapping, surveying, agriculture, and environmental monitoring.
5. Designing a robust and lightweight security framework enables drones to perform complex tasks autonomously, such as route planning, obstacle avoidance, and object recognition. This allows for more efficient and reliable operation in diverse environments.
6. Synergy is crucial among drones to operationalize them in clusters and that can enable them to communicate and coordinate for task completion collaboratively.
7. Tracking, accountability, and collision avoidance regulatory and safety measures should carefully be taken into consideration to restrict flight in certain areas and remote identification systems and prevent them from possible collisions.

Overall, these technological innovations continue to drive the evolution of drones, expanding their capabilities and enabling new applications across various fields, motivating us to design a provable, secure and lightweight authentication protocol and name it PSLAPS-IoD for securing the Internet-of-Drones (IoD) Environment.

G. PAPER LAYOUT

This research is organized as follows: In section II, we present the preliminaries of this research; section III demonstrates the comprehensive literature review; and section IV offers the proposed security protocols for achieving the objectives, such as using the hash cryptographic function ($h(\cdot)$), ($\oplus$) operations, MD5, Fuzzy Extractor methods, and concatenation function ($\|$) for the protocol's design. Section V evaluates the security and performance of the proposed security mechanism using the ROM. We simulate the proposed protocol using the programming verification toolkit ProVerif. The performance evaluation can be tackled by considering communication and computation costs. In section VI, we conclude the work.

II. PRELIMINARIES

In this section we go through the definitions and basic concepts of some cryptographic hard problems.

A. MESSAGE DIGEST (MD5)

A message-digest algorithm (MD5) is a collision-free one-way hash cryptographic function in which we input arbitrary values and output a fixed-length digest, which can be used to verify the validity of the exact message sent earlier. A prevalent hash function in cryptography is MD5, or "message digest 5." From the data input, which is normally stated as a 32-digit hexadecimal number, MD5 generates a 128-bit message digest. Regardless of the input size, MD5 hashes are distinguishable for miscellaneous inputs [11].

B. THREAT MODEL

According to the threat model [12], the possible threat to a system can either be passive or active. A prominent threat includes illicit tracking, in which an adversary can track the location of each uniquely identified object inside IoD. Eavesdropping is another threat in which an attacker listens to the communication among the IoD participants. At the same time, in an MITM attack, the adversary might divert, copy, or delete contents from a message or insert false information in it to masquerade the legitimate participants. Similarly, an adversary can also block a message by creating a desynchronization attack in which the GSS does not update its secret credentials. In the upcoming session, the forward and backward secrecy are badly affected. The adversary can also hang the services of a GSS for a drone as well as a mobile device (MD), which, in turn, causes a DoS attack. The adversary uses reverse engineering techniques to find the secret credentials from a message that they have caught from the open network channel. The adversary can get the private key by entering the GSS later and launching cold boot attacks, side-channel attacks, and physically captured attacks. While obtaining the secret key, the adversary can also trace the drone easily, including its location, coordinates, and flying time [13].

C. PROVERIF

ProVerif stands for protocol verifier—a software toolkit for checking, verifying, and certifying a protocol's internal secrets. It is a widely used language for analyzing a cryptographic-based protocol's reachability and correspondence assertions. It also proves a protocol's secrecy, evaluates events, and confirms authorization and authentication. A ProVerif model uses applied calculus to consist of the initialization/declaration, process, and core parts. We used the ProVerif toolkit to verify, validate, and confirm a protocol's security [14].

D. FUZZY EXTRACTOR

A fuzzy extractor method is used to verify a user's biometrics by applying two algorithms, Gen(.) and Rep(.). The Gen(.)

algorithm is probabilistic, takes biometrics as the input, and generates a biometric-based key (BK) with reproductive parameters (RP) like Gen(Bio) = {BK, RP}. The Rep(.) algorithm is deterministic, which means the input is noisy biometric (B^*), and the RP aims to recover the original biometric-based key (BK) like Rep(B^*, RP) = BK, which is subject to the condition that hamming distance between B and B^* is a pre-defined error tolerance [15].

E. NETWORK MODEL

The network model demonstrated herein consisted of four participating entities (i.e., an MD, a drone, the GSS, and the trusted third-party server [TTPS], as shown in Figure 1). These are described as follows:

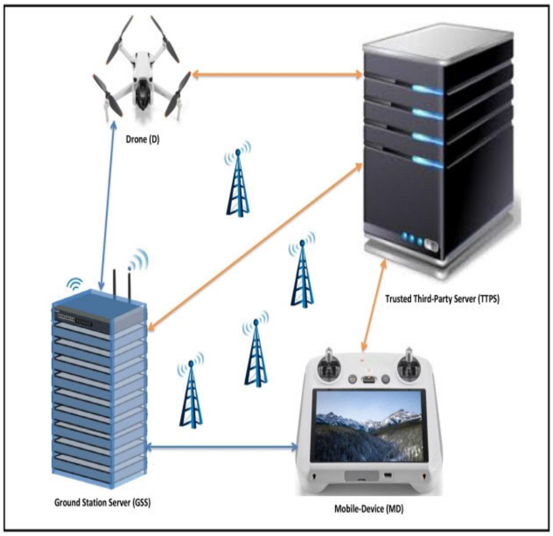

Drone (D)
Trusted Third-Party Server (TTPS)
Ground Station Server (GSS)
Mobile-Device (MD)

FIGURE 1. System model.

a) Mobile Device (MD): This hand-held device is used for receiving/sending messages to and from the GSS. Upon confirmation by the GSS, the MD will be authenticated with D to establish a secure secret session key (SK).
b) Drone (D): The drone sends/receives credentials to and from the GSS for record creation/checking and establishing a secure secret SK. It is also authenticated with the MD with the help of the GSS. The drone (D) is the leading participant and consists of sensors, actuators, propellers, batteries, and frames. All these are equipped for physical phenomenon checking and information gathering.
c) Ground Station Server (GSS): It facilitates the secure communication of the drone (D) and MD, mutually authenticates each other through wireless network channels, and establishes closed sessions for tactical task completion.
d) Trusted Third-Party Server (TTPS): A company that installs the whole system to provide networking and related facilities. This is a fully trusted entity because every entity is first registered with TTPS and then functionalized in IoD. TTPS stored all the shared credentials in all the participating entities for future communication and collaboration; however, synergy is mandatory among them; otherwise, they cannot perform complex tasks.

F. RANDOM ORACLE MODEL (ROM)

ROM [16], [17] should carefully consider and assess the robustness of a cryptographic-based protocol by utilizing system engineering concepts and confidence. The analysis determines if a protocol is credible and verifies the security of a protocol, synchronization, and integrity for parties in communication. It is a well-known and often-used method for formal security analysis of a cryptographic protocol. This paradigm gives an attacker every opportunity, and we will use ROM to verify it by forming all oracles.

III. LITERATURE SURVEY

Turkanovic et al. [18] proposed a simple hash cryptographic and XOR-based scheme, which can authenticate the user, sensor node, and gateway node reliably, and their scheme achieved high-security features. In their scheme, the IoT and wearable sensors agree on a secret session key SK, which can be used for secure message broadcasting. However, the Turkanovic et al. scheme is unsafe against MITM, IoT impersonation, and stolen smart card attacks. Also, the Turkanovic et al. scheme has failed to resist traceability, anonymity, and session key secrecy.

Farash et al. [19] proposed an improved scheme by cryptanalysis of the Turkanovic et al. [18] scheme by identifying many loopholes and saying that in the Turkanovic et al. [18] scheme, after successful authentication, the user and sensing node create a secure session for future secure communication. However, it was found that Farash et al. [19] scheme is also vulnerable to user impersonation, known session-specific temporary information, new smart card issues, and offline password-guessing attacks with the help of stolen or lost smart card attacks. In addition, their scheme fails to maintain user anonymity, and the gateway node secrecy is not preserved.

The signature-based user authentication and key-exchange schemes [20], [21], and [22] have been presented for IoT systems. Their mechanisms perfectly supported user authentication, non-repudiation, and key agreement among all the participating entities. Their hybrid cryptosystem makes the mechanisms for utilizing multiple IoT systems from very small to large. However, batch verification makes their schemes inefficient in communication and computation.

Hong et al. [23] designed a scheme using paring cryptography. Their scheme has caught much attention because it (i) offers a desired level of security, (ii) ensures the efficiency of pairing computations, and their scheme is responsible for generating and escrowing users' private keys. However, their protocol has many drawbacks, including (i) the communication costs of a paring-based key is 1024 bits, which maximizes storage and communication costs; (ii) their

TABLE 1. Critical literature review.

Article	Methodology	Drawbacks
Zhong et al. [31]	Bilinear Map, Paring Cryptography, Computational Diffie-Hellman Problem, and Certificateless Aggregate Signature-based scheme for VANET technology	Due to point multiplication, modular exponentiation, aggregation and bilinear pairing, the performance does not balance with security.
Tanveer et al. [32]	Biometric Fuzzy Extractor and Authenticated Encryption with Associative Data (AEAD)	Prone to insider and DoS threats because the message A_4 from MU to MS contains SID_{MU} and SID_{MS}, which an attacker can catch and launch insider and DoD attacks.
Pu and Li [33]	Physical Unclonable Function (PUF) and Chaotic Mapping strategies for UAVs deployed in IoD environment.	In the authentication phase of the protocol, the ID_x from the UAV side is transmitted openly towards the GCS, which means that the mechanism is prone to replay, traceability and impersonation attacks.
Alladi et al. [34]	Physical Unclonable Function (PUF) is a based authentication scheme for software-defined UAV networks.	The researchers did not implement their protocol for any well-known method, so how can one say that their strategy is suitable for practical implementation in Software Unmanned Aerial Vehicular Networks (SDUAVN?
Nikooghadam et al. [35]	Elliptic Curve Cryptography (ECC)-based key-agreement scheme for IoD environment	In the login and authentication phase of the protocol, the message from the control server towards the drone is vulnerable because the K_{ij} is in plain text format; thus, the attacker can catch and use it for numerous malicious purposes.
Ozmen and Yavuz [36]	Symmetric cryptography, Public Key Infrastructure (PKI), and elliptic curves-based framework for small areal UAVs.	The private key of their Boyko-Peinado-Venkatesan (BPV) mechanism is too high, which specifically degrades the performance metrics.
Li et al. [37]	Identity, ECDHP, and Elliptic Curve Cryptographic (ECC)-based authentication protocol for UAV and base stations.	The researchers failed to measure the communication and computation costs of their schemes.
Singh et al. [38]	Guillou-Quisquater, Elliptic Curve digital signature, and Diffie-Hellman Key exchange algorithms were used to design a scheme for human-centric IIoT.	They failed to analyze the security of their proposed security mechanism. Prone to traceability and insider threats.
Zhang et al. [39]	Hash cryptographic and XOR functions have been used to design a scheme for the IoD environment.	The scheme is prone to side-channel attacks, as the last round does not record the current timestamp. Prone to DoS and traceability attacks.
Park et al. [40]	Fuzzy extractor, PUF, hash, and XOR functions were used to design a mutual authentication and key-agreement scheme for the IoD environment.	The second message transmitted from the control server towards the drone has ID_m, which the attacker uses for traceability and violates anonymity.
Gope et al. [41]	Pseudo-random function, fuzzy extractor, and PUF-based authentication scheme for RFID-enabled UAVs.	It has been revealed from the study that their scheme is prone to impersonation and DoS attacks.

scheme was considered unmanageable; (iii) their scheme needs a private key generator (PKG) for each UAV, which is difficult for each UAV to have; (iv) they presented a more complex method; and (v) an indistinguishability problem is also noted in their technique.

Benzarti et al. [24] argued that public key cryptography could simultaneously fulfil both the functions of digital signature and public key encryption in a logically single step by reducing computational and communication overheads, static key management, and more substantial integrity, non-repudiation, unforgeability, and confidentiality. However, signing a message digitally and then encrypting consumes more hardware cycles, expanding the exchange message by presenting lengthy bits.

Haque et al. [25] presented an identity encryption-based protocol by saying that identity-based schemes can reduce encryption complexity and concentrate the software to deliver fast and secure services. It removes certification and can also be materialized for specified environments very easily. However, the third part, key generation, can easily be compromised; the issue of implicit key escrow is usually generated on the user's computer.

Won et al. [26] materialized three protocols suitable for drones, namely an efficient certificateless signcryption tag key encapsulation mechanism (eCLSC-TKEM), certificate multi-recipient encryption scheme (CL-MRES), and certificates data aggregation (CLDA). Though it is a secure mechanism, it does not deliver efficiently due to aggregation. Therefore, Won et al. [26] protocol suits suffer from low performance and balancing security with performance is a major issue.

Srinivas et al. [27] offered a TCALAS (Temporal Credential-Based Anonymous Lightweight Authentication Scheme) scheme for the IoD environment; however, it does not provide perfect forward secrecy. Chen et al. [28] and Ali et al. [29] proposed hybrid cryptosystem-based key-agreement schemes for civilian drones for controlling traffic, pollution, stealth, and pressure measurement in a big smart city. However, it has been observed that their schemes are suffering from stolen verifiers and forgery attacks. Cho et al. [30] proposed HMAC, PBKDF, and SHA-512-based schemes for small UAVs for package delivery purposes. However, with the existence of a strong adversary and weak cryptographic technique, their scheme is vulnerable to known-key, Ephemeral Secret Leakage (ESL), brute-force, and side-channel attacks. A summary of the literature review is shown in Table 1.

IV. PROPOSED PROTOCOL

This section presents an authentication scheme for securely authenticating each participant to ensure secure message broadcasting in the IoD environment. To do so, this mechanism consisted of setup, registration, and mutual authentication phases, which are described individually in the following subsections. The different notations used are shown in Table 2.

TABLE 2. Notations and their descriptions.

Notation	Description
S_{TTPS}	TTPS private key
ID_{GSS}	GSS identity
ID_{MD}	MD identity
AD_D	Drone identity
r_{GSS}	GSS random number
r_{MD}	MD random number
r_D	Drone random number
N_D	Nonce for Drone
$\|\|$	Concatenation function
$\oplus$	XOR Operations
PK_{GSS}	GSS Public Key
PK_{MD}	MD Public Key
PK_D	Drone Public Key
PW_D	Drone password
B	Biometric
Gen(.)	Generation function
Rep(.)	Replication Function
σ_D, β_D	Random values for Biometric
h(.)	Hash function
T	Timestamp
P	Large prime number
s	Secret key of TTPS
S_{GSS}	Hash image for Ground Station Server identity
S_{MD}	Hah image for Mobile Device identity
HID_D	Hah image for Drone identity

A. SETUP PHASE

Each IoD participant is configured, and the irreplaceable credentials are stored in the TTPS's memory. TTPS chooses a private key S_{TTPS} for registering each participating entity, including the ground station server (GSS), mobile device (MD) and drone (D).

B. GSS REGISTRATION

The TTPS, while registering GSS, chooses an identity ID_{GSS} for GSS, selects a random number r_{GSS}, computes $PK_{GSS} = r_{GSS}.P$, $S_{GSS} = h(ID_{GSS}||S_{TTPS})$, stores $\{ID_{GSS}, PK_{GSS}, S_{GSS}\}$ parameters and sends towards GSS. As shown in Phase 1, the GSS injects $\{ID_{GSS}, PK_{GSS}, S_{GSS}\}$ credentials in its memory.

TTPS	GSS
Choose: ID_{GSS}	
Select a random number r_{GSS}	
$PK_{GSS}=r_{GSS}.P$	
Compute: $S_{GSS}=h(ID_{GSS}\|\|S_{TTS})$	
Store: $\{PK_{GSS}, S_{GSS}, ID_{GSS}\}$	
$\xrightarrow{\{ID_{GSS}, PK_{GSS}, S_{GSS}\}}$	
	Store: $\{ID_{GSS}, PK_{GSS}, S_{GSS}\}$

PHASE 1. GSS registration phase.

C. MD REGISTRATION

The TTPS chooses an identity for the mobile device ID_{MD}, selects a random number r_{MD}, computes $PK_{MD} = r_{MD}.P$, $S_{MD} = h(ID_{MD}||S_{TTPS})$, and stores $\{ID_{MD}, PK_{MD}, S_{MD}\}$ in its memory and sends $\{S_{MD}\}$ towards the MD where it can also store $\{ID_{MD}, PK_{MD}, S_{MD}\}$ credentials for future usage, as shown in phase 2.

TTPS	MD
Choose: ID_{MD}	
Select a random number r_{MD}	
Compute: $PK_{MD}=r_{MD}.P$	
$S_{MD}=h(ID_{MD}\|\|S_{TTS})$	
Store: $\{S_{MD}, ID_{MD}\}$	
$\xrightarrow{\{ID_{MD}, PK_{MD}, S_{MD}\}}$	
	Store: $\{ID_{MD}, PK_{MD}, S_{MD}\}$

PHASE 2. MD registration phase.

D. DRONE REGISTRATION

A legitimate operator selects an identity ID_D, password PW_D, imprints biometrics B and selects a random number r_D for a drone (D), computes $PK_D = r_D.P$, Gen(B)= (σ_D, β_D), $HID_D = h(ID_D||\sigma_D)$, $HPW_D = h(PW_D||\sigma_D)$, and sends $\{PK_D, ID_{MD}, HID_D, HPW_D\}$ towards TTPS over a secure channel. Upon receiving $\{PK_D, ID_{MD}, HID_D, HPW_D\}$ message from a drone (D) through a private channel, the TTPS computes $Z_1 = h(HID_D||HPW_D)$, $Z_2 = h(HID_D||ID_{MD})$, and $Z_3 = Z_2 \oplus Z_1$ and sends $\{Z_3, PK_D\}$ back towards the drone (D). The drone (D), when receiving the $\{Z_3, PK_D\}$ message, computes $HPID_D = h(HID_D||PW_D||\sigma_D)$, $Z_4 = h(HID_D||HPID_D||\sigma_D)$, and stores $\{PK_D, Z_3, Z_4, h(.)\}$, as shown in phase 3.

Drone (D)	TTPS
Choose ID_D, PW_D, and imprint B	
Select a random number r_D	
Compute: $PK_D=r_D.P$	
$Gen(B)=(\sigma_D, \beta_D)$	
$HID_D=h(ID_D\|\|\sigma_D)$	
$HPW_D=h(PW_D\|\|\sigma_D)$	
$\xrightarrow{\{PK_D, ID_{MD}, HID_D, HPW_D\}}$	
	Compute: $Z_1=h(HID_D\|\|HPW_D)$
	$Z_2=h(HID_D\|\|ID_{MD})$
	$Z_3=Z_2 \oplus Z_1$
$\xleftarrow{\{Z_3, PK_D\}}$	
Compute: $HPID_D=h(HID_D\|\|PW_D\|\|\sigma_D)$	
$Z_4=h(HID_D\|\|HPID_D\|\|\sigma_D)$	
Store: $\{PK_D, Z_3, Z_4, h(.)\}$	

PHASE 3. Drone (D) registration phase.

E. MUTUAL AUTHENTICATION

This phase of the protocol is accomplished in the following steps:

Step 1: The user provides identity ID_D^*, PW_D^* and imprints biometric B^* into a drone (D). The drone (D) revokes $Rep(B^*, \beta_D) = \sigma_D^*$, $HID_D^* = h(ID_D^*||\sigma_D^*)$, $HPID_D^* = h(HID_D^*||PW_D^*||\sigma_D^*)$, $Z_4^* = h(HID_D^*||HPID_D^*||\sigma_D^*)$ and confirms Z_4^* ?= Z_4, if matched, extracts nonce $\mathrm{N_D}$ calculates $\mathrm{HPD_D} = \mathrm{h}(\mathrm{PW_D}||\sigma_{\mathrm{D}})$, $\mathrm{Z}_1 = \mathrm{h}(\mathrm{HID_D}||\mathrm{HPW_D})$, and $\mathrm{Z}_2 = \mathrm{Z}_3 \oplus \mathrm{Z}_1$, $\mathrm{Z}_5 = \mathrm{h}(\mathrm{HID_D}||\mathrm{N_D}||\mathrm{r_D}||\mathrm{T}_1)$, $\mathrm{Z}_6 =(\mathrm{Z}_2||\mathrm{HID_D}||\mathrm{ID_D}||) \oplus \mathrm{h}(\mathrm{Pk_D}||\mathrm{T}_1)$, $\mathrm{Z}_7 = \mathrm{h}(\mathrm{Z}_2||\mathrm{PK_D}||\mathrm{PK_{MD}}||\mathrm{HID_D}||\mathrm{ID_{MD}})$ and transmits $\{\mathrm{Z}_6, \mathrm{Z}_7, \mathrm{PK_D}, \mathrm{T}_1\}$ towards the GSS over an open channel.

Step 2: The GSS checks the timestamp with its current system time, T_1-$\mathrm{T}_2 \leq \Delta\mathrm{T}$, determines $(\mathrm{Z}_2||\mathrm{HID_D}||\mathrm{ID_D}||) = \mathrm{Z}_6 \oplus \mathrm{h}(\mathrm{PK_D}||\mathrm{T}_1)$, computes $\mathrm{Z}_7^* =(\mathrm{Z}_2||\mathrm{PK_D^*}||\mathrm{PK_{MD}}||\mathrm{HID_D}||\mathrm{ID_{MD}})$ and verifies Z_7^* ?= Z_7. If found correct, calculates $\mathrm{Z}_8 = \mathrm{h}(\mathrm{ID_{GSS}}||\mathrm{ID_{MD}}||\mathrm{PK_D}||\mathrm{PK_{GSS}}||\mathrm{T}_3)$, $\mathrm{Z}_9 = \mathrm{h}(\mathrm{PK_{GSS}}||\mathrm{r_{MD}}||\mathrm{ID_{GSS}}||\mathrm{T}_3)$ and sends $\{\mathrm{Z}_9, \mathrm{PK_D}, \mathrm{PK_{GSS}}, \mathrm{T}_3\}$ towards the MD over an open channel.

Step 3: The MD checks the timestamp with its current time, T_3-$\mathrm{T}_4 \leq \Delta\mathrm{T}$, determines $\mathrm{Z}_8^* = \mathrm{h}(\mathrm{ID_{GSS}}||\mathrm{ID_{MD}}||\mathrm{PK_D}||\mathrm{PK_{GSS}}||\mathrm{T}_3)$, matches Z_8^* ?= Z_8, if found valid, computes $\mathrm{Z}_{10} = \mathrm{h}(\mathrm{ID_{MD}}||\mathrm{PK_{MD}}||\mathrm{r_{MD}}||\mathrm{T}_3)$, $\mathrm{SK_{MD}} = \mathrm{h}(\mathrm{PK_D}||\mathrm{PK_{GSS}}||\mathrm{PK_{MD}}||\mathrm{T}_5)$, $\mathrm{Z}_{11} = \mathrm{h}(\mathrm{SK_{MD}}||\mathrm{PK_D}||\mathrm{T}_5)$ and transmits $\{\mathrm{PK_{GSS}}, \mathrm{Z}_{11}, \mathrm{T}_5\}$ back towards GSS over a public channel.

Step 4: The GSS again checks the timestamp with its current system time, T_6-$\mathrm{T}_5 \leq \Delta\mathrm{T}$, determines $\mathrm{PK_{GSS}}$, computes $\mathrm{SK_{GSS}} = \mathrm{h}(\mathrm{PK_D}||\mathrm{PK_{GSS}}||\mathrm{PK_{MD}}||\mathrm{T}_5)$, $\mathrm{Z}_{11}^* = \mathrm{h}(\mathrm{SK_{GSS}}||\mathrm{PK_{GSS}}||\mathrm{T}_5)$, and sends $\{\mathrm{PK_{GSS}}, \mathrm{Z}_{11}^*, \mathrm{T}_5, \mathrm{T}_7\}$ towards the drone (D) over a public network channel.

Step 5: Upon receiving the $\{\mathrm{PK_{GSS}}, \mathrm{Z}_{11}^*, \mathrm{T}_5, \mathrm{T}_7\}$ message, the drone (D) checks the timestamp with its current system time, T_8-$\mathrm{T}_7 \leq \Delta\mathrm{T}$, computes $\mathrm{SK_{GSS}} = \mathrm{h}(\mathrm{PK_D}||\mathrm{PK_{GSS}^*}||\mathrm{PK_{MD}}||\mathrm{T}_5)$ and $\mathrm{Z}_{11}^* = \mathrm{h}(\mathrm{SK_{MD}}||\mathrm{PK_D}||\mathrm{T}_5)$, confirms Z_{11}^* ?= Z_{11}, and calculates $\mathrm{SK_D} = \mathrm{h}(\mathrm{PK_D}||\mathrm{PK_{GSS}}||\mathrm{PK_{MD}}||\mathrm{T}_7)$. Finally, all three participants mutually authenticate each other. $\mathrm{SK_{MD}} = \mathrm{SK_{GSS}} = \mathrm{SK_D}$.

F. PASSWORD/BIOMETRIC UPDATE PHASE

If a legitimate operator desires to change the password and biometrics for which they operate the drone system, the proposed protocol provides the facility of changing it freely and securely. In this regard, the legitimate operator selects their previous identity $\mathrm{ID_D}$, password $\mathrm{PW_D}$, and imprint B for a drone (D). The drone computes $\mathrm{PK_D^*} = \mathrm{r_D.P}$, $\mathrm{Gen(B)}= (\alpha_{\mathrm{D}}, \beta_{\mathrm{D}})$, $\mathrm{HID_D^*} = \mathrm{h}(\mathrm{ID_D}||\alpha_{\mathrm{D}})$, $\mathrm{HPW_D^*} = \mathrm{h}(\mathrm{PW_D}||\alpha_{\mathrm{D}})$ and locally generate these parameters $\mathrm{ID_D}$, $\mathrm{HID_D^*}$, $\mathrm{HPW_D^*}$. The drone further computes $\mathrm{Z}_1^* = \mathrm{h}(\mathrm{HID_D^*}||\mathrm{HPW_D^*})$, $\mathrm{Z}_2^* = \mathrm{h}(\mathrm{HID_D^*}||\mathrm{ID_D^*})$, $\mathrm{Z}_3^* = \mathrm{Z}_2^* \oplus \mathrm{Z}_1^*$ and will be asked the operator to enter a new password $\mathrm{PW_D^{new}}$ and biometric $\mathrm{B^{new}}$ and computes: $\mathrm{HPID_D^*} = \mathrm{h}(\mathrm{ID_D^{new}}||\mathrm{PW_0^{new}}||\alpha_{\mathrm{D}}^*)$, $\mathrm{Z}_4^* = \mathrm{h}(\mathrm{HID_D^*}||\mathrm{HPID_D^*}||\alpha_{\mathrm{D}}^*)$ and replaces $\{\mathrm{Z}_3, \mathrm{Z}_4, \mathrm{PK_D}, \mathrm{h}(.)\}$ with $\{\mathrm{Z}_3^*, \mathrm{Z}_4^*, \mathrm{PK_D^*}, \mathrm{h}(.)\}$, shown in phase 4.

V. SECURITY ANALYSIS

In this section, we first analyze the security of the proposed security mechanism through a well-known technique, namely ROM analysis [16], [17] and then simulate it using a programming verification toolkit ProVerif [14]. We then discuss the different attacks for the proposed security mechanism. These are discussed one by one as follows:

A. ROM ANALYSIS

In this section, we analyze the proposed protocol's security using ROM [16], [17], which shows that an adversary cannot extract the SK between the drone, ground station server (GSS), and mobile device (MD). While using ROM, we first use semantic analysis and then the security of the SK. In this regard, the adversary executes different queries for cracking the session secret key. The adversary also checks the hash codes of our scheme for possible collision. These analyses are modelled as follows:

Suppose $\prod_D^{b_1}$ and $\prod_{GSS}^{b_2}$ are the instances of the drone (D) and GSS, which are called random oracle instances and are given as follows:

Execute$\left(\prod_D^{b_1}, \prod_{GSS}^{b_1}\right)$***:*** The adversary eavesdrops on the shared message between the D and GSS in this query.

Corrupt$(\prod^{b_1})$***:*** In this query, the adversary steals the stored parameters from the memory of the D.

Reveal$(\prod^{b})$***:*** In this query, the adversary reveals the session secret key between the GSS and D.

Test$(\prod^{b_1})$***:*** In this query, the adversary checks the originality of the session secret key by flipping a coin: 1 means the adversary has won, and 0 represents the adversary has lost.

Freshness: Suppose $\prod_D^{b_1}$ and $\prod_{GSS}^{b_2}$ are the instances of drone, and the adversary cannot determine the secret SK at any stage; then $\prod_D^{b_1}$ and $\prod_{GSS}^{b_2}$ instances are said to be fresh, and the adversary in the Reveal can recognize this feature (.) query stated above.

Semantic Security: Suppose the output of a hash oracle is $q^2_{\frac{h(.)}{2^{h(.)}}}$, $q^2_{\frac{h(.)}{2^{h(.)+1}}}$, and $q^2_{\frac{h(.)+1}{2^{h(.)+1}}}$, then the hash-code collision probability output will be $\frac{(q_s+q_r)^2}{2(q-1)}$ and the success chances with the adversary can mathematically be represented as follows:

$$\frac{|P|\,S_2 - P\,|S_1| + q^2_{h(.)} + q^2_{h1(.)} + q^2_{h2(.)}}{q^2_{h(.)} + 1} + \frac{(q_s + q_r)^2}{2(q-1)}$$

$$|P|\,S_3 - P|S_2| \leq \frac{2q_s + 2q_{h1(.)}}{2^{h(.)}}$$

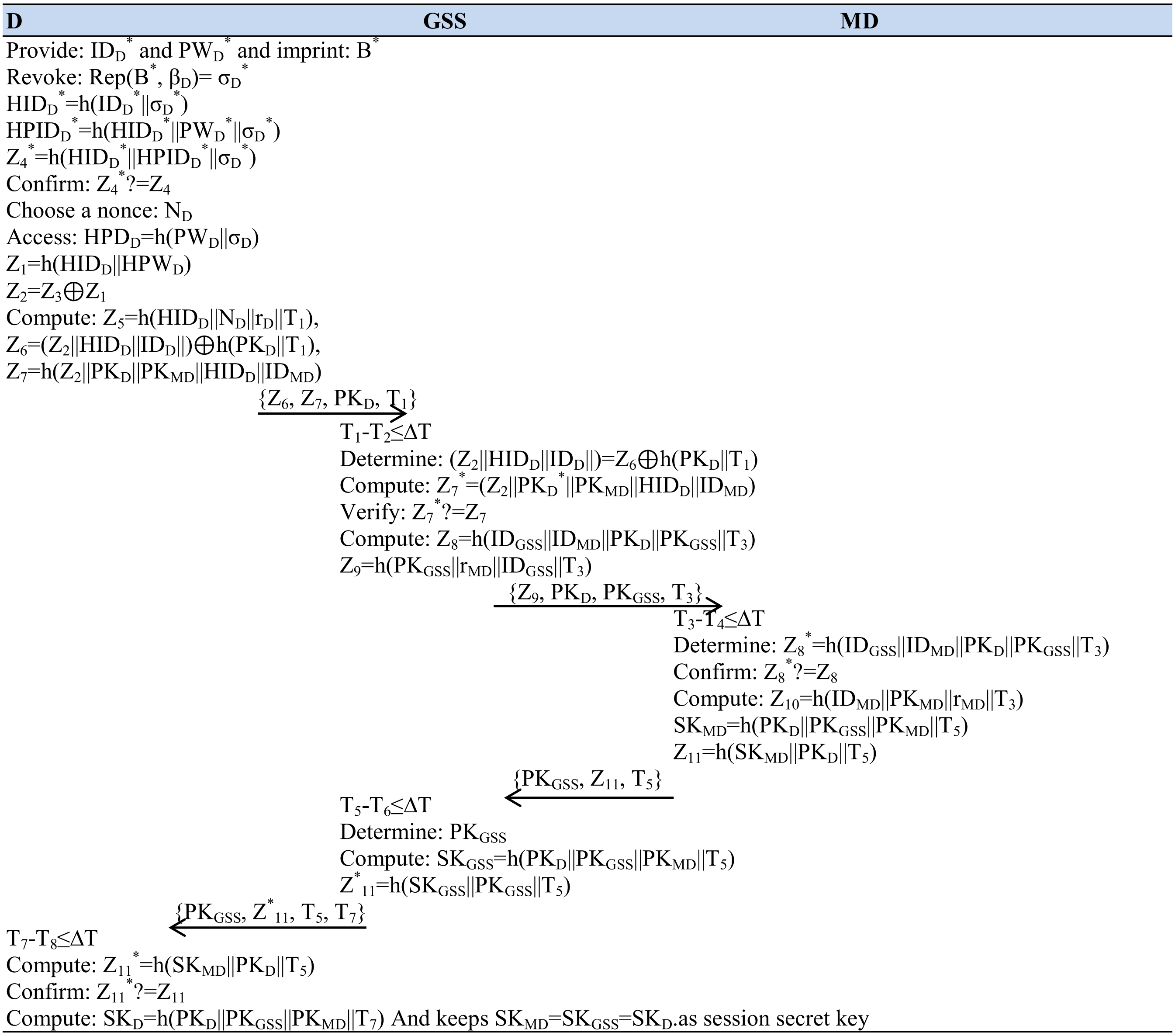
$$|P|\,S_1 - P\,|S_2| \leq q_r.\,(ADV)_A^{poly}\,(Key)$$

The key is any random number that the adversary considers the SK, and it belongs to a random numbers dictionary DC available with the adversary. The maximum probability with A is $\frac{1}{DC}$, which is represented as follows:

$$\leq P\,|S_3| \leq \frac{1}{2} + Max\left\{\frac{q_{h1(.)}}{2^{h(.)}}, \frac{q_s}{|DC|}\right\}$$

$$(ADV)_A^P \leq P\,|S_0| - 1$$

$$\leq 2\left(|P|\,S_0 - P\,|S_4| + Max\left\{\frac{q_{h1(.)}}{2^{h(.)}}, \frac{q_s}{|DC|}\right\}\right)$$



D | GSS | MD

Provide: ID_D^* and PW_D^* and imprint: B^*

Revoke: $Rep(B^*, \beta_D)= \sigma_D^*$

$HID_D^*=h(ID_D^*||\sigma_D^*)$

$HPID_D^*=h(HID_D^*||PW_D^*||\sigma_D^*)$

$Z_4^*=h(HID_D^*||HPID_D^*||\sigma_D^*)$

Confirm: $Z_4^*?=Z_4$

Choose a nonce: N_D

Access: $HPD_D=h(PW_D||\sigma_D)$

$Z_1=h(HID_D||HPW_D)$

$Z_2=Z_3\oplus Z_1$

Compute: $Z_5=h(HID_D||N_D||r_D||T_1)$,

$Z_6=(Z_2||HID_D||ID_D||)\oplus h(PK_D||T_1)$,

$Z_7=h(Z_2||PK_D||PK_{MD}||HID_D||ID_{MD})$

$\{Z_6, Z_7, PK_D, T_1\}$ →

$T_1\text{-}T_2\le\Delta T$

Determine: $(Z_2||HID_D||ID_D||)=Z_6\oplus h(PK_D||T_1)$

Compute: $Z_7^*=(Z_2||PK_D^*||PK_{MD}||HID_D||ID_{MD})$

Verify: $Z_7^*?=Z_7$

Compute: $Z_8=h(ID_{GSS}||ID_{MD}||PK_D||PK_{GSS}||T_3)$

$Z_9=h(PK_{GSS}||r_{MD}||ID_{GSS}||T_3)$

$\{Z_9, PK_D, PK_{GSS}, T_3\}$ →

$T_3\text{-}T_4\le\Delta T$

Determine: $Z_8^*=h(ID_{GSS}||ID_{MD}||PK_D||PK_{GSS}||T_3)$

Confirm: $Z_8^*?=Z_8$

Compute: $Z_{10}=h(ID_{MD}||PK_{MD}||r_{MD}||T_3)$

$SK_{MD}=h(PK_D||PK_{GSS}||PK_{MD}||T_5)$

$Z_{11}=h(SK_{MD}||PK_D||T_5)$

← $\{PK_{GSS}, Z_{11}, T_5\}$

$T_5\text{-}T_6\le\Delta T$

Determine: PK_{GSS}

Compute: $SK_{GSS}=h(PK_D||PK_{GSS}||PK_{MD}||T_5)$

$Z^*_{11}=h(SK_{GSS}||PK_{GSS}||T_5)$

← $\{PK_{GSS}, Z^*_{11}, T_5, T_7\}$

$T_7\text{-}T_8\le\Delta T$

Compute: $Z_{11}^*=h(SK_{MD}||PK_D||T_5)$

Confirm: $Z_{11}^*?=Z_{11}$

Compute: $SK_D=h(PK_D||PK_{GSS}||PK_{MD}||T_7)$ And keeps $SK_{MD}=SK_{GSS}=SK_D$.as session secret key

PHASE 4. **Mutual authentication phase.**

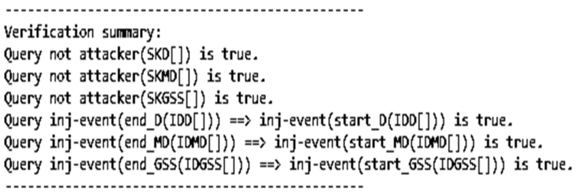
Combine all the above equations:

$$\le 2\left(|\{P|S_1| - P|S_2|\} + \{P|S_3| - P|S_4|\}| + Max\left\{\frac{q_{h1(.)}}{2^{h(.)}}, \frac{q_s}{|DC|}\right\}\right)$$

$$\le \frac{q_{h(.)}^2 + q_{h1(.)}^2 + q_{h2(.)}^2}{2^{h(.)}} + \frac{(q_s+q_r)^2}{2(q-1)} + 2q_r.(ADV)_A^{poly}(Key) + 2Max\left\{\frac{q_{h1(.)}}{2^{h(.)}}, \frac{q_s}{|DC|}\right\}$$

B. PROVERIF SIMULATION

To check the key secrecy, integrity, authorization, and reachability, we have simulated the protocol using a well-known software toolkit, ProVerif [14]. The result generated, as shown in Figure 2 below, demonstrated that the attacker cannot, at any stage, crack/hack the session secret key. Also, the confidentiality, authorization, and reachability of the secret SKs are verified, and each participant is reached without being cracked/hacked by anyone.



```
--------------------------------------------------
Verification summary:
Query not attacker(SKD[]) is true.
Query not attacker(SKMD[]) is true.
Query not attacker(SKGSS[]) is true.
Query inj-event(end_D(IDD[])) ==> inj-event(start_D(IDD[])) is true.
Query inj-event(end_MD(IDMD[])) ==> inj-event(start_MD(IDMD[])) is true.
Query inj-event(end_GSS(IDGSS[])) ==> inj-event(start_GSS(IDGSS[])) is true.
--------------------------------------------------
```

FIGURE 2. **ProVerif verification result.**

C. INFORMAL SECURITY ANALYSIS

In this sub-section, we pragmatically prove the proposed protocol's security via different attack analyses:

Proposition 1: The proposed protocol is secure against traceability attacks

Proof: Due to the random extraction of nonce for the GCS N_{GCS} and drone (d) N_D and the exchange of each message on the specified time threshold, no one can trace a drone at any location in the fly zone.

Proposition 2: The proposed protocol can resist DoS attacks

Proof: We have used MD5, biometrics fuzzy extractor and other cryptographic algorithms, and these are confirmed in both participants before going for further processing; similarly, in each round trip of the protocol, there are numerous checks, which show a strong resistance of the protocol against DoS attacks.

Proposition 3: The proposed protocol is strong against insider threats

Proof: We have used MD5 and bit-wise XOR operation that guarantees the security of stored credentials in the TTPS and GSS. If an adversary runs an insider threat program, they cannot sabotage, discover, or espionage any hurdle to the system due to accomplishing the registration via a secure channel. The TTPS is placed offline and cannot allow anyone to act as an insider.

Proposition 4: The proposed protocol can resist stolen verifier attacks

Proof: Due to no storage table, the SK being in a non-readable format, and changing the nonce for each session, we guarantee that the proposed protocol resists stolen verifier attacks. Similarly, suppose someone takes down/crashes or captures a drone and tries to identify sensitive credentials like identity, secret keys, or any other parameter from the stored values in a drone's memory. In that case, they cannot succeed due to the availability of all secret credentials (identity, keys, nonce, random numbers) in cypher (hidden) format and the presence of 160-bit keys; therefore, the proposed protocol strongly resists stolen verifier attacks.

Proposition 5: The proposed scenario is not vulnerable to replay attacks

Proof: Due to recording the time at each round trip, extracting random nonce, and numerous checks, the proposed protocol is safe against replay attacks. If, for example, an adversary captures a message from the public network channel and replays it some other time, they cannot launch a replay or get anything from the system due to the characteristics mentioned above in the proposed protocol; therefore, our strategy is safe against replay attacks.

Proposition 6: The proposed scenario resists MITM attacks

Proof: If a malicious deed tries to modify, delete, or divert any message from the public network channel, it cannot succeed due to not knowing anything about the different identities (i.e., ID_{GSS}, ID_D, and ID_{MD}) and other stored credentials. The dynamicity of each message guarantees that the protocol is safe against MIMT attacks.

Proposition 7: The proposed protocol has not detected a desynchronization attack.

Proof: In the proposed authentication protocol, ground station server stores $\{S_{GSS}\}$, mobile device stores $\{S_{MD}\}$ and drone stores $\{Z_3, Z_4, P, h\}$, if an attacker wants to disturb the synchrony of the shared secrets, they have to enter the trusted third party server (TTPS) which is one of the trusted entity in the whole system. Registration is performed with TTPS through a secure channel and then placed in offline mode. So, the adversary cannot, at any stage, enter the TTPS and change the shared secret in drones, GSS, and mobile devices.

Every authentication cycle has a distinct value carefully verified at both ends. Drone data is sent to GSS with a big random integer, and vice versa. If the drone's value in the GSS doesn't match, it should be viewed as an attack, which stops further exchange of credentials. For instance, if an attacker modifies a message's parameters, the GSS can quickly identify this as a tempering of the message and reject it. The authenticating parties fail for single-running session authentication if an adversary stops a transmission, but the adversary does not alter any parameters both peers hold. The mobile user is permitted to communicate securely in advance. As a result, the proposed scheme is safe against a desynchronization attack.

Proposition 8: The proposed scheme resists side-channel attacks.

Proof: Overall, the security technique proposed here in this article relies less on key numbers, evaluates the key attributes at different stages with strength, and generates a unique secret session key for every session, causing the order of moves to change for each subsequent session. Similarly, the presented security technique effectively resists a side-channel attack since timestamps are available during each protocol round trip and distinct random integers are sent for each session.

VI. PERFORMANCE AND COMPARATIVE ANALYSIS

In this article section, we will evaluate the performance metrics by considering communication and computation costs and then analyze the proposed protocol comparatively with prior works. These are given as under:

A. COMMUNICATION COSTS ANALYSIS

The messages exchanged between the D, GSS, and MD in the key agreement phase of the protocol are counted as the protocol's communication costs. Looking into the literature [42], MD5 is 128-bit, the timestamp is 32, and the key size is 160 bits. The communication costs of the proposed protocol are shown in Table 3 and diagrammatically represented in Figure 3.

TABLE 3. Communication costs analysis.

Participant	Message Exchanged	Values	Total
D→GSS	$\{Z_6, Z_7, PK_D, T_1\}$	(128x2)+160+32	448
GSS→MD	$\{Z_8, Z_9, PK_D, PK_{GSS}, T_3\}$	(128x2)+(160x2)+32	608
MD→GSS	$\{PK_{GSS}, Z_{11}, T_5\}$	160+128+32	320
GSS→D	$\{PK_{GSS}, Z^*_{11}, T_5, T_7\}$	160+128+(32x2)	352
		Communication Costs in bits	**1728**

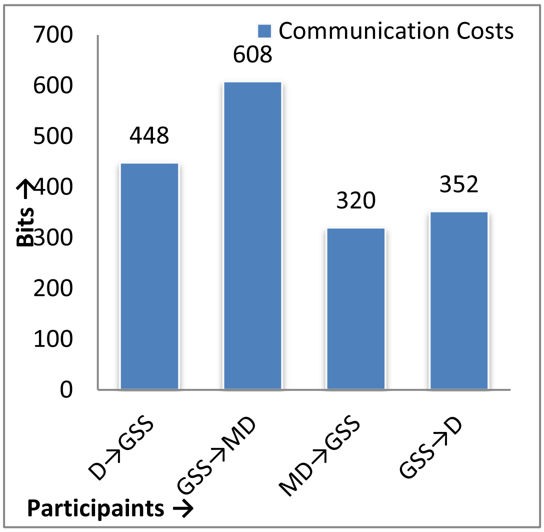


FIGURE 3. Communication costs.

B. COMPUTATION COSTS ANALYSIS

We count the computation costs for hash cryptographic functions, the time taken by the CPU for extracting random numbers, and XOR operations. Computation costs for a security mechanism are only considered during the SK establishment (Mutual Authentication) phase, as the registration phase is accomplished in offline mode. Suppose $T_h(.)$ represents the time taken by the CPU for the one-way hash(.) cryptographic function, which is 0.0046 ms; $T_{Enc(.)/Dc}(.)$ represents the time for generation and replication functions, which is 3.8500 ms; T_{XOR} is the time of XOR operation, which is negligibly equal to zero; and T_N means time taken by CPU for extracting random nonce and its value is 0.539 ms. According to [42], the execution time for the different millisecond operations is shown in Table 4 and graphically in Figure 4.

TABLE 4. Computation coasts analysis.

Participants	Phase	Operations	Cots
TTPS	Registration	$4T_{h(.)}+0T_{G(.)/R(.)}+1T_{XOR}+0T_N$	0.0184ms
GSS		$6T_{h(.)}+0T_{G(.)/R(.)}+1T_{XOR}+0T_N$	0.036ms
MD	Authentication	$4T_{h(.)}+0T_{G(.)/R(.)}+0T_{XOR}+0T_N$	0.0184ms
D		$9T_{h(.)}+1T_{G(.)/R(.)}+1T_{XOR}+1T_N$	4.431ms
		Total Costs in Milliseconds	**4.504ms**

C. COMPARATIVE ANALYSIS

Here we compare the proposed protocol with state-of-the-art work regarding communication and computation costs. The results are shown in Table 5 and diagrammatically plotted in Figure 5.

TABLE 5. Comparison analysis.

Metrics	[35]	[38]	[40]	Proposed
Communication Costs	2336 Bits	2048 Bits	2560 Bits	1728Bits
Computation Costs	54.292 ms	21.08 ms	5.114 ms	4.504 ms

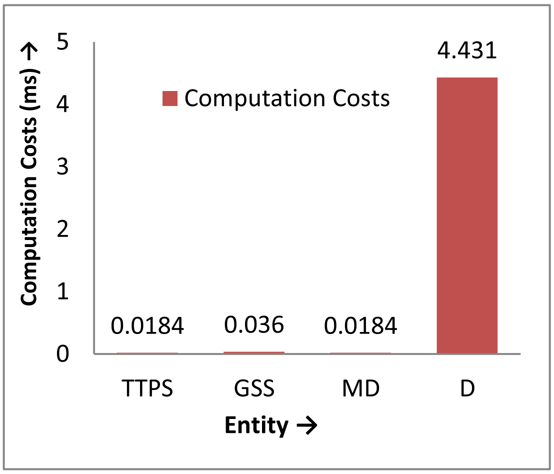


FIGURE 4. Computation costs.

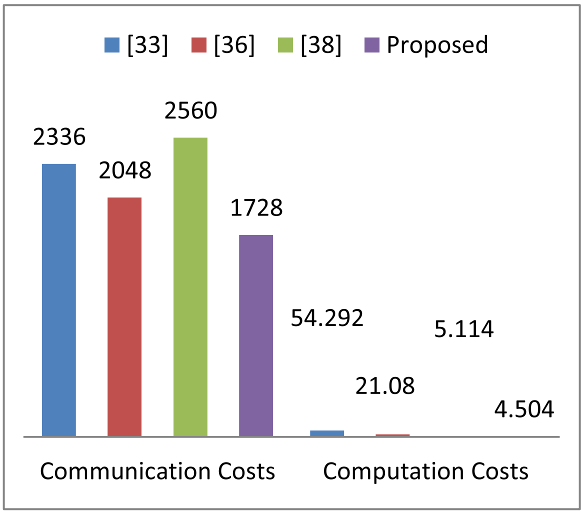


FIGURE 5. Comparative analysis.

The proposed scheme is 26.02% better in communication costs than [35], 15.62% from [38] and 32.5% from [40], while in terms of computation costs, the proposed scheme is 91.70% better than [35], 78.63% than [38] and 11.92% than [40]. Overall, the proposed protocol outperforms better than its competitors, as shown in Table 6.

TABLE 6. Percentage improvement.

Performance Metrics	[35]	[38]	[40]
% age improvement in Communication Costs	26.02%	15.62%	32.5%
% age improvement in Computation Costs	91.70%	78.63%	11.92%

Similarly, upon comparing the proposed scheme with [35], [38], and [40], in terms of security functionalities including I-Impersonation Attack, II-MITM Attack, III-Attack detection, IV-Forward Secrecy, V-Backward Secrecy, VI-Mutual Authentication, VII-Traceability Attack, VIII-Insider Attack, IX-Stolen-Verifier Attack, X-Password Guessing Attack, XI-DoS Attack, and XII-Replay Attack, ✓-Supported and

X–Not Supported. The results show that our scheme/protocol provides maximum security, as shown in Table 7.

TABLE 7. Security functionalities comparison analysis.

Security Functionalities	[35]	[38]	[40]	Proposed
I-Impersonation Attack	✓	✓	×	×
II-Man-in-the-Middle Attack	×	✓	×	×
III-Attack detection	✓	×	×	×
IV-Forward Secrecy	×	×	✓	✓
V-Backward Secrecy	×	×	✓	✓
VI-Mutual Authentication	×	✓	×	✓
VII-Traceability Attack	✓	✓	×	×
VIII-Insider Attack	×	×	×	×
IX-Stolen-Verifier Attack	×		✓	×
X-Password Guessing Attack	×	×	✓	×
XI-DoS Attack	×	×	×	×
XII-Replay Attack	✓	×	×	×

VII. CONCLUSION

We presented a scheme for ensuring the communication security of D, MD, and GSS working in IoD. We have formally analyzed the security through a well-known technique, ROM analysis and ProVerif simulation, and informally through propositions. We measured the performance metrics by counting communication and computation costs. The result shows that the scheme is lightweight and robust and can be recommended for practical implementation in IoD, as it will improve the logistical infrastructure because drone technology is a crucial enhancer of existing transport systems. Most importantly, if our security scheme is installed in reconnaissance and attacking drones, it could be used in traffic, damage investigation after earthquakes or floods, forest fire monitoring, troop movements, and other strategic activities.

REFERENCES

[1] Y. Kawamoto, H. Nishiyama, N. Kato, F. Ono, and R. Miura, "Toward future unmanned aerial vehicle networks: Architecture, resource allocation and field experiments," *IEEE Wireless Commun.*, vol. 26, no. 1, pp. 94–99, Feb. 2019.

[2] I. Jawhar, N. Mohamed, J. Al-Jaroodi, D. P. Agrawal, and S. Zhang, "Communication and networking of UAV-based systems: Classification and associated architectures," *J. Netw. Comput. Appl.*, vol. 84, pp. 93–108, Apr. 2017.

[3] J. Sun, W. Wang, L. Kou, Y. Lin, L. Zhang, Q. Da, and L. Chen, "A data authentication scheme for UAV ad hoc network communication," *J. Supercomput.*, vol. 76, no. 6, pp. 4041–4056, Jun. 2020.

[4] J. H. Sarker and A. M. Nahhas, "A secure wireless mission critical networking system for unmanned aerial vehicle communications," *Telecommun. Syst.*, vol. 69, no. 2, pp. 237–251, Oct. 2018.

[5] X. Liang, G. Meng, Y. Xu, and H. Luo, "A geometrical path planning method for unmanned aerial vehicle in 2D/3D complex environment," *Intell. Service Robot.*, vol. 11, no. 3, pp. 301–312, Jul. 2018.

[6] S. U. Jan and H. U. Khan, "Identity and aggregate signature-based authentication protocol for IoD deployment military drone," *IEEE Access*, vol. 9, pp. 130247–130263, 2021.

[7] J. Cui, Y. Chen, H. Zhong, D. He, L. Wei, I. Bolodurina, and L. Liu, "Lightweight encryption and authentication for controller area network of autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 72, no. 11, pp. 14756–14770, Nov. 2023.

[8] S. U. Jan, I. A. Abbasi, F. Algarni, and A. S. Khan, "A verifiably secure ECC based authentication scheme for securing IoD using FANET," *IEEE Access*, vol. 10, pp. 95321–95343, 2022.

[9] S. Itoo, A. A. Khan, M. Ahmad, and M. J. Idrisi, "A secure and privacy-preserving lightweight authentication and key exchange algorithm for smart agriculture monitoring system," *IEEE Access*, vol. 11, pp. 56875–56890, 2023.

[10] S. Hussain, M. Farooq, B. A. Alzahrani, A. Albeshri, K. Alsubhi, and S. A. Chaudhry, "An efficient and reliable user access protocol for Internet of Drones," *IEEE Access*, vol. 11, pp. 59688–59700, 2023.

[11] R. Rivest, "The MD5 message-digest algorithm," Tech. Rep., RFC1321, 1992.

[12] F. Swiderski and W. Snyder, *Threat Modeling*. Microsoft Press, 2004.

[13] Q. Do, B. Martini, and K.-K.-R. Choo, "The role of the adversary model in applied security research," *Comput. Secur.*, vol. 81, pp. 156–181, Mar. 2019.

[14] B. Blanchet, B. Smyth, V. Cheval, and M. Sylvestre, "ProVerif 2.00: Automatic cryptographic protocol verifier, user manual and tutorial," Tech. Rep., 2018.

[15] X. Boyen, "Reusable cryptographic fuzzy extractors," in *Proc. 11th ACM Conf. Comput. Commun. Secur.*, Oct. 2004, pp. 82–91.

[16] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Comput. Commun. Secur.*, 1993, pp. 62–73.

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

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

[19] M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment," *Ad Hoc Netw.*, vol. 36, pp. 152–176, Jan. 2016.

[20] S. Challa, M. Wazid, A. Kumar Das, N. Kumar, A. Goutham Reddy, E.-J. Yoon, and K.-Y. Yoo, "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[21] M. Wazid, A. K. Das, and S. Shetty, "TACAS-IoT: Trust aggregation certificate-based authentication scheme for edge-enabled IoT systems," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22643–22656, Nov. 2022.

[22] 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.

[23] W. Hong, L. Jianhua, L. Chengzhe, and W. Zhe, "A provably secure aggregate authentication scheme for unmanned aerial vehicle cluster networks," *Peer-Peer Netw. Appl.*, vol. 13, no. 1, pp. 53–63, Jan. 2020.

[24] S. Benzarti, B. Triki, and O. Korbaa, "Privacy preservation and drone authentication using id-based signcryption," in *SoMeT*, 2018, pp. 226–239.

[25] M. S. Haque and M. U. Chowdhury, "A new cyber security framework towards secure data communication for unmanned aerial vehicle (UAV)," in *Security and Privacy in Communication Networks*. Springer, 2018, pp. 113–122.

[26] J. Won, S.-H. Seo, and E. Bertino, "Certificateless cryptographic protocols for efficient drone-based smart city applications," *IEEE Access*, vol. 5, pp. 3721–3749, 2017.

[27] 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.

[28] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, and C.-M. Wu, "A traceable and privacy-preserving authentication for UAV communication control system," *Electronics*, vol. 9, no. 1, p. 62, Jan. 2020.

[29] 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.

[30] G. Cho, J. Cho, S. Hyun, and H. Kim, "SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles," *Appl. Sci.*, vol. 10, no. 9, p. 3149, Apr. 2020.

[31] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Inf. Sci.*, vol. 476, pp. 211–221, Feb. 2019.

[32] M. Tanveer, A. H. Zahid, M. Ahmad, A. Baz, and H. Alhakami, "LAKE-IoD: Lightweight authenticated key exchange protocol for the Internet of Drone environment," *IEEE Access*, vol. 8, pp. 155645–155659, 2020.

[33] C. Pu and Y. Li, "Lightweight authentication protocol for unmanned aerial vehicles using physical unclonable function and chaotic system," in *Proc. IEEE Int. Symp. Local Metrop. Area Netw. (LANMAN*, Jul. 2020, pp. 1–6.

[34] T. Alladi, V. Chamola, and N. Kumar, "PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks," *Comput. Commun.*, vol. 160, pp. 81–90, Jul. 2020.

[35] 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, May 2021, Art. no. 101955.

[36] M. O. Ozmen and A. A. Yavuz, "Dronecrypt—An efficient cryptographic framework for small aerial drones," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Oct. 2018, pp. 1–6.

[37] Y. Li, X. Du, and S. Zhou, "A lightweight identity authentication scheme for UAV and road base stations," in *Proc. Int. Conf. Cyberspace Innov. Adv. Technol.*, Dec. 2020, pp. 54–58.

[38] J. Singh, A. Gimekar, and S. Venkatesan, "An efficient lightweight authentication scheme for human-centered industrial Internet of Things," *Int. J. Commun. Syst.*, vol. 36, no. 12, p. e4189, Aug. 2023.

[39] 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.

[40] 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.

[41] P. Gope, O. Millwood, and N. Saxena, "A provably secure authentication scheme for RFID-enabled UAV applications," *Comput. Commun.*, vol. 166, pp. 19–25, Jan. 2021.

[42] M. Tanveer, A. Alkhayyat, A. U. Khan, N. Kumar, and A. G. Alharbi, "REAP-IIoT: Resource-efficient authentication protocol for the industrial Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 23, pp. 24453–24465, Dec. 2022.

[43] N. Koblitz and A. J. Menezes, "The random Oracle model: A twenty-year retrospective," *Des., Codes Cryptogr.*, vol. 77, nos. 2–3, pp. 587–610, Dec. 2015.

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

FAHAD ALGARNI received the bachelor's degree (Hons.) from the Department of Computer Science, King Abdulaziz University, the M.I.T. degree in computer networks from La Trobe University, Melbourne, Australia, and the Ph.D. degree from the Clayton School of Information Technology, Monash University, Melbourne. He is currently the Dean of the College of Computing and Information Technology, University of Bisha, Saudi Arabia. His research interests include wireless sensor networks, cloud computing, systems, design, reliability, the IoT, and cyber security.

SAEED ULLAH JAN received the Ph.D. degree from the University of Malakand, Pakistan. He is currently an Assistant Professor in computer science with the Higher Education, Achieves and Libraries Department Government of Khyber Pakhtunkhwa, Pakistan. He is also the Principal for the newly established Government College Darora (Dir Upper)—a far-flung remote area of the province where most of the youngsters have no access to universities/institutions for Higher Education. Furthermore, he has researched many areas, including information security, cloud computing, distributed computing, privacy-preserving parallel computation, drone security and authentication, teleworking, healthcare and telemedicine system security. He has published over 30 research articles in prestigious conferences and journals and he written an introductory Book in Computer Science for beginners. The Government of Khyber Pakhtunkhwa, Pakistan, awarded him the "Best Teacher Award" for 2019–2020 out of 11000 College Teachers in 309 public sector colleges in the province.