Bio-Authenticated ECC Framework for Secure Drone-to-Drone Communication in IoD Environments

Murtaja Ali Saare[1], Mohamed Abdulrahman Abdulhamed[2], Saad Abdulhussein Abbas[3], Aseel Jasim[4] and Mahmood A. Al-Shareeda[5]

[1]*Department of Computer Science, College of Computer Science and Information, University of Basrah, 61004 Basra, Iraq*
Science Department, Faculty of Computer Science and Information Technology, University of Basra, 61004 Basra, Iraq
[3]*Department of English, College of Education-Qurna, University of Basrah, 61004 Basra, Iraq*
[4]*Department of Computer Science, Shatt Al-Arab University College, 61004 Basra, Iraq*
[5]*Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, 61004 Basra, Iraq*
murtaja.sari@uobasrah.edu.iq, mohammed@uobasrah.edu.iq, saad.abdulhussein@uobasrah.edu.iq, aseel.jasim@sa-uc.edu.iq, Mahmood.alshareedah@stu.edu.iq

Keywords: Internet of Drones (IoD), Biometric Authentication, Elliptic Curve Cryptography (ECC), Lightweight Security, Mutual Authentication, Drone Communication, Cybersecurity in UAVs.

Abstract: The Internet of Drones (IoD) has become a vital infrastructure to provide surveillance, transportation, and combat support, and therefore a compact, secure solution. This article introduces a new Bio-authenticated Elliptic Curve Cryptography Framework (ECC) that integrates biometric fuzzy extractors with ECC. The protocol removes the dependence on fixed credentials by binding authentication to unique biological features, thereby strengthening identity assurance and resistance to replay, impersonation, and stolen-verifier attacks. The process supports both sides achieving mutual authentication. Ephemeral session keys are generated without any Ground Control Station (GCS), thus providing some relief, although not enough as yet. Informal security analysis indicates that it can withstand commonly known threat vectors. Performance assessment reveals that the cost of communication and computation has been reduced by more than 28%, compared with existing ECC-based schemes. Cryptographic-biometric fusion substantially reduces storage overhead and raises resilience against insider threats as well. This privacy-preserving, lightweight protocol provides a secure solution scalable for real-world operations environments where computing resources are still very much lacking.

1 INTRODUCTION

Compared to various other historical instances of this kind of duty performed utilizing manned aircraft, the extra rapid course of Unmanned Aerial Vehicles (UAVs), along with their incorporation into the Internet of Drones (IoD) has created new possibilities [1]-[3]. Surveillance, disaster management, logistics, and environmental monitoring - these are all ripe for transformation via drones. These drones operate autonomously and interactively; they operate within dynamic but hostile environments. Therefore, communications must be both secure and lightweight: it is a fundamental precondition [4]-[6]. A major point of attention in this area is how drones can be mutually authenticated between themselves to prevent access not desired by their owners, the impersonation of being reconnoitered stealthily, or raw data being tampered with in transit [7]-[9].

Nowadays, in actual IoD scenarios, It is not always the case that old-fashioned cryptographic protocols such as PKIs or SSPs can always make the mark. Limited computational resources, Energy constraints, Dynamic topologies [10]-[12]. About all of these factors stand in their way. Worse still, existing systems typically rely on static credentials or else lack identification (for example signatures). This makes them prone to session hijacking and insider attacks [13]-[15].

In response to these challenges, the authors put forward a Bio-Authenticated ECC Framework. This scheme makes use of biometric fuzzy extractors throughout, in association with ECC. Such a hybrid approach increases the robustness of authentication through the bonding of cryptographic operations to

unique biometric characteristics. It does not rely on any central infrastructure and does not store sensitive data templates. Mutual authentication, session key generation - this proposed protocol is not only resilient against known attacks but also has great efficiency in computation, communication, and storage. The main contributions of the paper are:

- A secure action-based ID card biological information binding algorithm for drones, which uses fuzzy extractors to bind the mental traits of drones and their identities. This way we can have robust mutual authentications without relying on static passwords.
- Development of a middleware authentication model, such as Bitcoin, which is suited for the limited resource environment of the Internet of Devices, reducing costs in calculation and communication by 50% compared with existing systems.
- A thorough review of security and performance, that demonstrates non-compliance in face, replay, and insider attacks; and also demonstrable efficiency improvements.

The remainder of the article is organized as follows: In Section II, we review related work on drone authentication and biometric cryptosystems. Section III shows the system model and threat. In Section IV we present a detailed explanation of the proposed bio-authenticated ECC protocol. Section V covers the security analysis. Section VI evaluates the performance of the protocol in terms of computation, communication, and storage metrics. Section VII indicates the end of this research paper with recommendations for future work in related fields.

2 RELATED WORK

In recent years, securing communication in the Internet of Drones (IoD) has become a subject of much interest, particularly in the field of lightweight authentication protocols applicable to widely dispersed and constrained environments such as UAVs.

PUF-based schemes (e.g., Chandran et al. [16]; Zhang et al., [17]) can provide lightweight, device-centered identity, but they are unreliable in noisy environments and often fail to incorporate human-related or biometric evidence for identity [18]. Other research workers employed timestamp-based verification like smart cards (e.g., Zhang et al., [19]), but many such devices require synchronized clocks or trusted hardware to function. In ad hoc clusters of UAVs, this may not be practical.

New work in mobile networks (many of which are also IoT deployments) has begun to examine how to combine biometric data and lightweight cryptography. Zhang et al. [20] and Ebrahimi et al. [21] have demonstrated that fuzzy extractors are capable of safeguarding biometric privacy while providing dependable generation for keys - albeit not yet in an aerial or drone network, where efficient mobility and unstable topologies create additional challenges for an attacker.

Algarni et al. [22] came up with a verifiably safe and robust ECC-based authentication protocol for synergistically assisted deployments of the Internet of Drones. Mutual authentication and session key secrecy were achieved by taking elliptic curve operations, hash functions, and ID commitments into consideration. Despite being effective, this protocol did not integrate any biometric components into itself, so it can be hacked by impersonation or another kind of insider threat with stolen verifiers. Table 1 offers a qualitative comparison of the security functionalities both protocols support.

Table 1: Security functionalities comparison between the proposed and baseline protocols

Security Feature	Algarni et. al [22]	Proposed Protool
Insider Threat Resistance	Limited	Enhanced (ZKP model)
Forward Secrecy	Partial	Yes
Stolen Verifier Resistance	Limited	Yes
Biometric Binding	No	Yes

We believe no work currently available worldwide blends biometric fuzzy extractors with ECC to create a decentralized, identity-focused authentication tool designed for IoD networks. This paper aims to fill that gap and devise a secure, participative system that is flexible and efficient too - it uses both cryptologic assurances and biometric guarantees for this end.

3 SYSTEM AND THREAT MODEL

3.1 System Model

The presented platform is envisioned for a distributed Internet of Drones (IoD) scenario, where unmanned

drones fly in swarms without continuous dependence on the Ground Control Station (GCS) after deployment, as shown in Figure 1. The relevant entities in the system are:

- Ground Control Station (GCS). A credible entity in which initializes the system parameters and registers the drones prior of assigning the mission. It computes Elliptic Curve Domain Parameters, hash functions, and biometric enrollment based on Fuzzy Extractor.
- Drone Di. Every drone is equipped with a biometric sensor (e.g., facial, fingerprint) and low-power computation. Drones are pre-registered with bio metric and ECC credential and they should authenticate with each other to start communication.
- Communication Model. The communication channels of the wireless connections among drones suffer from eavesdropping and message tampering.

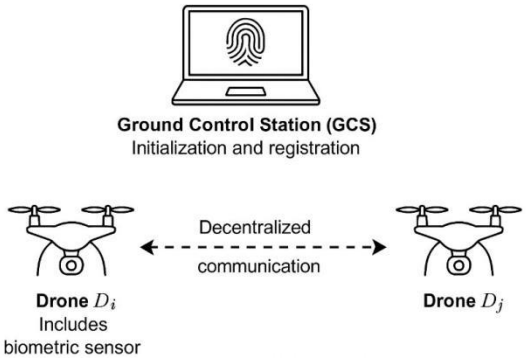

Figure 1: System model.

According to the GCS authority, there may be no need for GCS involvement after a UAD completes the registration process which will be in the form of one one-time registration, the AKA could be performed even if the GCS is not connected or in a dynamic environment to which the UAD belongs.

3.2 Threat Model

For the proposed protocol, we assume an adversarial model of Dolev-Yao and combine this with threats and risks affecting biometrics. It is assumed an attacker will have complete control over the communication channel, including the ability to intercept, replay, and forge messages, even if they cannot understand their contents. The threat under consideration here includes:

- Impersonation Attack. An adversary tries to be a legitimate drone by using either stolen or falsely made qualifications.
- Replay Attack. Authentication messages captured before are played again to obtain access without authority.
- Man-in-the-Middle (MITM) Attack. The adversary intercepts and/or alters the communication between any two drones during mutual authentication.
- Stolen-VerifierAttack. An attacker who has access to stored authentication data tries to recover secrets for forging a drone record;
- Biometric Inversion Attack. To reconstruct original biometric data from stored helper values is attempted.
- Insider Threat. A trusted party, such as a compromised GCS or drone, leaks credentials or attempts unauthorized access.
- Forward Secrecy Violation. If long-term keys fall into the hands of an adversary, they can decrypt past session keys and recover previous communications.

3.3 Security Goals

The proposed protocol seeks to attain the following security properties:

- Mutual Authentication. Both drones should confirm that each other is legal before communication occurs.
- Biometric Binding. Use Fuzzy extractors in order to tie authentication with the biometric properties of the person without disclosing or storing raw biometric templates.
- Session Key Freshness and Secrecy. Ephemeral keys should be generated for each session, to provide forward secrecy.
- Resistance to Known Attacks. Prevent degradation of integrity and privacy in the presence of impersonation, replay, MITM, and stolen-verifier attacks.
- Lightweight Efficiency. Keep the computational, communication, and storage assumptions small enough for deployment in a UAV.

4 PROPOSED BIO-AUTHENTICATED ECC PROTOCOL

This content looks at the problem from a fresh angle and proposes a Bio-Authenticated hybrid ECC Framework which helps secure drone-to-drone communications in an Internet of Drones environment. This proposed protocol uses a hybrid approach, Elliptic based on both biometric fuzzy extractors and Petty Curve Cryptography (ECC). The method ensures that mutual authentication is deeply integrated with a drone's physical identity, and at the same time, it is computationally efficient. The framework consists of three major issues: setup, biometric-based registration, and mutual authentication.

The expected general architecture structure of the ECC Framework, which requests verification by biometric data and then provides an ecc key to hold on an ID chip within uav is described in Figure 2 below. This captures all the crucial stages that need to be gone through for secure drone-to-drone communication within an IoD network. The protocol starts with a setup phase initiated by the Ground Control Station (GCS), followed by biometric registration of each drone through fuzzy extractors and ECC credentials. Once registered, drones use their biometrics to verify each other and exchange ECC keying material on an ephemeral basis until reaching the point where a secure session key can be derived. This design not only achieves cryptographic security but uses the unique biological attributes of a person's body to have their identity bound into authentication keys.

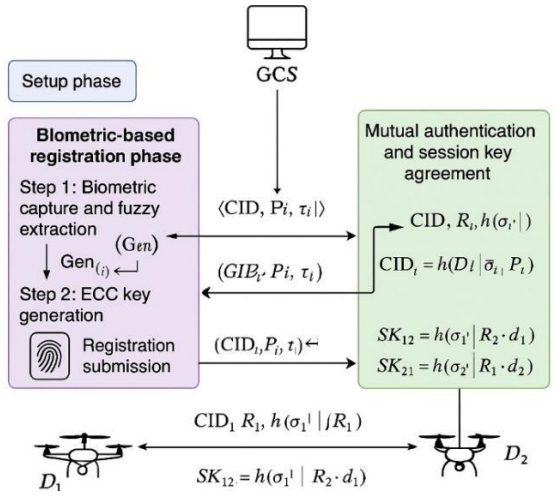

Figure 2: Bio-Authenticated ECC Framework for IoD drone communication.

4.1 Setup Phase

In the setup phase, the Ground Control Station (GCS) defines the domain parameters for the elliptic curve E(Fp), selects a base point P, and generates its ECC private key and corresponding public key PGCS = s · P. It also defines a cryptographic hash function h(.), and selects a fuzzy extractor function pair (Gen,Rep) for biometric processing. The public system parameters {E(Fp),P,PGCS,h(.),Gen(.),Rep(.)} are published, while the private keys remain securely stored in the GCS.

4.2 Biometric-Based Registration Phase

Each drone registers with the GCS before deployment. During registration, both the biometric identity and the ECC credentials are securely provisioned into the drone through the following steps:

1) Step 1: Biometric Capture and Fuzzy Extraction. Let drone Di capture its biometric trait BIOi (e.g., fingerprint or facial vector). The fuzzy extractor generates a stable representation using: (σi,τi) = Gen(BIOi). Here, σi serves as the biometric key, while τi is the helper data required for reconstruction.
2) Step 2: ECC Key Generation: The drone selects a private. ECC key and computes its public key: Pi = di·P. It then computes an identity commitment: CIDi = h(IDi ‖ σi ‖ Pi).
3) Step 3: Registration Submission: Drone Di sends {CIDi,Pi,τi} to the GCS via a secure offline channel. The GCS verifies the information, stores the commitment, and confirms registration. After successful registration, the GCS provisions the drone memory with: τi (helper data), PGCS, the Drone's ECC private key di, and the shared hash function h(.).

4.3 Mutual Authentication and Session Key Agreement

When two drones, D1 and D2, seek to communicate in a secure IoD cluster, the mutual authentication protocol proceeds as follows:

1) Step 1: Biometric Verification and ECC Nonce Exchange. D1 captures a fresh biometric sample BIO′1, and reconstructs the key: Rep . It selects a random nonce and computes an ephemeral public key: R1 = r1 · P. It constructs message: M1 = sends M1 over an insecure channel.

2) Step 2: Verification and Response. D2 retrieves CID1 and verifies using stored parameters. If valid, D2 captures its own biometric BIO′2, reconstructs, and selects a nonce r2. Computes R2 = r2 · P and send M2 in response.
3) Step 3: Session Key Derivation. Both drones now derive a shared session key using ECDH and their biometric binding: and SK21.

Due to the properties of ECC and matched biometric keys, we have: SK12 = SK21. At this point, both drones have established a secure session key authenticated by both cryptographic and biometric means, enabling encrypted communication.

5 INFORMAL SECURITY ANALYSIS

This section provides an informal evaluation of the proposed. Bio-Authenticated ECC Framework, demonstrating its robustness against a wide range of cryptographic and biometric-related threats. The hybrid use of biometric authentication and elliptic curve cryptographic primitives significantly enhances the resilience of the system, particularly within the constrained and adversarial IoD environment:

- Impersonation Attack. An impersonation attempt requires the adversary to successfully reconstruct the biometric key σi and possess the ECC private key di of a legitimate drone. However, the biometric data is never transmitted directly, and the ECC private key remains securely stored within the drone.
- Replay Attack. To resist replay attacks, the protocol employs ephemeral ECC keys (R1, R2) that are generated fresh in each session and bound with biometric hash commitments.
- Man-in-the-Middle (MITM) Attack. The use of ECCbased Diffie–Hellman key exchange in conjunction with biometric verification provides resistance against MITM attacks.
- Stolen-Verifier Attack. In case a drone is physically compromised, the attacker may gain access to stored data such as τi, Pi, and possibly even di. However, the protocol ensures that biometric credentials σi are not stored, only reconstructed transiently during authentication;
- Biometric Template Inversion. The fuzzy extractor mechanism ensures that helper data τi reveals no significant information about the original biometric.
- Forward Secrecy. Forward secrecy is achieved by the use of ephemeral ECC keys R1, and R2, which are discarded after session completion. Even if an adversary compromises a drone's long-term keys di, it will not enable the decryption of past session keys, as these depend on transient random values and fresh biometric samples not retained post-session.
- Insider Threat Resistance. The Ground Control Station (GCS) never retains or transmits the biometric key σi, and its knowledge is limited to identity commitments CIDi and public parameters.
- Desynchronization Attack. Because the authentication relies on session-specific ephemeral data and on-the-fly biometric reconstruction rather than synchronized shared secrets or counters, desynchronization attacks have no effect.

6 PERFORMANCE EVALUATION

he evaluation also includes the comparison with Algarni et al. [22]'s baseline protocol to illustrate improvements in authentication security and system efficiency within unreliable contexts.

6.1 Computational Cost

When the computational cost of both protocols is measured in cryptographic operations per authentication session, for purposes of information transfer we will adopt the following unit operation signs as needed. Figure 3 illustrates the computational cost comparison between the proposed Bio-Authenticated ECC Framework and the baseline protocol by Algarni et al. (2025).

6.2 Communication Overhead

The proposed protocol's authentication exchange will consume fewer cryptographic points at each exchange as the relay of GCS is removed. Messages are expressed in bits. Figure 4 presents a comparison of communication overhead between the proposed protocol and the scheme by Algarni et al. (2025).

The results demonstrate that the proposed approach significantly reduces the total number of transmitted bits per authentication session—from 1340 bits to 960 bits—highlighting its efficiency and suitability for bandwidth-constrained IoD environments.

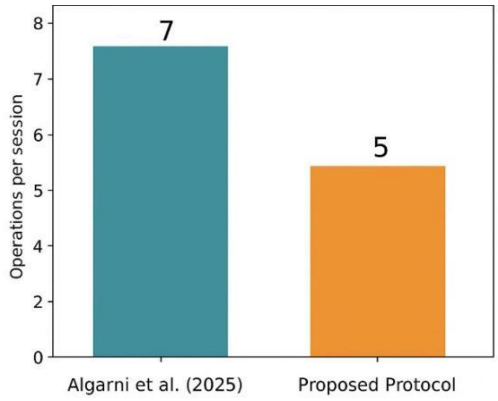

Figure 3: Comparison of computational cost.

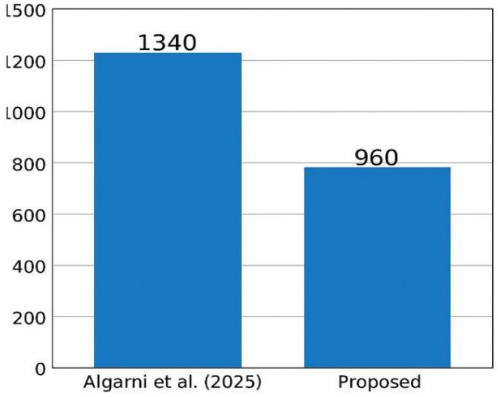

Figure 4: Communication overhead comparison.

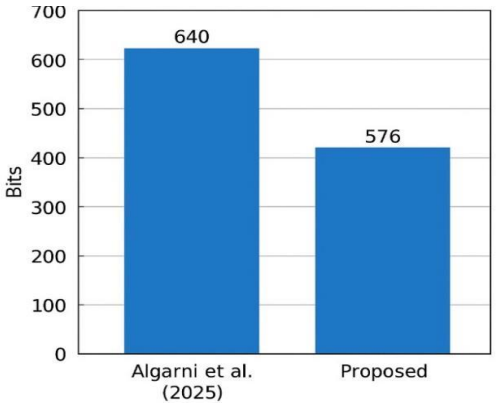

Figure 5: Storage cost comparison.

6.3 Storage Cost

Most of the storage requirements consist of ECC keys, helper data for fuzzy extractors and pre-loaded public parameters. The biometric template never gets directly stored. Figure 5 illustrates the storage requirements for both the proposed protocol and the scheme by Algarni et al. (2025).

7 CONCLUSIONS

An Applied Biometric-Based ECC Framework for Secure Drone-to-Drone Communication in the Internet of Drones (IoD) Environments has been presented in this paper. By integrating biometric fuzzy cryptography with elliptic curve cryptography, the protocol guarantees statistically mutual authentication that is fast, lightweight, and attack-resistant. Performance evaluations reported in this work show that the proposed scheme reduces the computational load, communication overhead, and storage requirements compared with existing protocols like that of Algarni et al. (2025). By incorporating biometric binding performance, the certainty of the protocol is higher and at the same time, its performance is very stable indeed. This makes the system especially suitable for resource-constrained and mission-critical drone deployments. These features make the framework particularly well-suited for resource-constrained and mission-critical drone deployments, where both security and efficiency are paramount. Furthermore, the approach offers strong scalability potential, allowing seamless integration into larger IoD networks. Future work could focus on adapting the framework for heterogeneous drone fleets, testing in highly dynamic environments, and exploring integration with AI-driven threat detection systems to further enhance autonomous security capabilities.

REFERENCES

[1] S. A. H. Mohsan, M. A. Khan, F. Noor, I. Ullah, and M. H. Alsharif, “Towards the unmanned aerial vehicles (UAVs): A comprehensive review,” Drones, vol. 6, no. 6, p. 147, 2022.

[2] A. K. Nanda, S. R. Marukanti, U. Harish, B. V. Dheeraj, B. S. Adoni, C. R. Reddy, and S. Nanda, “Evaluating lightweight asymmetric cryptography for secure communication in Internet of Drones,” in Proc. 2025 Fourth Int. Conf. Power, Control and Computing Technologies (ICPC2T), IEEE, 2025, pp. 875–879.

[3] K. Osmani and D. Schulz, “Comprehensive investigation of unmanned aerial vehicles (UAVs): An in-depth analysis of avionics systems,” Sensors, vol. 24, no. 10, p. 3064, 2024.

[4] J. Shan, W. Jiang, Y. Huang, D. Yuan, and Y. Liu, “Unmanned aerial vehicle (UAV)-based pavement image stitching without occlusion, crack semantic segmentation, and quantification,” IEEE Trans. Intell. Transp. Syst., 2024.

[5] Z. Ren, K. Hussain, M. Faheem, et al., “K-means online-learning routing protocol (K-MORP) for unmanned aerial vehicles (UAV) ad hoc networks,” Ad Hoc Networks, vol. 154, p. 103354, 2024.

[6] N. Alzahrani, "A verifiably secure and lightweight device-to-device (D2D) authentication protocol for resource-constrained IoT networks," IEEE Access, 2025.

[7] Z. Zhang and Z. Shu, "Unmanned aerial vehicle (UAV)-assisted damage detection of wind turbine blades: A review," Energies, vol. 17, no. 15, p. 3731, 2024.

[8] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey, and A. A. Almazroi, "Chebyshev polynomial based emergency conditions with authentication scheme for 5G-assisted vehicular fog computing," IEEE Trans. Dependable Secure Comput., 2025.

[9] J. Zhang, X. Chen, Q. Cheng, X. Chen, and X. Luo, "An enhanced certificateless blockchain-assisted authentication and key agreement protocol for Internet of Drones," IEEE Trans. Netw. Sci. Eng., 2025.

[10] V. Jithu Vijay and S. M. Thampi, "Navigating the skies: Exploring dynamic access control in the Internet of Drones (IoD)," in Securing the Connected World: Exploring Emerging Threats and Innovative Solutions, Springer, 2025, pp. 345–380.

[11] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: A review and future directions," Indonesian J. Electr. Eng. Comput. Sci., 2023.

[12] Z. Oudina, M. Derdour, A. Dib, and M. M. Bouhamed, "Empirical analysis of the security threats and risks that drones face, represent, and mitigation," in Proc. 2024 6th Int. Conf. Pattern Anal. Intell. Syst. (PAIS), IEEE, 2024, pp. 1–8.

[13] O. Ceviz, S. Sen, and P. Sadioglu, "A survey of security in UAVs and FANETs: Issues, threats, analysis of attacks, and solutions," IEEE Commun. Surveys Tuts., 2024.

[14] M. Kabi, N. Dayal, and P. Raikwal, "ECC-based lightweight authentication for resource-constrained devices leveraging the edge node," IEEE Trans. Rel., 2025.

[15] S. M. Gilani, A. Anjum, A. Khan, M. H. Syed, S. A. Moqurrab, and G. Srivastava, "A robust Internet of Drones security surveillance communication network based on IOTA," Internet of Things, vol. 25, p. 101066, 2024.

[16] I. Chandran and K. Vipin, "A PUF secured lightweight mutual authentication protocol for multi-UAV networks," Comput. Networks, vol. 253, p. 110717, 2024.

[17] L. Zhang, J. Xu, M. S. Obaidat, X. Li, and P. Vijayakumar, "A PUF-based lightweight authentication and key agreement protocol for smart UAV networks," IET Commun., vol. 16, no. 10, pp. 1142–1159, 2022.

[18] W. Wang, Z. Han, T. R. Gadekallu, S. Raza, J. Tanveer, and C. Su, "Lightweight blockchain-enhanced mutual authentication protocol for UAVs," IEEE Internet Things J., vol. 11, no. 6, pp. 9547–9557, 2023.

[19] 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, 2023.

[20] S. Zhang, Z. Yan, W. Liang, K.-C. Li, and C. Dobre, "BAKA: Biometric authentication and key agreement scheme based on fuzzy extractor for wireless body area networks," IEEE Internet Things J., vol. 11, no. 3, pp. 5118–5128, 2023.

[21] S. Ebrahimi and S. Bayat-Sarmadi, "Lightweight fuzzy extractor based on LPN for device and biometric authentication in IoT," IEEE Internet Things J., vol. 8, no. 13, pp. 10706–10713, 2021.

[22] A. D. Algarni, N. Innab, and F. Algarni, "A verifiably secure and robust authentication protocol for synergistically-assisted IoD deployment drones," PLoS One, vol. 20, no. 3, p. e0314475, 2025.