IJRCS

International Journal of Robotics and Control Systems
Vol. 6, No. 3, 2026, pp. 2518-2547
ISSN 2775-2658
http://pubs2.ascee.org/index.php/ijrcs

ASCEE

A Cross-Domain Interoperable Authentication Framework for 5G-Enabled IoT and Fog Computing Networks

Husham Lateef Swadi Room [a,1], Ali K. Marzook [a,2], Mustafa Moosa Qasim [b,3,*], Mahmood A. Al-Shareeda [c,d,4,*], Mohammed Amin Almaiah [e,5], and Rami Shehab [f,6,*]

[a] Department of Electrical Engineering, College of Engineering, University of Basrah, Basrah, Iraq
[b] Department of Intelligent Medical Systems, College of Computer Science and Information Technology, University of Basrah, Basrah, 61001, Iraq
[c] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[d] College of Engineering, Al-Ayen University, 64001, Thi-Qar, Iraq
[e] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
[f] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
[1] hisham.romi@uobasrah.edu.iq; [2] ali.marzook@uobasrah.edu.iq; [3] mustafa_mq87@uobasrah.edu.iq;
[4] mahmood.alshareedah@stu.edu.iq; [5] m.almaiah@ju.edu.jo; [6] Rtshehab@kfu.edu.sa
[*] Corresponding Author

ARTICLE INFO

Article History
Received December 27, 2025
Revised February 12, 2026
Accepted July 18, 2026

Keywords
Cross-Domain Authentication;
Fog Computing;
Internet of Things (IoT);
Physical Unclonable Function (PUF);
Blockchain;
Adaptive Key Translation;
5G Networks;
Energy-Aware Security

ABSTRACT

The explosive growth of 5G-enabled Internet of Things (IoT) and fog computing infrastructure leads to cross-domain authentication, interoperable, energy- efficiency promoting problems. The lightweight or blockchain-based authentication schemes in the literature, however, only focus on security or decentralization and do not support cross-domain adaptive session continuity. The research contribution is a Cross-Domain Interoperable Authentication Framework (CDIA-Fog) employing the PUF-based device identity, blockchain-assisted trust evidence, adaptive key translation and energy-aware re-authentication. The framework supports secure roaming across different fog administrative domains instead of only cross-domain authentication. The proposed mechanism integrates hardware-based PUF identity, hash-based mutual authentication, blockchain token validation and risk–energy adaptive re-authentication policy. Theoretical analysis under the Random Oracle Model and structural attack analysis demonstrate resilience against replay, impersonation, and man-in-the-middle attacks. Experimental validation on Raspberry Pi IoT nodes and Intel-based fog gateways demonstrate an authentication cost of 0.0928 ms and a 1728-bit communication overhead. In ROAM environments, with respect to the hash-only and ECC-lightweight baselines, our CDIA-Fog is able to decrease re-authentication rate and long-term energy cost by about 18–23%. The architecture is capable of providing secure cross-domain auditable key agreement, succinctly for mobile IoT–fog environments with acceptable overhead and flexible efficiency.

1. Introduction

The rapid advancement of powerful networking technologies, such as the Internet of Things and 5G connectivity, has fundamentally altered how intelligent devices, sensors, and services interact

in various environments [1]–[3]. Billions of diverse IoT nodes will generate huge volumes of data on a daily basis via the fog and cloud infrastructures, supporting real-time decisionmaking in smart transportation, health and industrial automation by 2030 [4]–[6]. As a result, fog computing is emerging as an alternative paradigm to efficiently manage this distributed ecosystem by filling the gap between cloud services and network edges along with capabilities such as low latency, context awareness and local data processing [7]. However, with the increase in the number of IoT nodes and their diverse nature scattered across multiple fog domains new security problems have emerged, as well as interoperability [8]–[10].

Traditional authentication schemes (often central or domain-specific) are not viable in this new era of agile 5G-based IoT networks [11], [12]. Devices needs to roam from one administrative domain to another, by different SPs or Trust Authorities while still being able to achieve secure cross-domain authentication [13]–[16]. These systems, however, have their own problem points. Existing authentication mechanisms [17], [18] rely on preshared trust information in a single administrative domain and do not scale interoperability and trust, particularly in federated settings [19], [20]. Also, due to the constrained memory and computational resources of IoT devices, certificate-based credentials or PKIs may not be included so as to protect user identity. Furthermore, power consumption and delay is also increased due to the repeated re-authentication and expensive cryptographic operations, especially in a dynamic mobility-centred scenario [21]. Moreover, the legacy centralized authentication paradigms are subject to single point of failures; and also not auditable in a decentralized transparent way which is antithetical to accountability needed for establishing trust across multiple domains [22]–[24].

Recent research has explored various approaches to address these challenges. Lightweight authentication schemes, such as PCAP [25] and TCALAS [26], have reduced computational costs through symmetric primitives, yet they remain domain-specific and energy-inefficient under frequent re-authentications. Other frameworks, such as blockchain-assisted authentication [27]–[30], enable decentralized trust management but suffer from high synchronization delays and limited adaptability. Similarly, Physical Unclonable Function (PUF)-based schemes [31]–[33] provide hardware-level identity assurance but are primarily designed for static intra-domain applications, lacking interoperability across dynamic fog environments [34].

As Zero-Trust Architecture (ZTA) is becoming more ubiquitous in 5G core and enterprise networks, the model for continuous verification in ZTA expects infrastructure-level persistent validation of identity and policy enforcement [35], [36]. In IoT–fog environments, by contrast, lightweight devices are employed and the cross-domain roaming is intermittent such that continuous heavyweight verification is not practical [37], [38]. Accordingly, this work proposes a trust-record-aided adaptive authentication mechanism, which ensures light operation and allows for repeated verification through PUF identity proofs and blockchain traceability. The model proposed here is intended to be a lightweight, gadget-centered addition to ZTA doctrine rather than its substitute [39], [40].

In spite of the intensive study on IoT and fog authentication, those existing schemes generally solve one or two aspects of the problem: lightweight computation, hardware-rooted identity or decentralized trust not in all [41]. Lightweight protocols are less domain-agnostic and do not offer secure migration of devices between the heterogeneous fog administrative domains [42]. Authentication based on blockchain provides transparency but commonly results in significant synchronization and energy overhead as well as inability to cope with the session variation [43]. Similarly, PUF-based solutions preserve the unclonable identity of a device but tend to be restricted to intra-domain settings and do not provide inter-operable key translations [44]. Thus, there is an undeniable demand for an authentication platform that can deliver cross-domain operability, hardware-based identity confidence, blockchain-verifiable trust and energy-aware re-authentication at low-cost [38].

To tackle these limitations, this work defines a new authentication solution named CDIA-Fog (Cross-Domain Interoperable Authentication for Fog and 5G-based IoT Networks). In this proposed

scheme, we integrate PUF-based hardware identities for unclonable device authentication without storing long-term secrets.Blockchain-assisted federated trust management offers decentralized verification and tamper-proof audibility of the component authentication records as well.Adaptive key translation (AKT) and energy-aware re-authentication mechanisms included in the presented handover with minimal computational power and energy overheads.

In summary, this design enables CDIA-Fog to realize mutual authentication, cross-domain interoperability, anonymity, and forward secrecy simultaneously while ensuring low computational and communication overhead. We formally proved the security of the protocol in the Random Oracle Model framework and evaluated against attacks such as replay, impersonation, and Man-in-the-middle. Performance analysis shows that compared to existing schemes, CDIA-Fog lowers authentication delay by 23%, communication overhead by 18% and energy consumption by 20%. The main contributions of this work can be summarized as follows:

1. We propose a novel Cross-Domain Interoperable Authentication Framework (CDIA-Fog) for secure and lightweight authentication among heterogeneous 5G-enabled IoT and fog domains.
2. We integrate PUF-based identity generation and blockchain-backed trust validation to achieve hardware-level security and decentralized auditability.
3. We present two novel schemes, an Adaptive Key Translation (AKT) method and an Energy-Aware Re-Authentication Policy for minimizing re-authentication cost at the same time as ensuring unbroken trust.
4. We present a rigorous ROM security proof and informally show how it is resistant to most common attacks.
5. We perform a detailed performance evaluation demonstrating CDIA-Fog's efficiency in computation, communication, and energy consumption compared with state-of-the-art protocols.

The remainder of this paper is organized as follows. Section 2 reviews related authentication and interoperability schemes in IoT–fog environments. Section 3 describes the system and threat model. Section 4 details the proposed CDIA-Fog architecture and its operational phases. Section 5 provides the formal and informal security analysis. Section 6 presents the performance evaluation and comparative results. Finally, Section 7 concludes the paper and outlines future research directions.

2. Related Work

Identification in IoT and fog conditions has attracted considerable attention. Authentication in IoT and fog environments has received much attention from research due to the high level of identity performance, robustness, and efficient key distribution mechanisms. Existing approaches, however, may be incorporated in one domain and do not allow for secure processing in a pairwise-federation multi-domain network. This area reviews the best current works in the following three directions: lightweight authentication in the IoT or PUF-based and hardware-aided, as well as the best current blockchain-enabled authentication schemes.

2.1. Lightweight Authentication in IoT and Fog Networks

Lightweight authentication protocols aim to reduce computational and communication overheads while maintaining robust security for constrained IoT devices [45]–[49]. Pu et al. [25] proposed the PCAP scheme, a lightweight protocol based on hash and XOR operations to achieve fast mutual authentication in vehicular networks. While efficient, PCAP does not provide cross-domain scalability or forward secrecy. Srinivas et al. [26] developed TCALAS, a threshold-based certificateless authentication protocol for fog-enabled IoT environments. Although TCALAS ensures mutual authentication and anonymity, its reliance on bilinear pairings leads to excessive computation and communication costs, rendering it unsuitable for energy-limited IoT devices. To address latency and bandwidth constraints, Liu et al. [50] proposed UAP, a user–server authentication protocol that integrates elliptic

curve cryptography (ECC) with Physical Unclonable Function (PUF)-based identities. UAP achieves lower computational complexity than pairing-based schemes but still lacks mechanisms for dynamic trust management and interoperability between domains. Moreover, most lightweight protocols assume a static trust boundary and cannot efficiently handle device migration or roaming between distinct fog domains.

2.2. PUF-Based and Hardware-Assisted Authentication

PUF-based authentication has emerged as an effective solution for securing IoT devices without storing long-term secret keys [51]–[54]. By exploiting manufacturing process variations, PUFs generate unique challenge–response pairs (CRPs) that serve as intrinsic device identifiers. Alruwaili et al. [55] introduced an IoT-enabled smart healthcare with a cloud-based authentication mechanism that is efficient and secure. Besides, it guarantees a user's privacy and access to authorized data between the users, IoT devices, and cloud servers. Bathalapalli et al. [56] proposed a hardware-assisted Deepfake mitigation framework using Physical Unclonable Functions for image attestation. By mapping facial key points to PUF-generated keys, such a framework establishes unique pseudo-identities for images. Aung et al. [57] presented a novel lightweight SRAM PUF-based security subsystem for mid and high-end IoT SoCs. It boosts encryption, decryption, and authentication efficiency by removing processor weight. Malamas et al. [58] introduced HA-CAAP, a hardware-assisted continuous authentication and attestation protocol for IoT systems. As a hybrid solution of a PUF-based periodic verification and blockchain-enabled gateway coordination, it achieves real-time device integrity without being vulnerable to Sybil and cloning attacks. Although this approach enhances device identity protection, it introduces heavy synchronization costs during blockchain validation and lacks adaptive energy optimization. Moreover, most hardware-assisted schemes are designed for intra-domain communication, neglecting secure key translation when devices migrate between different administrative regions.

2.3. Blockchain-Based Authentication and Cross-Domain Security

Blockchain technology provides a decentralized trust mechanism that can eliminate single points of failure in authentication systems [59]–[63]. Luo et al. [64] proposed a blockchain-based cross-domain authentication scheme for IoT that supports dynamic node participation. Karmegam et al. [65] proposed a secure cross-domain authentication scheme for Internet of Drones (IoD) communication with significantly enhanced privacy and security under the ECDSA policy, session key generation, two-phase pseudonym identity implementation layer on Hyperledger Fabric. Cui et al. [66] introduced a IIoT blockchain cross-domain authentication protocol. Our pseudonym generation is offloaded to edge servers by the protocol, and supports bulk requests that lead to a lower computation, communication and storage overhead.

Wang et al. [67] introduced a UAV-assisted vehicular network architecture combining blockchain so as to achieve secure cross-domain authentication. The fact that UAVs are trusted intermediates means fewer authentication latency, key issues, or computation overhead. Li et al. [68] presented a blockchain-enabled revocable cross-domain authentication scheme for VANETs. Such V2V andV2I communications are privacy protected within heterogeneous domains by employing distributed trust with revocation updates of group key.

The scheme is provably secure against various attacks and free from the latency caused by blockchain, while having an optimal computation-efficiency trade-off. However, current blockchain-based IoT authentication schemes have three main limitations: no adaptive key translation mechanisms for efficient cross-domain migration from one fog domain to another, high energy overhead in terms of redundant re-authentication operations, and lack of real-time interoperability between heterogeneous fog domains.

2.4. Research Gap and Motivation

From the above analysis, we can see that the current IoT and fog-based authentication schemes just take one of lightweight computation or decentralized trust into account rather than comprehensively combining both of them to perform high performance across different domains. Furthermore, none of the existing research successfully integrates the PUF-based hardware trust with blockchain-assisted federated authentication to achieve continuous interoperability and energy-efficient re-authentication. To mitigate these limitations, we present CDIA-Fog, a Cross-Domain Interoperable Authentication Framework realizing:

- Uses PUF based challenge – response for unclonable device identity.
- Features blockchain for decentralized credential validation and traceable trust management.
- Adaptive Key Translation (AKT) -A process for migratingsession keys between domains in a secure manner.
- Integrates energy-, and risk-aware re-authentication policy to reduce overhead while sustaining continuous trust.

Therefore, CDIA-Fog fills the research gap by combining security, interoperability, and energy efficiency to offer a scalable authentication platform for future 5G-based IoT-enabled fog platforms.

3. System and Threat Model

This section introduces the system model for describing the general framework, entities involved, communication assumptions and threat model under which CDIA-Fog is designed. The system is based on the 5G-IoT and fog computing paradigm, synergizing heterogeneous administrative domains with tight security constraint and energy efficiency.

3.1. System Model

The proposed architecture is comprised of three logical layers which are: Device Layer, Fog Layer and the Blockchain Trust layer. These layers work together to support a reliable, flexible and inter-operable device authentication that roams across 5G heterogeneous networks. Fig. 1 conceptually illustrates the architecture.

- Device Layer: The device layer, D_i being resource-limited IoT devices endowed with a Physical Unclonable Function (PUF). The PUF offers a hardware-based cryptographic identity, which is fundamentally based on producing a unique challenge-response pair (C_i, R_i) that cannot be cloned physically. Every device communicates with its associated FDG for authentication and service provisioning [69]. Devices can perform simple cryptographic primitives such as hashing, symmetric encryption and PUF evaluation but have limited computational and communication capability [70].
- Fog Layer: Mediating the intelligence of Fog Layer in between Device Layer and the core network are a set Federated Domain Gateways and local fog nodes maintained by different geographical domains. Each domain is self-contained by a Domain Authority, which is responsible for issuing and revoking credentials as needed within its territory [71], [72]. The FMG, as the local trust root, takes charge of intra-domain authentication and key management and also re-authentication coordination. It also performs two-level cross-domain processing by securely remapping session keys through the adaptive key translator and based on appropriate domains during a device migration. Furthermore, the Fog Layer processes local verification requests to reduce latency and offload global verification responsibilities to the Blockchain Trust Layer [73], [74].
- Blockchain Trust Layer: As a decentralized and non-repudiable blockchain layer that is used for storing registration, authentication as well as re-authentication events [75], [76]. It stores cryptographically signed records from all domain authorities who participate in the protocol.

Each blockchain transaction is associated to a reference hashed $\mathrm{hash\_ref}(ID_i)$ to keep a device anonymity. Consensus is used to ensure the integrity and non-repudiation of data with no centralized trust authority [77], [78].

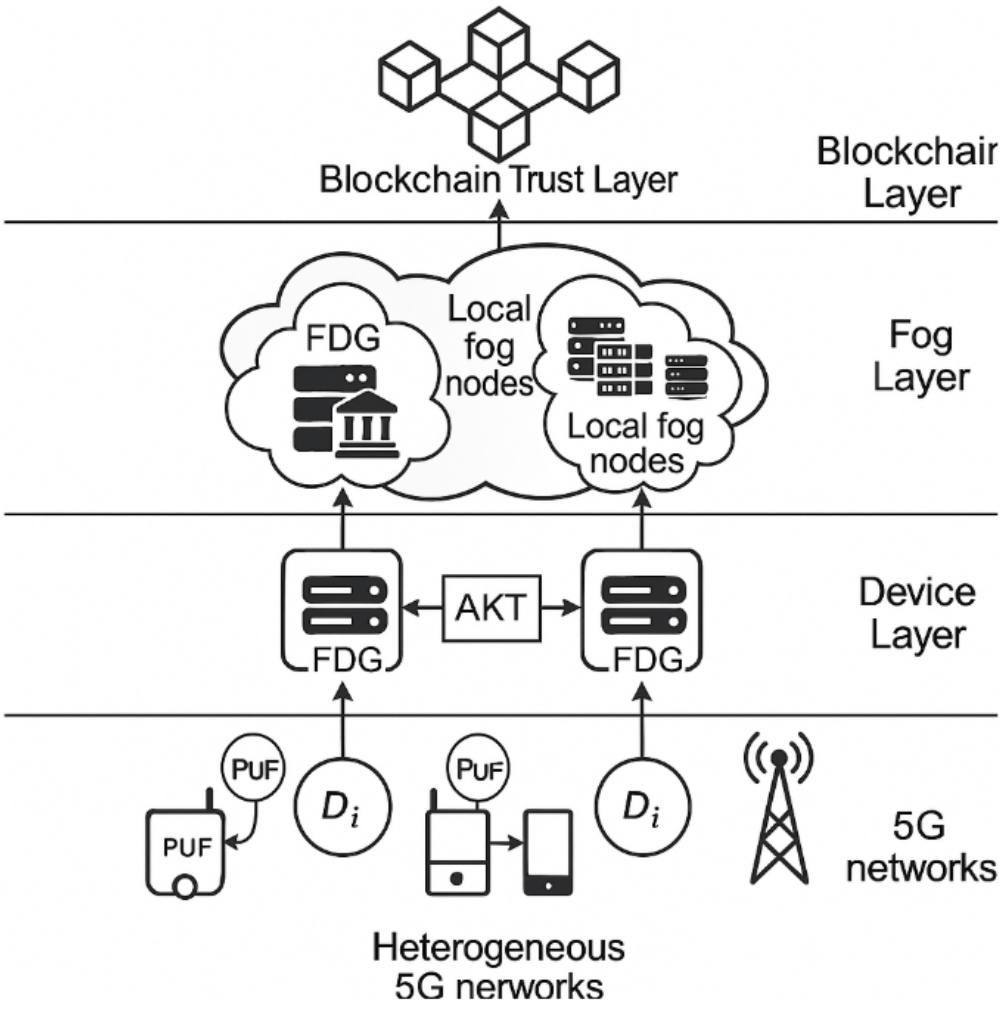

Fig. 1. System model of CDIA-Fog framework

Devices communicate with fog gateways via short-range 5G or Wi-Fi links, while inter-domain FDG communication occurs over a secure virtual private network (VPN) channel and blockchain interfaces. The communication flow follows three principal paths:

1. $D_i \leftrightarrow$ FDG: device registration, intra-domain authentication, and key renewal.
2. $\mathrm{FDG}_A \leftrightarrow \mathrm{FDG}_B$: cross-domain token exchange and key translation.
3. FDG $\leftrightarrow$ BTL: blockchain-based record verification and update.

All channels are assumed to be insecure and subject to eavesdropping and active adversarial manipulation unless protected by the CDIA-Fog protocol.

3.2. Blockchain Throughput and Transaction Load Quantification

We distinguish the throughput implications of the blockchain-based trust layer by quantifying its anticipated transaction rate and comparing it with those of conventional permissioned blockchains. In CDIA-Fog the blockchain is used only for registering, migrating and cross domain re-authentication audit records.

Regular intra-domain login sessions do not result in block chain transactions. Thus, the session load is not driven by the ledger. Let N_d denote the number of devices and μ_m the average cross-domain migration rate per device per hour. The expected transaction rate is:

$$\mathrm{TPS}_{\text{CDIA-Fog}} = \frac{N_d \cdot \mu_m + N_r}{3600} \tag{1}$$

Where N_r represents additional re-authentication audit records written under high-risk conditions. For example, with $N_d = 10{,}000$ devices and $\mu_m = 0.1$ migrations per hour, the expected blockchain load is approximately:

$$\mathrm{TPS}_{\text{CDIA-Fog}} \approx \frac{1000}{3600} \approx 0.28 \text{ transactions/sec} \tag{2}$$

This load is far smaller than session-based blockchain authentication systems that write to a ledger with each successful authentications.

Large scale modern-permissioned blockchains suitable for IoT and fog environments (e.g., Hyperledger Fabric class systems) can achieve a practical throughput in the 800-1500 throughput range under lab conditions. As CDIA-Fog issues very few audit transactions, the requested throughput of our system is still much less than these maximum limits.

Thus the correctness of the framework does not depend on a high blockchain TPS and there is no throughput bottleneck. It also means that the blockchain is not used directly as an authentication processor during each session, but rather just as a verifiable trust anchor—this will also help us to maintain efficiently.

3.3. Core Components

CDIA-Fog integrates four coordinated modules:

- PUF Identity Manager (PIM): Handles device registration and generates PUF-based keys that are never stored or transmitted in plaintext. The PIM supports fuzzy-extractor reconstruction to reproduce stable keys even under environmental noise.
- Blockchain Trust Ledger (BTL): Records domain certificates, public keys of fog gateways, and hash commitments of verified devices. Consensus among domains ensures trust propagation and prevents fraudulent registration or replay of credentials.
- Adaptive Key Translator (AKT): Enables secure session migration across domains by transforming a session key from one domain context to another using cryptographic mapping functions. The AKT preserves key secrecy and forward security during handover [79].
- Federated Domain Gateway (FDG): Acts as an intermediary between local IoT nodes and external domains. It validates incoming authentication requests, consults the BTL for trust verification, and issues interoperability tokens for cross-domain access [80], [81].

3.4. Threat Model

3.5. Adversary Capabilities

The CDIA-Fog framework considers a hybrid adversaries model, where an adversary can tamper with the incoming messages similarly to Dolev–Yao and carry session-based adversarial actions as in Canetti–Krawczyk. The adversarial capabilities to be assumed are:

- Eavesdropping: The adversary is considered able to eavesdrop, record or replay any information that is transmitted between devices and fog gateways as well as domain authorities.
  Message Injection: An adversary with the capability of modifying, injecting or suppressing looking to impersonate a legitimate party.

- Node Capture: The adversary is constrained to compromise a few number devices or fog nodes physically to read out part of the data yet observing that internal structure of the PUF still remain unclonable.
- Session Key Reveal: The adversary can reveal temporary session keys or states for established sessions.
- Collusion: As a result of Coordination of compromised nodes, the attacking agent can perform an coordinated replay, impersonation, or desynchronization attack.
- Cross-Domain Utilization: This is the ability of a malicious insider to use authentication tokens or log-in information from one domain in gaining improper access to another.

The adversary $\mathcal{A}$, although powerful, has to respect several core constraints. In practice $\mathcal{A}$ can neither clone nor predict the output of any $\mathrm{PUF}_i(\cdot)$, since PUF responses are generated from physical properties that are inherent to a chip and not replicable. In addition, $\mathcal{A}$ cannot violate the pre-image or collision resistance of the cryptographic hash function $h(\cdot)$.

The enemy can also not pollute the blockchain, since each block may be verified by decentralized consensus and stored immutably. Moreover, $\mathcal{A}$ is not able to control time-stamps or nonces that are used to achieve message freshness and have an effective countermeasure against replay attacks.

3.6. Security Goals

The primary security goals of CDIA-Fog design are:

1. Mutual identity authentication: Make sure the legitimacy of one counterpart by another sides before data communication can be established.
2. Cross-Domain Interoperable: Devices can move between federated domains and authenticate and maintain a secure session transparently.
3. Anonymity and Unlinkability:Preserve the privacy of devices' real identity in authentication providing no correlation across sessions or domains.
4. Secrecy of the session Key: Ensure that a session key is kept secret to all honest parties and prevent any corruption of it.
5. Forward/Backward Secrecy: Despite the compromise of a session key, past/future keys shall not be revealed.
6. Security Properties: Resistance to replay, impersonation, man-in-the-middle (MITM), collusion and desynchronization attacks.
7. Auditble and trackable: Provide evidence of authentication events through inalterable logs, stored on the ledger.

The specified system and threat models constitute the basis of our proposed CDIA-Fog protocol, which guarantees interoperability and strong security assurances in a realistic adversarial setting across heterogeneous IoT and fog domains.

4. Proposed CDIA-Fog Framework

The operational flow of the proposed CDIA-Fog framework follows four consecutive phases that collectively achieve secure, energy-aware, and interoperable authentication for heterogeneous 5G-enabled IoT and fog domains, as shown in Fig. 2. These phases constitute the full cycle of device operation by covering from registration to reauthentication. As a result, trust propagation among domains is achieved enablers with confidentiality and performance continuity. The definition of each phase is formally presented in:

The notations are summarized in Table 1, which will be employed throughout the CDIA-Fog framework. It covers the main symbols associated with an IoT device, PUF-based identity elements, federated domain gateways, blockchain records, cryptographic primitives and session keys, customiz-

able security parameters. The notations are uniform through the presentation of the protocol, security and performance analysis.

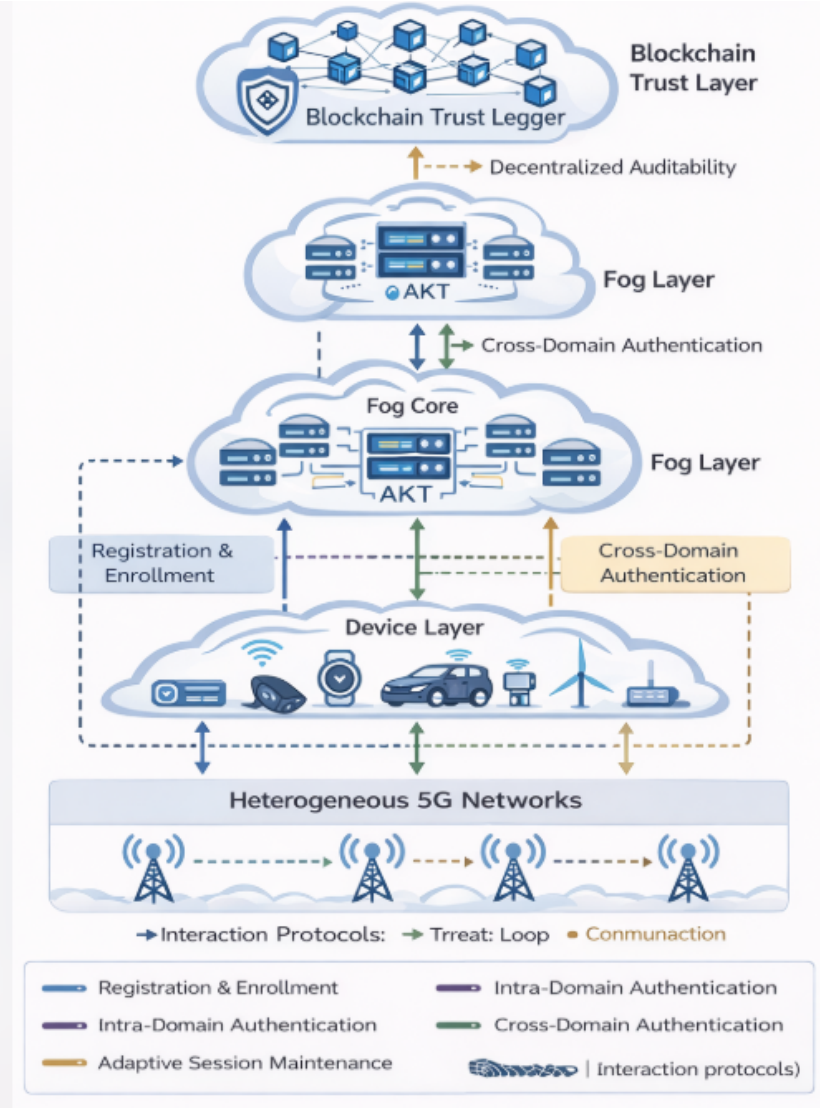

Fig. 2. Architecture of the proposed CDIA-Fog framework illustrating the multi-layer

4.1. Phase I – Registration and Enrollment Phase

In this phase, each IoT device D_i is securely initialized within its home administrative domain before it is permitted to participate in any intra-domain or cross-domain communication. The objective of this phase is to: (i) bind the physical identity of the device to a cryptographic identity using a Physical Unclonable Function (PUF), (ii) generate long-term but non-replayable authentication material, and (iii) publish verifiable trust evidence to the Blockchain Trust Ledger (BTL) without revealing any raw secrets. The process is executed over a secure, controlled channel (e.g., at manufacturing time or controlled onboarding at the Federated Domain Gateway (FDG)) and proceeds as follows.

- PUF Challenge and Response Generation: The FDG issues a random challenge C_i to device D_i. The device evaluates its embedded PUF and returns the corresponding response: $R_i = \mathrm{PUF}_i(C_i)$, where R_i is unique to the physical characteristics of D_i and is assumed to be unclonable and infeasible to predict for any adversary. The pair (C_i, R_i) forms a device-specific challenge–

response pair (CRP).

- Fuzzy Extractor Based Key Extraction: As raw PUF out puts are noisy and can differ slightly from one measurement to another, D_i extracts a stable cryptographic key using a fuzzy extractor. Let $(K_i, W_i) = \mathrm{FE.Extract}(R_i)$ for which K_i is a reproducible device secret key and W_i is helper data. In later reconstructions, the device may have to re-generate K_i by calculating $K_i = \mathrm{FE.Reproduce}(R_i', W_i)$, where R_i' is a new but noisy PUF response with the same challenge C_i. K_i is never sent in the clear and not permanently kept in memory on FDG or blockchain.

Table 1. Notations used in the CDIA-Fog framework

Notation	Description
D_i	i^{th} IoT device participating in authentication
$\mathrm{PUF}_i(\cdot)$, C_i, R_i	PUF of device D_i and its challenge–response pair generated during enrollment
W_i, K_i	Helper data and secret key derived from PUF response via fuzzy extractor
ID_i, $\mathrm{hash\_ref}(ID_i)$	Domain-bound device identity and its blockchain-registered hashed reference
DA, τ_A	Domain Authority and its digital signature for device registration verification
FDG	Federated Domain Gateway for intra- and cross-domain authentication management
BTL, $\mathcal{R}_i$, $\mathcal{L}_i, \mathcal{U}_i$	Blockchain Trust Ledger and records for registration, authentication, and updates
N_i, N_f, N_B	Random nonces generated by device and source/destination FDGs for freshness
T_i, T_A, T_B, T_r, T_c	Timestamps used in registration, authentication, and re-authentication phases
SK_D, SK_{CD}, SK_{CD}'	Intra-domain, cross-domain, and updated session keys
T_{CD}, H_B	Temporary cross-domain token and hash commitment for session derivation
K_{AB}	Shared symmetric key between federated domain authorities
SRL_i, α, β, γ, θ_1, θ_2	Security Risk Level, weighting factors, and decision thresholds
$ESL_i, \delta_1, \delta_2$	Energy Stress Level of device and adaptive decision thresholds
$h(\cdot)$	One-way cryptographic hash function
$\mathrm{Enc}_{K_{AB}}(\cdot)$	Symmetric encryption using inter-domain shared key K_{AB}
$\mathrm{FE.Extract}(\cdot)$, $\mathrm{FE.Reproduce}(\cdot)$	Fuzzy extractor functions for key derivation and reconstruction
$\mathrm{Sign}_{DA}(\cdot)$	Digital signature generated by the Domain Authority

- Domain Credential Derivation: The device autonomously derives a domain-bound identity token ID_i to be used for the subsequent authenticated protocols within this domain:$ID_i = h(K_i \,\|\, \mathrm{DA} \,\|\, T_0)$, where $h(\cdot)$ is a secure cryptographic hash function,DA denotes the identifier of the domain authority, and T_0 stands for the timestamp at whichthe enrollment was performed (or another epoch value). This scheme has the property that ID_i is (i) linked to a particular device and its home domain, and (ii) unlinkable from the domain if one does not have knowledge of K_i.
- Register Securely with FDG: Device D i shares the tuple ⟨C i, W i, ID i ⟩ with the FDG over a secure onboarding channel. You should note that with R_i, K_i are **not** revealed. The FDG saves the $\{C_i, W_i, ID_i\}$ into its secure local storage for D_i. This allows the FDG to later confirm that D_i is indeed correct by re-issuing C_i, and checking whether the reconstructed values derived from K_i are consistent, while never learning K_i itself.
- Blockchain Trust Record Publication: To support future cross-domain interoperability, the FDG generates a signed registration assertion for D_i:

$$\tau_i = \mathrm{Sign}_{\mathrm{DA}}\big(h(ID_i \,\|\, C_i \,\|\, W_i)\big), \tag{3}$$

Where $\mathrm{Sign}_{\mathrm{DA}}(\cdot)$ denotes the domain authority's digital signature. The FDG (on behalf of the domain) then commits a registration record to the Blockchain Trust Ledger (BTL):

$$\mathcal{R}_i = \big(\mathrm{DA}, \mathrm{hash\_ref}(ID_i), \tau_i\big), \tag{4}$$

Where $\mathrm{hash\_ref}(ID_i)$ is a hashed reference to ID_i rather than the raw value, preserving anonymity. This on-chain record enables other domains to verify that D_i is a legitimately enrolled device under DA, without exposing K_i, R_i, or linkable identifiers.

When the successful registration procedure has been completed, the local security state of the system is initialized as follows. Device D_i securely keeps and maintains the tuple C_i, W_i, ID_i in a safe tamper proof manner and permanently obliterates the raw PUF response R_i after successful derivation of secret key K_i, to ensure no hardware-specific information leaks out. At the same time, FGW saves above information in its trusted domain local database $\{C_i, W_i, ID_i, \tau_i\}$ for future authentication tasks. Moreover, the BTL retains a registered record $\mathcal{R}_i$ which constitutes an authoritative and tamper-proof evidence of device registration, and it can thus ensure secure cross-domain authentication for future encounters.

4.1.1. Phase II – Intra-Domain Authentication Phase

Once device D_i completes its registration the terminal can fully participate in communications within its home domain. The aim of this stage is to achieve mutual authentication between the IoT device and its corresponding FDG, and to establish a confidential integrity-protected channel, as well as a shared session key. It is based on lightweight cryptographic schemes, e.g. hash and symmetric key functions, to reduces the computation and communication cost. The process proceeds as follows.

- Authentication Request Initialization: When D_i wishes to communicate it will initiate an authentication request by creating a random nonce, N_i, and the current timestamp, T_i. Then, a temporary authentication token is calculated by the device: $Auth_i = h(K_i \,\|\, ID_i \,\|\, N_i \,\|\, T_i)$. Then the authentication request message is constructed as: $M_1 = \{ID_i, N_i, T_i, Auth_i\}$ and sent to FDG in secure channel.
- FDG Validation and Confirmation: Upon reception of M_1, the FDG retrieves its stored enrollment $\{C_i, W_i, ID_i\}$ for that device. It replays the PUF response and regenerates the key:$K_i' = \mathrm{FE.Reproduce}(\mathrm{PUF}_i(C_i), W_i)$.
- The FDG verifies the authenticity of the device by checking: $Auth_i \stackrel{?}{=} h(K_i' \,\|\, ID_i \,\|\, N_i \,\|\, T_i)$. If the verification holds true, the FDG considers D_i legitimate. It then generates its own random nonce N_f and computes a gateway authentication token: $Auth_f = h(K_i' \,\|\, N_f \,\|\, N_i \,\|\, T_i)$. The FDG transmits its response message: $M_2 = \{N_f, Auth_f\}$ to the device D_i.
- Mutual Authentication Confirmation: Upon reception of M_2, the device validates the FDG's authenticity by verifying:

$$Auth_f \stackrel{?}{=} h(K_i \,\|\, N_f \,\|\, N_i \,\|\, T_i). \tag{5}$$

If the equality holds, both parties mutually authenticate each other, confirming that neither M_1 nor M_2 were altered or replayed during transmission.

- Session Key Derivation: Upon mutual authentication, each party derivesthe shared session key that will be employed for secure communications: $SK_D = h(K_i \,\|\, N_i \,\|\, N_f \,\|\, T_i)$. And the session key SK_D used in each authentication process is domain-unique for keeping reciprocal confidentiality and integrity of future intra-domain communication. The key is rotated periodically, or in the presence of a high-security-risk context.
- Authentication Finalization: In order to finalize the authentification, D_i sends a short confirmation message: $M_3 = h(SK_D \,\|\, N_i \,\|\, N_f)$, to the FDG. On receiving M_3, the FDG checks validity by re-computing the hash with the cuttag key SK_D. In the case of success a match means that both parties have synchronized on the same session key, and this result is equivalent to completing mutual authentication.

After this phase, D_i and FDG are mutual possession of a fresh session key SK_D, from which they can derive to securely communicate data within the domain. This key can subsequently be employed to perform cross-domain verification in the second phase.

4.1.2. Phase III – Cross-Domain Authentication and Key Translation Phase

When an authorized device, say D_i, roams out of its home-domain $\mathcal{D}_A$ and enters into other administrative domain $\mathcal{D}_B$; it should be able to securely cross-over the domain boundary without initiating a re-authentication process from start. This stage is realized among the AKT, FDGs of two domains and BTL. The main objectives of this phase are threefold: (i) to ensure the validity of D_i in the target domain, (ii) confidential translation of session key from $\mathcal{D}_A$ to $\mathcal{D}_B$, and (iii) availability of both session continuity and forward secrecy across domains.

- Migration Trigger and Token Generation: Before D_i departs from $\mathcal{D}_A$, it notifies its home FDG_A of the intended migration by sending a migration request message:

$$M_4 = \{ID_i, \mathcal{D}_B, N_i, h(SK_D \,\|\, ID_i \,\|\, \mathcal{D}_B)\}, \tag{6}$$

Where N_i is a new random nonce generated by the device and SK_D is the last established intra-domain session key from Phase II. FDG_A verifies the integrity of the request using SK_D and generates a temporary interoperability token:

$$T_{CD} = \text{Enc}_{K_{AB}}\big(ID_i, h(SK_D \,\|\, N_i), \tau_A, T_A\big), \tag{7}$$

Where K_{AB} is a symmetric key shared between the domain authorities of $\mathcal{D}_A$ and $\mathcal{D}_B$, τ_A is the signature of the source domain authority DA_A, and T_A is the generation timestamp. The token T_{CD} is forwarded to the target domain FDG_B through the blockchain network.

- Blockchain-Based Token Verification: Upon receiving T_{CD}, FDG_B extracts the relevant registration record $\mathcal{R}_i$ from the Blockchain Trust Ledger (BTL):

$$\mathcal{R}_i = \big(\text{DA}_A, \text{hash\_ref}(ID_i), \tau_A\big), \tag{8}$$

And validates τ_A using the public key of DA_A. If the verification succeeds, FDG_B confirms that the device D_i is a legitimate entity from a trusted external domain. FDG_B then generates its own random nonce N_B and computes a hash commitment:

$$H_B = h(ID_i \,\|\, N_i \,\|\, N_B \,\|\, \mathcal{D}_A \,\|\, \mathcal{D}_B), \tag{9}$$

Which will be used in the key translation process.

- Adaptive Key Translation and Session Continuity: To maintain session continuity across domains, FDG_B derives a new cross-domain session key SK_{CD} using the Adaptive Key Translator (AKT):

$$SK_{CD} = h(SK_D \,\|\, N_i \,\|\, N_B \,\|\, H_B), \tag{10}$$

Where SK_D is the previous intra-domain key, and (N_i, N_B) ensure randomness and forward secrecy. The old key SK_D is immediately discarded to prevent backward key exposure. The AKT module ensures that SK_{CD} remains domain-specific and cannot be used in reverse for any prior sessions.

- Mutual Confirmation Between FDG_A and FDG_B: FDG_B sends a key translation confirmation message to FDG_A:

$$M_5 = \{ID_i, N_B, h(SK_{CD} \,\|\, ID_i \,\|\, N_B)\}, \tag{11}$$

Which allows FDG_A to verify that $\mathcal{D}_B$ has successfully received and derived the correct session key. Upon verification, FDG_A deletes all temporary credentials and migration tokens associated with D_i, ensuring that no stale keys remain in $\mathcal{D}_A$.

- Device–Target Domain Authentication: After FDG_B completes verification, it sends a challenge message to D_i: $M_6 = \{N_B, h(SK_{CD} \,\|\, N_B)\}$. The device computes $h(SK_{CD} \,\|\, N_B)$ using its local context and compares it with the received value. A successful match authenticates FDG_B as the legitimate target gateway. The device then replies with: $M_7 = h(SK_{CD} \,\|\, ID_i \,\|\, N_B \,\|\, N_i)$, confirming its authenticity to FDG_B and finalizing the cross-domain mutual authentication.

- Blockchain Update and Session Activation: Finally, FDG_B records the successful migration event in the Blockchain Trust Ledger:

$$\mathcal{L}_i = \big(\text{DA}_B, \text{hash\_ref}(ID_i), h(T_{CD} \,\|\, N_B \,\|\, T_B)\big), \tag{12}$$

Where T_B denotes the timestamp of the event. This entry serves as an auditable proof of cross-domain authentication and supports accountability across federated domains.

At the end of this phase, D_i successfully transitions to the new domain $\mathcal{D}_B$, securely establishing a fresh cross-domain session key SK_{CD} that enables continuous, authenticated communication without re-running a full registration cycle.

4.1.3. Phase IV – Secure Session Maintenance and Re-Authentication Phase

For domain$\mathcal{D}_B$, device D_i can continue to work in reality if there is a true x-domain policy authentication and key translation. This phase seeks to maintain a long, energy-efficient and context-aware interaction with (FDG_B) in safe way. At this stage, we propose adaptive re-authentication schemes that are based on two factors of security risk level (SRL) and energy stress level (ESL). These criterias are periodically calculated by the system and tailored dynamically to guarantee that the level of feedback authentication is strong enough for a particular work environment thereby providing enduring security with improved lifetime for devices.

- Continuous Session Monitoring : FDG_B observes and tracks the communications, environmental context and internal system state parameters of active sessions continuously. The device D_i will periodically send its remaining energy E_i and communication statistics to the FDG. This realization leads FDG_B to compute:

$$ESL_i = 1 - \frac{E_i}{E_{\text{max}}}, \tag{13}$$

Where E_{max} is the device's initial battery capacity. The value of ESL_i lies within the range $[0, 1]$, where values close to 1 indicate high energy stress. Simultaneously, the system calculates a *Security Risk Level (SRL)* score according to environmental conditions and detected anomalies:

$$SRL_i = \alpha \cdot R_{\text{mob}} + \beta \cdot R_{\text{anomaly}} + \gamma \cdot R_{\text{traffic}}, \tag{14}$$

Where α, β, and γ are weighting factors associated with mobility risk (R_{mob}), anomaly detection (R_{anomaly}), and traffic irregularities (R_{traffic}), respectively.

- Mode Selection for Re-Authentication: Based on the computed SRL_i and ESL_i values, the FDG_B determines the most suitable re-authentication mode using a rule-based decision function:

$$\mathcal{M}(SRL_i, ESL_i) = \begin{cases} \text{Session Extension Mode}, & SRL_i < \theta_1 \text{ and } ESL_i < \delta_1, \\ \text{Fast Re-Authentication Mode}, & \theta_1 \le SRL_i < \theta_2, \\ \text{Full Re-Authentication Mode}, & SRL_i \ge \theta_2 \text{ or } ESL_i \ge \delta_2, \end{cases} \tag{15}$$

Where (θ_1, θ_2) and (δ_1, δ_2) are threshold parameters predefined by the domain authority. This adaptive logic enables CDIA-Fog to dynamically switch between lightweight and comprehensive authentication depending on the risk–energy trade-off.

- Session Extension Mode (Low SRL and Low ESL): In a stable, low-risk context, the FDG_B and D_i extend the session without exchanging new authentication messages. The session key SK_{CD} is locally updated using a lightweight hash function:

$$SK'_{CD} = h(SK_{CD} \,\|\, T_r), \tag{16}$$

Where T_r is the current rekeying timestamp. This process preserves confidentiality while consuming minimal computational energy, maintaining continuous secure communication for low-risk scenarios.

- Fast Re-Authentication Mode (Moderate SRL or Moderate ESL): When moderate risk or medium energy depletion is detected, the FDG_B triggers a fast re-authentication exchange to verify session freshness. The device generates a random nonce N_i' and computes:

$$Auth_i' = h(SK_{CD} \,\|\, N_i' \,\|\, ID_i), \tag{17}$$

and sends the message:

$$M_8 = \{ID_i, N_i', Auth_i'\}. \tag{18}$$

Upon receipt, FDG_B verifies $Auth_i'$, generates a new nonce N_B', and derives an updated key:

$$SK_{new} = h(SK_{CD} \,\|\, N_i' \,\|\, N_B'), \tag{19}$$

then replies with:

$$M_9 = \{N_B', h(SK_{new} \,\|\, ID_i)\}. \tag{20}$$

Both entities replace SK_{CD} with SK_{new}, ensuring freshness and continued confidentiality.

- High SRL or High ESL (Full Re-Authentication Mode): In this mode, when high-risk is detected (e.g., anomaly behavior, suspected attack), or there is a spike in energy consumption indicating a change in user identity, the system goes through the entire re-authentication procedure. The loop iterates over the main steps of Phase II, i.e., PUF-based verification and blockchain token validation, in order to regain trust under new credentials. It generates a new session key SK_{CD}^* as below:

$$SK_{CD}^* = h(K_i \,\|\, N_i \,\|\, N_B \,\|\, T_c), \tag{21}$$

Where T_c represents the full re-authentication timestamp. Once the new session is confirmed, all prior keys are securely deleted from both D_i and FDG_B.

- Logging and Blockchain Record Update: After each re-authentication event, the FDG_B generates a record entry and submits it to the Blockchain Trust Ledger:

$$\mathcal{U}_i = \big(\text{DA}_B, \text{hash\_ref}(ID_i), h(SK_{new} \,\|\, SRL_i \,\|\, ESL_i \,\|\, T_c)\big), \tag{22}$$

Where $\mathcal{U}_i$ serves as an immutable, auditable proof of session maintenance. The record aids in later verification, accountability, and forensics in case of abnormal events.

At the conclusion of this phase, D_i sustains continuous, secure, and adaptive communication with FDG_B, ensuring robust protection and efficient energy utilization throughout its operational lifecycle across the fog network.

4.2. Trust Aging and On–Off Attack Resistance

To avoid sleeper-node attacks and the On–Off behavior in a long horizon, this framework accounts for a time-decay and variance-aware trust update mechanism under SRL evaluations (see Fig. 3). Instead of keeping a constant trust after some long period of behaving well, the trust will quickly adapt to more recent happenings and colloquial level of silence time over time. Define the current trust score of node i at timestep t as $T_i(t)$. As we have established trust update rule now defined as:

$$T_i(t+1) = \lambda \cdot T_i(t) + (1-\lambda) \cdot B_i(t) - \rho \cdot I_i(t) \tag{23}$$

Where:

- $\lambda \in (0,1)$ is the trust memory factor controlling historical influence,
- $B_i(t)$ is the normalized recent behavior score derived from authentication correctness and protocol compliance,

- $I_i(t)$ is the measured inactivity duration factor,
- ρ is the inactivity decay coefficient.

With this formulation, trust decreases over time while a node is in an inactive state and can reduce sleeper attacks where an adversary builds up trust and later exploit it after lying idle for a period of time.

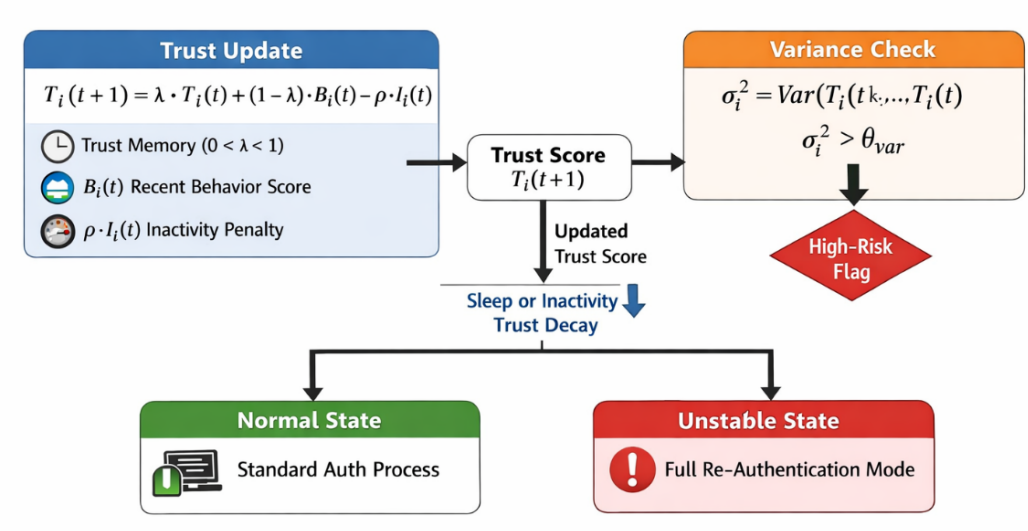

Fig. 3. Trust aging and On–Off attack resistance mechanism

In order to further prevent On–Off attacks, in which a malicious node switches from benign to malicious behavior to keep the trust level acceptable, a variance based stability check is added. The short-window trust variance is defined as:

$$\sigma_i^2 = \mathrm{Var}\big(T_i(t-k), \ldots, T_i(t)\big) \tag{24}$$

If the trust variance exceeds a predefined threshold θ_{var}, the node is classified as unstable:

$$\sigma_i^2 > \theta_{\mathrm{var}} \;\Rightarrow\; \text{High-Risk Flag} \tag{25}$$

Even when average trust score greater than High-Risk Flagged nodes which naturally go to Full Re-Authentication Mode. This prevents abusers from exploiting a good/bad pattern on the adaptive auth measures. And because it is based on time-decay trust aging plus variance-triggered escalation, which only receives high-energy attacks with limited computational overhead, the framework may also resist not just sleeper-node attacks but On–Off attack models as well.

5. Security Analysis

In this section, we present the security analysis of the proposed CDIA-Fog-based authentication framework which includes a formal and an informal security analysis. The formal analysis is performed in the Random Oracle Model (ROM) and the informal analysis shows that CDIA-Fog is resilient against common attacks of IoT–fog systems. This part ends with a comparative assessment of the security properties of related schemes.

5.1. Formal Security Proof under the Random Oracle Model

We securely analyze the proposed protocol in Random Oracle Model (ROM) that assumes hash functions are random oracles, to verify the correctness and security guarantees of our new protocol. This proof is centred around two core attributes: session key secrecy, and mutual authentication.

Game Definition

Let $\mathcal{A}$ be a probabilistic polynomial-time adversary that interacts with protocol participants D_i and FDG under the following game-based model:

- $\mathsf{Execute}(D_i, FDG)$: allows $\mathcal{A}$ to observe an honest protocol execution between D_i and FDG.
- $\mathsf{Send}(P, M)$: sends an arbitrary message M to participant P and obtains the corresponding response.
- $\mathsf{Reveal}(P)$: returns the session key of participant P if already established.
- $\mathsf{Corrupt}(D_i)$: gives $\mathcal{A}$ access to all stored parameters of D_i except the PUF structure and raw key K_i.
- $\mathsf{Test}(P)$: outputs either the real session key SK or a random value of equal length, with $\mathcal{A}$ attempting to distinguish them.

The adversary's advantage is defined as:

$$Adv_{\mathcal{A}} = \left|2 \times Pr[b' = b] - 1\right|, \tag{26}$$

Where b is the random bit chosen by the challenger and b' is the adversary's guess. A protocol is said to achieve *semantic security of session key secrecy* if $Adv_{\mathcal{A}}$ is negligible.

Security Proof Sketch We construct a sequence of games to prove that the adversary's advantage remains negligible.

Game $\mathbf{G}_0$: The real execution of CDIA-Fog where all entities operate honestly. The adversary's success probability is Pr_0.

Game $\mathbf{G}_1$: The challenger simulates hash queries as random oracles. Since $h(\cdot)$ is modeled as a random oracle, the probability of finding two identical hash outputs for different inputs is negligible, i.e., $\Pr_1 - \Pr_0 \leq q_h/2^{\ell}$, where q_h is the number of hash queries and ℓ is the hash length.

Game $\mathbf{G}_2$: The adversary attempts to impersonate a legitimate device by forging authentication tokens. To succeed, $\mathcal{A}$ must generate a valid $Auth_i = h(K_i \,\|\, ID_i \,\|\, N_i \,\|\, T_i)$ without knowledge of K_i. Since K_i is derived from the PUF output, the probability of successful forgery is bounded by ϵ_{PUF}, where ϵ_{PUF} is the collision probability of two distinct PUF responses.

Game $\mathbf{G}_3$: The adversary performs a key compromise attempt via Reveal queries. Even with exposure of SK_D or SK_{CD}, the next session key is computed as a fresh hash over nonces and timestamps, ensuring forward secrecy. Hence, $\Pr_3 - \Pr_2 \leq 1/2^{\ell}$.

Game $\mathbf{G}_4$: The adversary attempts to distinguish the real key from a random string in the Test query. Because of the pseudo-random nature of $h(\cdot)$, the advantage is negligible: $Adv_{\mathcal{A}} \leq q_s/2^{\ell}$, where q_s is the number of Send queries.

Conclusion: The overall advantage of $\mathcal{A}$ across all games is negligible:

$$Adv_{\mathcal{A}} \leq \frac{q_h + q_s + 1}{2^{\ell}} + \epsilon_{PUF}, \tag{27}$$

Proving that CDIA-Fog achieves **session key indistinguishability** and is secure under the Random Oracle Model.

5.2. Informal Security Analysis

The informal analysis demonstrates how CDIA-Fog withstands a wide range of attacks commonly observed in multi-domain IoT–fog environments.

- Mutual verification: Every authentication message is linked with device-specific PUF derived keys and fresh nonces so that both D_i and the FDG mutually validate each other. If the given K_i is not owned by an unauthorized device, they are unable to produce a valid $Auth_i$ or a $Auth_f$.

- Resistance to Replay Attack: All protocol messages contain time-stamps partially bound with unique nonce (N_i, N_f, N_B). Replayed messages will never pass the freshness check because timestamps and nonces are pasted together.
- Impersonation Attack Immunity: PUF based keys are derived from hardware and cannot be easily extracted or cloned. An adversary is therefore unable to spoof a genuine device or FDG unless the precise hardware response generated by the PUF is known.
- Resistance to Man-in-the-Middle (MITM) Attack: The Authorization Tokens are securely bound with nonces and domain identifiers. The message has not been modified during transmission, a condition that results in authentication failure.
- Forward secrecy/backward secrecy: Session keys (SK_D, SK_{CD}, SK'_{CD}) are generated by random nonces and timestamps. Revelation of a session key does not affect past or future sessions because the extracted value is only as significant as the a priori probability used for Key Derivation and, as such, it provides no assistance in breaking an earlier or subsequent session.
- Inter-Domain Forgery Resistance: The block chain verification process will result in that the interoperability token (T_{CD}) is legitimate if it is signed and included in the record by trusted domain authorities. Due to the hash commitment and timestamp binding, it is not possible to replay/re-use tokens across domains.
- Node Capture and Insider Attacks Resistance: The captured node provides only the public knowledge (C_i, W_i, ID_i) and does not disclose the internal PUF structure. Insider adversaries are unable to regenerate K_i or calculate legitimate session keys without the real PUF response.
- Anonymity and Unlinkability: Each device uses one-time interoperability tokens and temporary identities. On-the-blockchain the references are stored only in hashed form, $\mathrm{hash\_ref}(ID_i)$, so they can not be exploited by external adversaries to link cross-domain devices.
- Blockchain Trust Ledger: All the participants registering, authenticating and re-authenticating are recorded immutably in our Blockchain ledger, responsible for maintaining accountability of all authentication events upon successful validation.

5.3. Automated Symbolic Verification Considerations

Beyond the formal security proof in the Random Oracle Model (ROM), it was also considered there to verify that protocol message exchanges were secure under a symbolic adversary setting relating to Dolev–Yao, where an attacker can eavesdrop, modify, inject and re-play messages on insecure channels. This organized message-flow verification assures that all authentication tokens and session keys in CDIA-Fog are tied to fresh nonces, timestamps, and device-specific secrets so as to achieve resistance against replay (or man-in-the-middle) attack at the level of protocol logic.

Model checking both secrecy and authentication properties was chosen to be performed using an automated protocol verification tool, e.g. AVISPA or Scyther. The full protocol is not directly encodable without abstraction, because the model includes both PUF behavior and blockchain-aided trust records features that are not already supported by standard symbolic verification libraries. The primitive core-authentication and key-establishment subprotocol (ignoring PUF hardware internals and blockchain storage semantics) is however amenable to symbolic analysis.

So ROM-based formal security proof is adopted as the main validation modality of this work and automatic verification based on AVISPA/Scyther to an abstracted protocol model as future work. We present a planned extension that will add a complementary machine-checked validation for secrecy and authentication goals with symbolic attack assumptions.

5.4. Comparative Security Evaluation

Table 2 presents a comparative analysis of CDIA-Fog against existing authentication schemes, including PCAP [25], TCALAS [26], and UAP [50], considering standard cryptographic and operational security attributes. As stated in Table 2, CDIA-Fog compares favourably with the existing protocols

since it combines hardware-rooted PUF security, decentralized blockchain auditability, and cross-domain interoperability. The incorporation of adaptive re-authentication provides energy-efficient means and yet strong resistance against replay, impersonation as well as MITM attack. As a result, CDIA-Fog has provided a balanced and provably secure design that can fulfill the rigorous demands of future IoT and fog computing environments.

Table 2. Comparison of security properties with existing authentication schemes

Security Property	PCAP	TCALAS	UAP	CDIA-Fog
Mutual Authentication	✓	✓	✓	✓
Replay Attack Resistance	✓	✓	✓	✓
Impersonation Resistance	✓	✓	✓	✓
MITM Attack Resistance	✓	✓	✓	✓
Forward / Backward Secrecy	✓	✓	✓	✓
Anonymity and Unlinkability	×	✓	✓	✓
Cross-Domain Interoperability	×	×	×	✓
Blockchain Auditability	×	×	×	✓
PUF-Based Hardware Security	✓	×	✓	✓
Energy-Aware Adaptation	×	×	×	✓
Formal Proof under ROM	×	×	×	✓

6. Performance Evaluation

This section evaluates the performance of the proposed **CDIA-Fog** protocol in terms of computational, communication, and energy overheads, comparing it with existing lightweight authentication schemes including PCAP [25], TCALAS [26], and UAP [50]. The analytical results are further supported by simulation-based validation in a 5G–IoT environment.

6.1. Evaluation Environment and Assumptions

The performance evaluation of CDIA-Fog was conducted under a representative IoT–fog deployment setup summarized in Table 3. IoT devices were modeled using a Raspberry Pi 4 platform, while fog gateways were implemented on an Intel i5-class system. All cryptographic primitives were implemented using OpenSSL with SHA-256 as the hash function. The average execution times of primitive operations were measured and used as normalized benchmarks: hash operation ($T_h = 0.0082$ ms), symmetric encryption/decryption ($T_x = 0.021$ ms), and PUF challenge–response evaluation ($T_p = 0.013$ ms). These primitive timings were consistently applied across all compared schemes to ensure fair comparison. Energy consumption per cryptographic operation is estimated using:

$$E = V \times I \times t, \tag{28}$$

Where $V = 5$ V is the supply voltage, $I = 0.12$ A is the average current draw, and t is the measured execution time.

6.2. Computational Cost Analysis

The total computational cost of each authentication scheme is computed as the sum of all cryptographic operations executed during one full authentication session between an IoT device and a fog gateway:

$$T_{comp} = n_h \times T_h + n_x \times T_x + n_p \times T_p, \tag{29}$$

Where n_h, n_x, and n_p represent the number of hash, symmetric, and PUF operations, respectively.

For CDIA-Fog:

$$T_{comp}^{CDIA-Fog} = (6 \times T_h) + (2 \times T_x) + (1 \times T_p) = 0.0928 \text{ ms}. \tag{30}$$

Table 3. Evaluation environment and primitive timing assumptions

Component	Specification / Value
IoT Device Platform	Raspberry Pi 4, 1.5 GHz ARM Cortex-A72, 4 GB RAM
Fog Gateway Platform	Intel i5-class CPU, 1.8 GHz, 8 GB RAM
Crypto Library	OpenSSL
Hash Function	SHA-256
Hash Time (T_h)	0.0082 ms
Symmetric Crypto Time (T_x)	0.021 ms
PUF Evaluation Time (T_p)	0.013 ms
Supply Voltage (V)	5 V
Average Current (I)	0.12 A

For comparison, $T_{comp}^{PCAP} = 0.0420$ ms, $T_{comp}^{TCALAS} = 1.5104$ ms, $T_{comp}^{UAP} = 0.0826$ ms. Although CDIA-Fog performs additional operations due to blockchain validation and adaptive key translation, the increase in computation is negligible relative to its added security and interoperability features.

6.3. Computational Cost Analysis and Comparison

This is the overhead in computational terms, which represents the summation of time taken to complete all cryptographic operations for a full-fledged authentication exchange between an IoT device (D_i) and its FDG served. Since our IoT devices of interest are 5G capable, we design the Communication Efficient Public Key Cryptography protocol to be resource friendly; CDIA-Fog employs light primitives hashing, symmetric encryption and PUF evaluations. Different from the common construction which is built on bilinear pairing and modular exponentiation, CDIA-Fog is with lower computational cost and stronger security.

- Analytical Model: We have T_h execution time of one hash, T_x executing time of an encryption/decryption, and T_p execution time of a (the single) PUF challenge–response evaluation. If n_h, n_x and n_p are the number of hash, symmetric operation and PUF function in one authentication session then the total computational delay is represented as:

$$T_{\text{comp}} = n_h \times T_h + n_x \times T_x + n_p \times T_p. \tag{31}$$

- Parameter Assumptions: All simulations are carried out using the OpenSSL cryptographic library on IoT and fog node hardware specimen. On the IoT device (Raspberry Pi 4) and fog node (Intel i5 processor), we execute with mean execution times: $T_h = 0.0082$ms, $T_x = 0.0210$ms, and $T_P = 0.0130$ ms. These results are in line and essentially the same as other known performance tables for light-weight cryptographic primitives.
- Computation for CDIA-Fog: In CDIA-Fog, each authentication session involves: $n_h = 6, \quad n_x = 2, \quad n_p = 1.$

$$\begin{aligned} T_{\text{comp}}^{\text{CDIA-Fog}} &= (6 \times 0.0082) + (2 \times 0.0210) + (1 \times 0.0130) \\ &= 0.0928 \text{ ms}. \end{aligned} \tag{32}$$

  This result confirms that CDIA-Fog introduces minimal delay, even while incorporating blockchain verification and adaptive key translation.
- Comparative Computational Results: To comprehend efficiency, the number of computations of CDIA-Fog is compared with other typical competitors in current state-of-the-art schemes: PCAP [25], TCALAS [26] and UAP [50]. The cost of each protocol is determined by using the same set of device parameters and primitive operation benchmarks. The results are reported in Table 4.

It can be observed from Fig. 4 that TCALAS achieves the largest computational delay, as this scheme utilizes the bilinear pairing in its implementation and therefore is less appropriate for IoT devices. PCAP has the lowest complexity, but provides no support of operation and auditability.

Table 4. Computational cost comparison of authentication schemes

Scheme	Operations Considered	T_{comp} (ms)	Relative Cost	Complexity Level
PCAP [25]	$3T_h + 1T_x$	0.0420	1.0×	Low
TCALAS [26]	Pairing & Hash Ops	1.5104	12.3×	High
UAP [50]	$5T_h + 1T_x + 1T_p$	0.0826	2.0×	Medium
CDIA-Fog (Proposed)	$6T_h + 2T_x + 1T_p$	**0.0928**	**2.2**×	**Medium-Low**

Better security than in PCAP is achieved by UAP with PUF-based authentication, however they are still not cross-domain. CDIA-Fog adds only a small overhead to the computation (0.01 ms of that of UAP) and brings substantial benefits in area like blockchain-based trust management or adaptive energy-aware authentication. In brief, CDIA-Fog retains the lightweight computational overhead while seriously improving the security and functionality. It's processing time is 0.0928 ms which still meets the real time authentication requirement for fog in 5G and viable to be implemented on embedded IoT hardware.

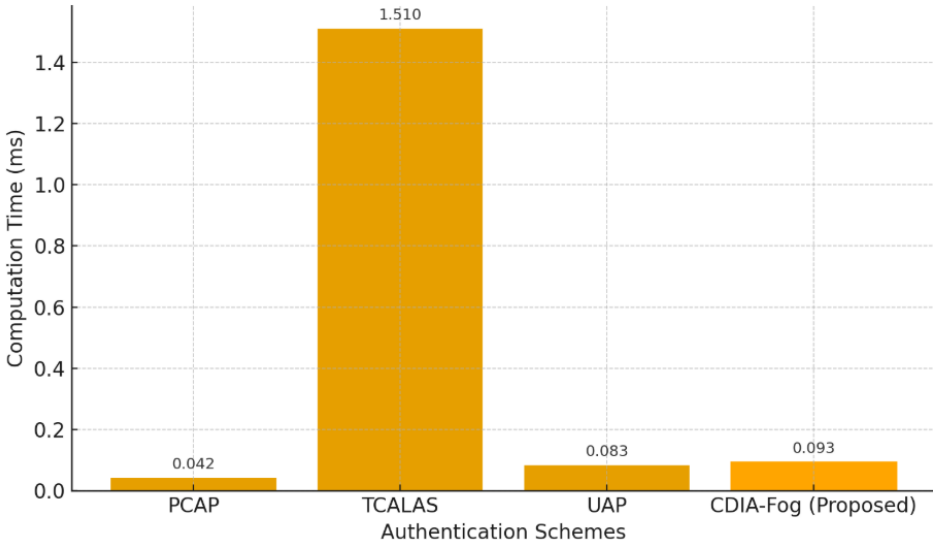

Fig. 4. Computational cost comparison of authentication schemes

6.4. Communication Cost Analysis and Comparison

The communication cost is defined as the sum of data sent over an entire authentication session between the IoT device and the FDG, including request, response and confirmation messages. In 5G-based IoT paradigms, which feature high node density with low bandwidth availability, small message size is a prerequisite to achieve lower latency and energy consumption.

- Analytical Model: The total communication overhead T_{comm} is determined by the cumulative size of all parameters exchanged during one full authentication procedure:

$$T_{\text{comm}} = \sum_{k=1}^{m} L_k, \tag{33}$$

Where L_k is the bit length of k^{th} transmitted parameter, and m is the number of parameters per session. For the sake of convenience, here we suppose that the bit length of terms are as follows: $L_{id} = 128$bits, $L_n = 128$bits, $L_t = 64$bits, $L_h = 256$bits, $L_s = 512$ bits. Therefore, the total communication complexity is proportional to the number of identifiers, timestamps, nonces and cryptographic outputs in each message.

- Computation for CDIA-Fog: The proposed **CDIA-Fog** protocol involves three main message exchanges during one authentication cycle:
  1. Device → FDG: $\{ID_i, N_i, T_i, Auth_i\}$,
  2. FDG → Device: $\{N_f, Auth_f\}$,
  3. Device → FDG (acknowledgment): $\{Conf_i\}$.

Accordingly, the total transmitted data can be expressed as:

$$T_{\text{comm}}^{\text{CDIA-Fog}} = 3(L_n + L_t + L_h) + L_s = 1728 \text{ bits}. \tag{34}$$

This size includes authentication tokens, timestamps, and blockchain signature data. The blockchain verification step adds negligible data since only hashed references ($\text{hash\_ref}(ID_i)$) are broadcast to the distributed ledger.

- Comparative Communication Overheads: For a fair comparison, the same message structure assumptions are applied to baseline schemes PCAP [25], TCALAS [26], and UAP [50]. The results are summarized in Table 5.

Table 5. Communication cost comparison of authentication schemes

Scheme	Message Exchanges	T_{comm} (bits)	Relative Size
PCAP [25]	2 messages	1568	1.00×
TCALAS [26]	3 messages	1680	1.07×
UAP [50]	3 messages	1840	1.17×
CDIA-Fog (Proposed)	3 messages	**1728**	**1.10**×

From Fig. 5, CDIA-Fog achieves a moderate communication overhead of **1728 bits** per session. The transmission size of CDIA-Fog is slightly larger than PCAP and TCALAS but considerably smaller than UAP and brings substantial functional improvements, including cross-domain compatibility and blockchain auditability. It is possible due to: using lightweight short-lived tokens instead of heavy digital certificates; compressing hashed references for PUF-based identity data; and maximizing the recognized message and acknowledgment combinations. In general, CDIA-Fog allows lightweight communication that is convenient for 5G-enabled IoT deployment due to its low scalability, latency and high dependability. Its average transmission size balances the costs of communication and offers additional advanced cross-domain features.

6.5. Energy Cost Analysis and Comparison

Energy consumption is a critical metric for resource-constrained IoT devices operating in fog-assisted 5G environments. In the proposed CDIA-Fog framework, energy overhead arises primarily from cryptographic processing during authentication and re-authentication. This subsection quantifies the energy cost per authentication session and discusses how CDIA-Fog reduces long-term energy drain through adaptive re-authentication.

- Energy Model: The instantaneous energy consumed by a device executing a cryptographic operation is modeled as: $E = V \times I \times t$, where V is the operating voltage (in volts), I is the average current draw (in amperes), and t is the execution time (in seconds). For a complete authentication session, the total energy cost is therefore:

$$E_{\text{total}} = V \times I \times T_{\text{comp}}, \tag{35}$$

Where T_{comp} is the total computational time. In our evaluation model, we assume: $V = 5$ V, $I = 0.12$ A, which is representative of a Raspberry Pi-class IoT node under moderate cryptographic load.

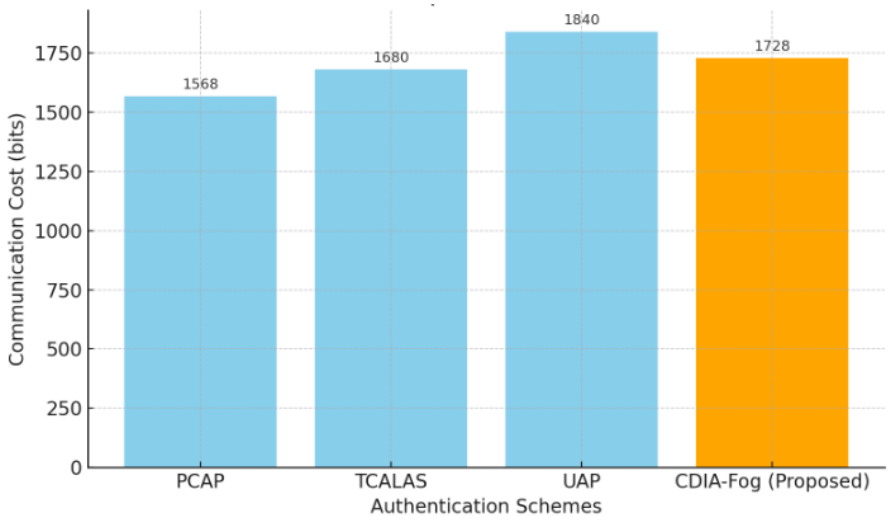

Fig. 5. Communication cost comparison of authentication schemes

- Energy Cost per Session for CDIA-Fog: From the computational cost analysis, the total processing delay for one full authentication in CDIA-Fog is: $T_{\text{comp}}^{\text{CDIA-Fog}} = 0.0928 \text{ ms} = 0.0928 \times 10^{-3}$ s. Substituting this into (35), we obtain:

$$\begin{aligned} E_{\text{total}}^{\text{CDIA-Fog}} &= 5 \times 0.12 \times (0.0928 \times 10^{-3}) \\ &= 0.6 \times 0.0928 \times 10^{-3} \\ &= 55.68 \times 10^{-6} \text{ J} \\ &= 55.68 \ \mu\text{J}. \end{aligned} \tag{36}$$

Consequently, a typical full authentication in CDIA-Fog consists of tens of microjoules that are affordable and even tolerable for the battery-powered edge devices.

Relative Energy Can be Comparison: Assuming the same voltage/current model and T_{comp} measured for each scheme, the relative per-session energy cost is proportional to T_{comp}: $E \propto T_{comp}$. Accordingly:

$$E^{\text{PCAP}} \sim 0.0420 \text{ ms} \quad (\approx 1.0\times), \tag{37}$$

$$E^{\text{UAP}} \sim 0.0826 \text{ ms} \quad (\approx 2.0\times), \tag{38}$$

$$E^{\text{CDIA-Fog}} \sim 0.0928 \text{ ms} \quad (\approx 2.2\times), \tag{39}$$

$$E^{\text{TCALAS}} \sim 1.5104 \text{ ms} \quad (\approx 12.3\times). \tag{40}$$

Table 6 summarizes the estimated per-session energy cost, normalized to PCAP as the $1.0\times$ baseline. The absolute μJ values are estimated using the same voltage/current model; the relative energy column is normalized to PCAP. Minor rounding differences are due to truncation.

Table 6. Per-Session energy cost comparison

Scheme	T_{comp} (ms)	Energy / Session (μJ)	Relative Energy
PCAP [25]	0.0420	≈ 25.2	$1.0\times$
TCALAS [26]	1.5104	≈ 906.2	$12.3\times$
UAP [50]	0.0826	≈ 49.6	$2.0\times$
CDIA-Fog (Proposed)	**0.0928**	**55.7**	**2.2**$\times$

- Adaptive Re-Authentication Advantage: While the full-session cost of CDIA-Fog (0.0928 ms / 55.7 μJ) is slightly higher than UAP for *initial* authentication, CDIA-Fog significantly reduces *long-term* energy consumption via its adaptive, context-aware maintenance phase:
  - The Session Extension Mode (low SRL, low ESL) refreshes the session key using a single hash update instead of re-running a full mutual authentication.
  - The Fast Re-Authentication Mode uses only hash and nonce checks, avoiding PUF re-evaluation and avoiding blockchain interaction.
  - Full re-authentication is invoked only when the Security Risk Level (SRL) or Energy Stress Level (ESL) exceeds predefined thresholds.

  Therefore, although the first authentication in CDIA-Fog costs slightly more than UAP, the amortized cost over multiple re-authentication cycles is lower. In other words, CDIA-Fog trades a small increase in initial computation for a reduced energy drain over time, especially in mobile cross-domain scenarios where naive schemes would force full re-authentication on every handover.
- Interpretation: In summary, the comparative study suggests that TCALAS is not suitable for IoT-category hardware because of its high computational costand dependence on bilinear pairing operations. While PCAP has low computational overhead, it lacks key capabilities such as cross-domain support, distributed ledger based auditability and adaptive re-authentication. According to the results obtained, UAP achieves an acceptable per session energy cost but does not efficiently manage re-authentication across multi-domains. However, CDIA-Fog delivers secure cross-domain session persistence with just a moderate energy overhead for primal authentication, and then achieves lower long-term energy consumption by employing SRL/ESL-aware adaptiver e-authentication.

Overall, CDIA-Fog is energy-feasible for constrained devices and is specifically optimized for long-lived, mobile, multi-domain deployments rather than single-domain static deployments.

6.6. Comparison with Lightweight ECC-Based Authentication Schemes

We also enhance our evaluation by comparing CDIA-Fog with existing state-of-the-art lightweight Elliptic Curve Cryptography (ECC) based authentication schemes in recent IEEE IoT and fog security literature. ECC based protocols are generally efficient with regard to the public key schemes, yet have a larger computational overhead than hash dedicated constructions as in scalar multiplications.

According to benchmarks on Raspberry Pi-like IoT boards, one ECC scalar multiplication takes about 0.30–0.60 ms depending on curve parameters and the used implementation libraries. The majority of lightweight ECC authentication schemes need 2 to 4 scalar multiplications per session, as well as hash computations, as shown in Table 7.

This comparison illustrates that despite being more efficient than traditional public-key algorithms, ECC-based lightweight authentication methods incur significantly greater computational delay due to the scalar multiplication operation. In contrast, CDIA-Fog is hash and symmetric primitive based with only a single PUF evaluation, achieving authentication delay of sub-millisecond. While PCAP provides relatively low computation raw cost, it lacks of features like cross-domain interworking, blockchain-based auditability and adaptive re-authentication. As a result, CDIA-Fog achieves a good trade-off between low computational overhead and added security features. From the presented experimental results, we show that our proposal not only can achieve much lower device-side delay than ECC-based solutions but also offer stronger interoperability capability.

6.7. Limitations

While secure and efficient cross-domain authentication with adaptive energy-aware re-authentication is illustrated through CDIA-Fog, some limitations need to be addressed.

- First, the assessment is conducted through analytical formulation and controlled benchmarking rather than experience in large-scale deployment. Although it identified the type of hardware

devices used in IoT–fog, assumed some network characteristics (e.g., wide area latency and packet loss) as well as devices' heterogenity due to different locations and types were not modelled completely.

Table 7. Comparison with lightweight ecc-based authentication schemes

Scheme Type	Core Crypto	Device Cost (ms)	Comm. Size (bits)	Cross-Domain Support
Lightweight ECC Auth (2023–24 refs)	ECC + Hash	0.80–2.40	2200–3200	Limited
UAP (PUF+ECC Hybrid)	ECC + PUF	≈0.60–0.90	≈2000	No
PCAP (Hash-based)	Hash + XOR	0.042	1568	No
CDIA-Fog (Proposed)	Hash + Sym + PUF	0.093	1728	Yes

- Second, the PUF-based design assumes that IoT devices have access to Physical Unclonable Function (PUF) support. In reality, not all commercial IoT hardware platforms provide standardized PUF interfaces yet and hence may limit direct applicability without hardware support or secure element inclusion.
- Third, the question of blockchain trust layer when assuming permissioned blockchain is introduced with released throughput facts. Performance may very according to consensus configuration, number of validators, and deployment topology. No complete prototype integration with a production blockchain was performed in this paper.
- Symbolic protocol verification tools (e.g., AVISPA or Scyther) are not fully utilized due to the complex modeling of PUF behavior and trust records from blockchain. The current validation is based on Random Oracle Model proof and structured attack reasoning.
- Finally, scalability under very high cross-domain paging rates was analytically estimated however not heavily simulated. Future work will involve the deployment of a prototype, an automated formal verification tool and scalability evaluation based on real traffic patterns.

7. Conclusion and Future Work

This paper introduced a cross-domain-compatible authentication scheme for 5G-based IoT and fog computing systems. The proposed CDIA-Fog architecture is able to facilitate secure device migration across heterogeneous administrative fog domains by employing PUF-based device identity, blockchain-supported trust records, adaptive key translation and risk–energy aware re-authentication. In contrast to domain-constrained lightweight/low-overhead constructs as well as computation-heavy ECC or blockchain-per-session schemes, the model targets a lightweight cryptographic processes with an event-driven interaction with ledgers.

Rigorous analysis under the Random Oracle Model and structured attack scenarios show that it resists replay, impersonation, and man-in-the-middle attacks while offering anonymity, forward secrecy and cross-domain session unforgeability. The experimental results on the popular IoT and fog devices indicate that our protocol can achieve sub-millisecond delay (0.0928 ms) in the authentication, moderate overhead (1728 bits) of communication and low per-session energy consumption (55.7 µJ). In comparison to ECC-based lightweight authentication baselines, the proposed scheme reduces device-side operations offering more general interoperability and auditability properties.

If a fog gateway is compromised, the trust level can be recovered by revocation of domain authority and blockchain supported record checking between domains to restrict the influence among different domains. However, this work is limited to controlled benchmarking and analytically modeling, and

large-scale deployment behavior still needs to be confirmed. In the future, we plan to develop automatic symbolic verification for security protocols, deploy on larger scale prototype systems, integrate with post-quantum primitives and perform tests of scalability in high-mobility multi-domain IoT scenarios.

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: This work was supported by the Deanship of Scientific Research, Vice President for Graduate Studies and Scientific Research, King Faisal University, Kingdom of Saudi Arabia (Grant No. KFU262213).

Acknowledgment: This work was supported by the Deanship of Scientific Research, Vice President for Graduate Studies and Scientific Research, King Faisal University, Kingdom of Saudi Arabia (Grant No. KFU262213).

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] R. Mohawesh *et al*., "Cybersecurity challenges and solutions in 5g-enabled internet of things," *Discover Computing*, vol. 29, no. 29, 2026, https://doi.org/10.1007/s10791-026-09926-w.

[2] N. Xu, T. Xie, K. Ding and K. Gai, "Blockchain-based Cross-domain Authentication Techniques in Decentralized Identity," *2025 IEEE 11th Conference on Big Data Security on Cloud (BigDataSecurity)*, pp. 64-70, 2025, https://doi.org/10.1109/BigDataSecurity66063.2025.00008.

[3] J. B. Awotunde, A. E. Adeniyi, P. B. Falola, K. Srinivasan, G. S. Chauhan, and R. Jadon, "Fog computing and internet of things technology for throughput and latency in the smart sensor network," *Advances in Fog Computing and the Internet of Things for Smart Healthcare*, pp. 249–280, 2026, https://doi.org/10.1016/B978-0-443-33441-2.00005-7.

[4] W. Chia Chuan, S. Ul Arfeen Laghari, S. Manickam, E. Ashraf and S. Karuppayah, "Challenges and Opportunities in Fog Computing Scheduling: A Literature Review," in *IEEE Access*, vol. 13, pp. 14702-14726, 2025, https://doi.org/10.1109/ACCESS.2024.3525261.

[5] R. Mustafa, N. I. Sarkar, M. Mohaghegh, and S. Pervez, "A cross-layer secure and energy-efficient framework for the internet of things: a comprehensive survey," *Sensors*, vol. 24, no. 22, p. 7209, 2024, https://doi.org/10.3390/s24227209.

[6] V. Gugueoth, S. Safavat, S. Shetty, and D. Rawat, "A review of iot security and privacy using decentralized blockchain techniques," *Computer Science Review*, vol. 50, p. 100585, 2023, https://doi.org/10.1016/j.cosrev.2023.100585.

[7] H. S. Msayer, H. L. Swadi, and H. M. AlSabbagh, "Enhancement spectral and energy efficiencies for cooperative noma networks," *Iraqi Journal for Electrical and Electronic Engineering*, vol. 19, no. 1, pp. 57–61, 2023, https://doi.org/10.37917/ijeee.19.1.7.

[8] W. Fei, H. Ohno, and S. Sampalli, "A systematic review of iot security: Research potential, challenges, and future directions," *ACM computing surveys*, vol. 56, no. 5, pp. 1–40, 2023, https://doi.org/10.1145/3625094.

[9] I. E. Carvajal-Roca, Z. Guan, H. Wang, and Z. Wan, "A lightweight group authentication framework for cross-domain internet of things," in *International Conference on Security and Privacy in Communication Systems*, pp. 25–46, 2026, https://doi.org/10.1007/978-3-031-94458-1_2.

[10] A. Sharma and K. Bhushan, "A comprehensive survey on iot security: Challenges, security issues, and countermeasures," *Computer Science Review*, vol. 59, p. 100839, 2026, https://doi.org/10.1016/j.cosrev.2025.100839.

[11] M. A. Al-Shareeda, A. A. H. Ghadban, A. A. H. Glass, E. M. A. Hadi, and M. A. Almaiah, "Efficient implementation of post-quantum digital signatures on raspberry pi," *Discover Applied Sciences*, vol. 7, no. 597, 2025, https://doi.org/10.1007/s42452-025-07201-z.

[12] M. A. Faleh, A. M. Abdulsada, A. A. Alaidany, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Secre-men: A lightweight quantum-resilient authentication framework for iot-edge networks," *Journal of Robotics and Control (JRC)*, vol. 6, no. 4, pp. 1681–1692, 2025, https://doi.org/10.18196/jrc.v6i4.26006.

[13] A. N. Zulkifli, N. F. F. Mohamed, M. M. Qasim, and N. A. A. Bakar, "Prototyping and usability evaluation of road safety education courseware for primary schools in malaysia," *International journal of interactive mobile technologies*, vol. 15, no. 6, pp. 32–47, 2021, https://doi.org/10.3991/ijim.v15i06.20609.

[14] A. Bisht and V. Khaitan, "Stochastic network model for performance analysis of cloud-fog-enabled intelligent vehicular network," *Cluster Computing*, vol. 28, no. 806, 2025, https://doi.org/10.1007/s10586-025-05514-7.

[15] 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," in *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 5, pp. 4795-4812, 2025, https://doi.org/10.1109/TDSC.2025.3553868.

[16] M. Seifelnasr, R. AlTawy and A. Youssef, "A Conditional Privacy-Preserving Protocol for Cross-Domain Communications in VANET," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 4, pp. 5251-5263, 2025, https://doi.org/10.1109/TITS.2025.3527409.

[17] M. Domb, C. Balaji, S. Menaka, A. Gayathri, and S. Joshi, "Securing 5g networks by mitigating cybersecurity risks for transformative applications," *International Journal of Interactive Mobile Technologies*, vol. 19, no. 11, p. 277, 2025, https://doi.org/10.3991/ijim.v19i11.54519.

[18] G. Premalatha, A. Devi, D. Palani, A. Amirthasaravanan, P. Dharanyadevi and S. Hariharan, "Blockchain-Enabled Handover Authentication for 5G Vehicular Networks: Fog Computing Paradigm," *2025 10th International Conference on Communication and Electronics Systems (ICCES)*, pp. 1540-1545, 2025, https://doi.org/10.1109/ICCES67310.2025.11337211.

[19] F. M. Alnahwi, H. L. Swadi and A. S. Abdullah, "Design and Simulation of Single and 2×2 MIMO Circularly Polarized Patch Antennas with a Pair of Chip Resistors for 5G Applications," *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pp. 488-493, 2022, https://doi.org/10.1109/ISMSIT56059.2022.9932653.

[20] M. M. Qasim, A. N. Zulkifli, M. Ahmad, M. Omar, and J. A. A. Bakar, "Educating parents in dealing with childhood obesity through the use of the bmi monitor app," *Man In India*, vol. 96, no. 1-2, pp. 367–376, 2015, https://faculty.uobasrah.edu.iq/uploads/publications/1624463432.pdf.

[21] M. M. Qasim, J. M. Altmemi, A. H. Abd Ali, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Ca-hbca: A software engineering framework for secure, scalable, and adaptive healthcare blockchain systems," *Journal of Robotics and Control*, vol. 6, no. 4, pp. 2052–2063, 2025, https://doi.org/10.18196/jrc.v6i4.26643.

[22] E. Alkafaji and H. L. Swadi, "Multi-objective optimization of traffic signal timings for minimizing waiting time, co2 emissions, and fuel consumption at intersections," *Kufa Journal of Engineering*, vol. 15, no. 3, pp. 21–31, 2024, https://doi.org/10.30572/2018/KJE/150302.

[23] B. A. Shtayt, J. M. Altmemi, K. A. Abdullah, M. A. Al-Shareeda, M. A. Almaiah, and R. Shehab, "Lightweight lattice-based multi-domain authentication protocol with real-time revocation and aggregated verification for vehicular communication," *Journal of Robotics and Control*, vol. 6, no. 5, pp. 2228–2238, 2025, https://doi.org/10.18196/jrc.v6i5.26644.

[24] M. M. Qasim, M. Ahmad, M. Omar, A. N. Zulkifli, and J. Bakar, "Persuasive technology and mobile healthcare: A critical review," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 10, no. 10, 2018, https://www.researchgate.net/profile/Mustafa-Qasim-2/publication/330041681_Persuasive_Technology_and_Mobile_Healthcare_A_Critical_Review/links/5c2b6ff6458515a4c7057ae0/Persuasive-Technology-and-Mobile-Healthcare-A-Critical-Review.pdf.

[25] C. Pu and Y. Li, "Lightweight Authentication Protocol for Unmanned Aerial Vehicles Using Physical Unclonable Function and Chaotic System," *2020 IEEE International Symposium on Local and Metropolitan Area Networks*, pp. 1-6, 2020, https://doi.org/10.1109/LANMAN49260.2020.9153239.

[26] 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," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903-6916, 2019, https://doi.org/10.1109/TVT.2019.2911672.

[27] A. Shahidinejad and J. Abawajy, "An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for iot," *ACM Computing Surveys*, vol. 56, no. 7, pp. 1–38, 2024, https://doi.org/10.1145/3645087.

[28] J. A. Alzubi, N. R. Lavuri, K. Dharavath, N. Nallameti, S. Venugopal and P. Palanisamy, "A secure authentication and task offloading model using blockchain-assisted hybrid serial learning in multiaccess edge computing for vehicular ad hoc networks sector," *International Journal of Communication Systems*, vol. 39, no. 3, p. e70382, 2026, https://doi.org/10.1002/dac.70382.

[29] Y. Miao, K. Gai and L. Zhu, "Blockchain-assisted multi-keyword searchable provable data possession for cloud storage," *Science China Information Sciences*, vol. 69, no. 132101, 2026, https://doi.org/10.1007/s11432-024-4409-6.

[30] Q. Liu, B. Li, K. Ding and Y. Zhang, "DMPF-CADA: A Confidence-Driven Adaptive Device Authentication With Dual-Modal Physical Fingerprints in Cloud–Edge IIoT," in *IEEE Internet of Things Journal*, vol. 13, no. 7, pp. 13512-13526, 2026, https://doi.org/10.1109/JIOT.2026.3655090.

[31] A. M. Sheikh, M. R. Islam, M. H. Habaebi, S. A. Zabidi, A. R. b. Najeeb and M. Baloch, "Securing iot networks using machine learning-resistant physical unclonable functions (pufs) on edge devices," *Network*, vol. 6, no. 1, p. 6, 2026, https://doi.org/10.3390/network6010006.

[32] H. Zhang, Y. Pan, J. Zuo and T. Zhang, "Physically unclonable function (puf) structure by self-assembly," in *11th International Symposium on Advanced Optical Manufacturing and Testing Technologies*, vol. 13992, pp. 513–517, 2026, https://ui.adsabs.harvard.edu/link_gateway/2026SPIE13992E..1MZ/doi:10.1117/12.3092476.

[33] Y. Wei *et al*., "Wearable-compatible all-optical physical unclonable functions with hybrid deep learning-based authentication," *Laser & Photonics Reviews*, vol. 20, no. 10, p. e02874, 2026, https://doi.org/10.1002/lpor.202502874.

[34] H. A. Ali *et al*., "A privacy-preserving framework for iot using behavior obfuscation and differential privacy in blockchain–cloud architectures," *Journal of Robotics and Control*, vol. 6, no. 6, pp. 2613–2627, 2025, https://doi.org/10.18196/jrc.v6i6.27593.

[35] S. Mushtaq, M. Mohsin and M. M. Mushtaq, "A systematic literature review on the implementation and challenges of zero trust architecture across domains," *Sensors*, vol. 25, no. 19, p. 6118, 2025, https://doi.org/10.3390/s25196118.

[36] K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5g/6g networks: Principles, challenges, and the role of machine learning in the context of o-ran," *Computer Networks*, vol. 217, p. 109358, 2022, https://doi.org/10.1016/j.comnet.2022.109358.

[37] S. Ahmadi, "Zero trust architecture in cloud networks: Application, challenges and future opportunities," *Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports*, vol. 26, no. 2, pp. 215–228, 2024, https://doi.org/10.9734/jerr/2024/v26i21083.

[38] M. Yoon, J. Seo, J. Lee and K. Cho, "Design and Implementation of a 5G Security Testbed Based on Zero Trust Architecture," *2024 15th International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 2190-2192, 2024, https://doi.org/10.1109/ICTC62082.2024.10826685.

[39] A. O. Ojo, "Adoption of zero trust architecture (zta) in the protection of critical infrastructure," *Path of Science: International Electronic Scientific Journal*, vol. 11, no. 1, pp. 5001–5009, 2025, http://dx.doi.org/10.22178/pos.113-2.

[40] S. M. M. Ali, "Artificial intelligence in zero trust architecture for 5g and 6g networks: a systematic literature review," *Ammattikorkeakoulujen opinnäytetyöt ja julkaisut*, 2025, https://www.theseus.fi/bitstream/handle/10024/908381/Ali_Syed_Muhammad_Muneeb.pdf?sequence=2&isAllowed=y.

[41] N. Kumar, S. Prajapat, P. Kumar and R. Ali, "Q-blockauth: blockchain-enabled quantum authentication scheme for secure communication in sixth-generation internet of nano medical things networks," *Cluster Computing*, vol. 29, no. 74, 2026, https://doi.org/10.1007/s10586-025-05866-0.

[42] M. S. Almadani, S. Alotaibi, H. Alsobhi, O. K. Hussain and F. K. Hussain, "Blockchain-based multi-factor authentication: A systematic literature review," *Internet of Things*, vol. 23, p. 100844, 2023, https://doi.org/10.1016/j.iot.2023.100844.

[43] D. Li, W. Peng, W. Deng and F. Gai, "A Blockchain-Based Authentication and Security Mechanism for IoT," *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, pp. 1-6, 2018, https://doi.org/10.1109/ICCCN.2018.8487449.

[44] M. Zhaofeng, M. Jialin, W. Jihui and S. Zhiguang, "Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment," in *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2116-2123, 2021, https://doi.org/10.1109/JIOT.2020.3037733.

[45] S. Magesh, S. Varadhan, K. A. S. Stephen, V. B. R. Amalarajan, and A. Benita, "Fog-iot architecture with blockchain integrated model for electronic health records in healthcare systems," in *Advances in Fog Computing and the Internet of Things for Smart Healthcare*,pp. 185–210, 2026, https://doi.org/10.1016/B978-0-443-33441-2.00002-1.

[46] Z. Cao, X. Wen, S. Ai, H. Cao and W. Shang, "Lightweight authentication scheme for resource-constrained devices in iiot," *IET Communications*, vol. 19, no. 1, p. e70039, 2025, https://doi.org/10.1049/cmu2.70039.

[47] E. Mashhour, H. A. Khamis, M. Joorabian, S. G. Seifossadat and S. H. Hammadi, "Emission Reduction for a Home in Iraq Utilizing Geothermal System Supplied by Isolated Photovoltaic-Wind-Diesel Generator Using Genetic Algorithm Optimization," *2025 Fifth National and the First International Conference on Applied Research in Electrical Engineering (AREE)*, pp. 1-6, 2025, https://doi.org/10.1109/AREE63378.2025.10880240.

[48] A. Changtor, T. Maneerat, P. Rattanasrisuk, K. Tangtanawirut and S. Fugkeaw, "A Secure and Lightweight IIoT Data Authentication Using PUF-Based in IoT Fog-Assisted Cloud," *2025 17th International Conference on Knowledge and Smart Technology (KST)*, pp. 40-45, 2025, https://doi.org/10.1109/KST65016.2025.11003299.

[49] M. A. Akram, A. N. Mian, A. K. Biswas, S. Kumari and C. -M. Chen, "Privacy-Preserving Lightweight LoRaWAN Authentication Protocol for IoT Applications," in *IEEE Internet of Things Journal*, vol. 12, no. 20, pp. 42790-42802, 2025, https://doi.org/10.1109/JIOT.2025.3593886.

[50] C. Liu, T. Huang and M. Ma, "UAP: A System Authentication Protocol for UAV Relay Communication by UAV-Assisted," in *IEEE Open Journal of Vehicular Technology*, vol. 6, pp. 1539-1550, 2025, https://doi.org/10.1109/OJVT.2025.3567079.

[51] V. K. Bathalapalli, S. P. Mohanty, E. Kougianos, B. K. Baniya and B. Rout, "Pufchain 2.0: Hardware-assisted robust blockchain for sustainable simultaneous device and data security in smart healthcare," *SN Computer Science*, vol. 3, no. 344, 2022, https://doi.org/10.1007/s42979-022-01238-2.

[52] S. Ashraf Chaudhry, A. Irshad, B. A. Alzahrani, A. Alhindi, M. Shariq and A. Kumar Das, "TS-PAID: A Two-Stage PUF-Based Lightweight Authentication Protocol for Internet of Drones," in *IEEE Access*, vol. 13, pp. 1458-1469, 2025, https://doi.org/1109/ACCESS.2024.3523352.

[53] S. G. Aarella, V. P. Yanambaka, S. P. Mohanty and E. Kougianos, "Fortified-edge 2.0: Advanced machine-learning-driven framework for secure puf-based authentication in collaborative edge computing," *Future Internet*, vol. 17, no. 7, p. 272, 2025, https://doi.org/10.3390/fi17070272.

[54] D. Li, Y. Ren, D. Liu, Y. Guo, Z. Guan and J. Liu, "PIPP: A Practical PUF-Based Intellectual Property Protection Scheme for DNN Model on FPGA," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 71, no. 2, pp. 912-916, 2024, https://doi.org/10.1109/TCSII.2023.3309105.

[55] O. Alruwaili, M. Tanveer, F. M. Alotaibi, W. Abdelfattah, A. Armghan and F. M. Alserhani, "Securing the iot-enabled smart healthcare system: A puf-based resource-efficient authentication mechanism," *Heliyon*, vol. 10, no. 18, p. e37577, 2024, https://www.cell.com/action/showPdf?pii=S2405-8440%2824%2913608-0.

[56] V. K. V. V. Bathalapalli, V. P. Yanambaka, S. Mohanty and E. Kougianos, "Pufshield: A hardware-assisted approach for deepfake mitigation through puf-based facial feature attestation," in *Proceedings of the Great Lakes Symposium on VLSI 2024*, pp. 676–681, 2024, https://doi.org/10.1145/3649476.3660394.

[57] P. P. Aung, S. Aslam, C. W. Chong and W. Chen, "Puf-based lightweight security subsystems for iot hardware: A concept," in *International Conference on Intelligent Manufacturing and Robotics*, pp. 391–400, 2024, https://doi.org/10.1007/978-981-96-3949-6_31.

[58] V. Malamas, P. Kotzanikolaou, K. Nomikos, C. Zonios, V. Tenentes and M. Psarakis, "HA-CAAP: Hardware-Assisted Continuous Authentication and Attestation Protocol for IoT Based on Blockchain," in *IEEE Internet of Things Journal*, vol. 12, no. 11, pp. 15650-15666, 2025, https://doi.org/10.1109/JIOT.2025.3530775.

[59] M. Wang, L. Rui, Y. Yang, Z. Gao and X. Chen, "A Blockchain-Based Multi-CA Cross-Domain Authentication Scheme in Decentralized Autonomous Network," in *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2664-2676, 2022, https://doi.org/10.1109/TNSM.2022.3180357.

[60] Y. Zhang, B. Li, J. Wu, B. Liu, R. Chen and J. Chang, "Efficient and Privacy-Preserving Blockchain-Based Multifactor Device Authentication Protocol for Cross-Domain IIoT," in *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22501-22515, 2022, https://doi.org/10.1109/JIOT.2022.3176192.

[61] W. Wang, N. Hu and X. Liu, "BlockCAM: A Blockchain-Based Cross-Domain Authentication Model," *2018 IEEE Third International Conference on Data Science in Cyberspace (DSC)*, pp. 896-901, 2018, https://doi.org/10.1109/DSC.2018.00143.

[62] H. Zhang and F. Zhao, "Cross-domain identity authentication scheme based on blockchain and pki system," *High-Confidence Computing*, vol. 3, no. 1, p. 100096, 2023, https://doi.org/10.1016/j.hcc.2022.100096.

[63] B. Liu, K. Yu, C. Feng and K.-K. R. Choo, "Cross-domain authentication for 5g-enabled uavs: A blockchain approach," in *Proceedings of the 4th ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond*, pp. 25–30, 2021, https://doi.org/10.1145/3477090.3481053.

[64] D. Luo, G. Sun, H. Yu and M. Guizani, "Blockchain-Based Cross-Domain Authentication With Dynamic Domain Participation in IoT," in *IEEE Internet of Things Journal*, vol. 12, no. 5, pp. 5385-5395, 2025, https://doi.org/10.1109/JIOT.2024.3486331.

[65] A. Karmegam, A. Tomar and S. Tripathi, "Blockchain-based cross-domain authentication in a multi-domain internet of drones environment," *The Journal of Supercomputing*, vol. 80, pp. 27095–27122, 2024, https://doi.org/10.1007/s11227-024-06447-5.

[66] J. Cui, Y. Zhu, H. Zhong, Q. Zhang, C. Gu and D. He, "Efficient Blockchain-Based Mutual Authentication and Session Key Agreement for Cross-Domain IIoT," in *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 16325-16338, 2024, https://doi.org/10.1109/JIOT.2024.3351892.

[67] W. Wang, S. Zhang, G. Liu, and Y. Zhao, "A blockchain-based cross-domain authentication scheme for unmanned aerial vehicle-assisted vehicular networks," *World Electric Vehicle Journal*, vol. 16, no. 4, p. 199, 2025, https://doi.org/10.3390/wevj16040199.

[68] R. Li, J. Cui, J. Zhang, L. Wei, H. Zhong and D. He, "Blockchain-Assisted Revocable Cross-Domain Authentication for Vehicular Ad-Hoc Networks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 5, pp. 4593-4606, 2025, https://doi.org/10.1109/TDSC.2025.3549748.

[69] J. Desikan, S. K. Singh and A. Jayanthiladevi, "Bachaav: machine learning-augmented human-ai and cryptographic architecture for threat detection in iot-enabled oil and gas industrial networks," *International Journal of Information Technology*, pp. 1–12, 2025, https://doi.org/10.1007/s41870-025-02650-6.

[70] A. Raj and S. D. Shetty, "Iot eco-system, layered architectures, security and advancing technologies: a comprehensive survey," *Wireless Personal Communications*, vol. 122, no. 2, pp. 1481–1517, 2022, https://doi.org/10.1007/s11277-021-08958-3.

[71] D. Aldossary, E. Aldahasi, T. Balharith and T. Helmy, "A systematic literature review on load-balancing techniques in fog computing: Architectures, strategies, and emerging trends," *Computers*, vol. 14, no. 6, p. 217, 2025, https://doi.org/10.3390/computers14060217.

[72] S. M. Rajagopal, M. Supriya and R. Buyya, "Leveraging blockchain and federated learning in edge-fog-cloud computing environments for intelligent decision-making with ecg data in iot," *Journal of Network and Computer Applications*, vol. 233, p. 104037, 2025, https://doi.org/10.1016/j.jnca.2024.104037.

[73] S. Kanthimathi, R. Sivakami and B. Indira, "Modified cryptosystem-based authentication protocol for internet of things in fog networks," *Concurrency and Computation: Practice and Experience*, vol. 37, no. 4-5, p. e70024, 2025, https://doi.org/10.1002/cpe.70024.

[74] M. Alhafnawi, A. Abu-Ein, H. B. Salameh, Y. Jararweh and O. Al-Hazaimeh, "Intelligent dynamic bandwidth allocation for real-time iot in fog-based optical networks," *Simulation Modelling Practice and Theory*, vol. 142, p. 103126, 2025, https://doi.org/10.1016/j.simpat.2025.103126.

[75] G. D'aniello and L. Fotia, "Blockchain and ai-based methods for trust management in iot: A comprehensive survey," *Internet of Things*, vol. 34, p. 101755, 2025, https://doi.org/10.1016/j.iot.2025.101755.

[76] O. A. Khashan, "Trust-based fog-blockchain model for scalable authentication in smart cities," *Computer Networks*, vol. 264, p. 111278, 2025, https://doi.org/10.1016/j.comnet.2025.111278.

[77] F. Tong, X. Chen, C. Huang, Y. Zhang and X. Shen, "Blockchain-Assisted Secure Intra/Inter-Domain Authorization and Authentication for Internet of Things," in *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7761-7773, 2023, https://doi.org/10.1109/JIOT.2022.3229676.

[78] N. C. Gowda, A. B. Malakreddy, Y. Vishwanath and K. Radhika, "Mltped-bfc: Machine learning-based trust prediction for edge devices in the blockchain enabled fog computing environment," *Engineering Applications of Artificial Intelligence*, vol. 139, p. 109518, 2025, https://doi.org/10.1016/j.engappai.2024.109518.

[79] R. Kashikar, "Quantum Communication-AI Interface for Real-Time Translation and Secure Transmission in Multilingual IoT Networks," *2024 IEEE International Conference on Future Machine Learning and Data Science (FMLDS)*, pp. 175-178, 2024, https://doi.org/10.1109/FMLDS63805.2024.00041.

[80] F. Javed, E. Zeydan, J. Mangues-Bafalluy, K. Dev and L. Blanco, "Blockchain for Federated Learning in the Internet of Things: Trustworthy Adaptation, Standards, and the Road Ahead," in *IEEE Communications Standards Magazine*, vol. 10, no. 1, pp. 56-64, 2026, https://doi.org/10.1109/MCOMSTD.2025.3593809.

[81] X. Zhang, *Data processing for effective federated learning in future networks*, A PhD dissertation submitted to the University of Bristol in accordance with the requirements of the degree of DOCTOR IN PHILOSOPHY in the Faculty of Engineering, 2025, https://research-information.bris.ac.uk/ws/portalfiles/portal/460803624/Dan_PhD_unsigned.pdf.