SECRE-MEN: A Lightweight Quantum-Resilient Authentication Framework for IoT-Edge Networks

May Adnan Faleh [1], Ali M. Abdulsada [2], Ali A. Alaidany [3], Mahmood A. Al-Shareeda [4*], Mohammed Amin Almaiah [5], Rami Shehab [6]

[1, 4] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, 61001, Basra, Iraq

[2] Biomedical Engineering Department, College of Engineering, University of Warith Al Anbiyaa, Karbala, 56001, Iraq

[2] Technical Institute of Karbala, Al Furat Al Awsat Technical University, Najaf, Iraq

[3] Fuel and Energy Techniques Engineering Department, Shatt Al-Arab University College, Basra ,Iraq

[5] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman 11942, Jordan

[6] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa 31982, Saudi Arabia

Email: [1] afrah.alasady@stu.edu.iq, [2] ali.abdalsadaa.ikr24@atu.edu.iq, [3] ali.ahmmad@sa-uc.edu.iq, [4] mahmood.alshareedah@stu.edu.iq, [5] m.almaiah@ju.edu.jo, [6] ralali@kfu.edu.sa

Corresponding Author

***Abstract*—The wide 6G-IoT and Mobile Edge Computing (MEC) deployments give rise to severe concerns in authentication, revocation and protection against quantum-post and side channel attacks. In this paper, SECRE-MEN (Secure and Efficient Cryptographic Revocable Authentication for MEC enabled Networks) is presented to be a lightweight and scalable authentication architecture specifically designed for the resource limited IoT systems. SECRE-MEN consists of three main parts: (1) Masked Cryptographic Techniques that are used to randomise elliptic curve operations, thereby mitigate side-channel attacks, (2) VCs, providing support for digitally-signed, lightweight authentication, without requiring the use of bulky certificates, and (3) a Bloom filter-based RDB, which is distributed across multiple MEC nodes, to allow for fast, memory-efficient revocation checks. To enable future-proof security post-quantum cryptography (PQC) is included in SECRE-MEN by lattice-based schemes, such as Kyber and Dilithium, which may incur additional computational cost on ultra-low-power platforms according to the trade-off introduced in this paper. Effort experiments show that the proposed RAM-MENAMI decreases 29.3% the computation cost, and reduces 21.8% the communication budget and improve 20.3% of power efficiency in comparison with the RAM-MEN. In addition, SECRE-MEN is resistant against impersonation, MITM, replay and quantum attacks, as well as allows for dynamic revocation and secure synchronization among MEC nodes. This places SECRE-MEN as an effective toolkit for cybersecurity of massive IoT-MEC networks in the era of the evolving 6G.**

***Keywords*—*Masked Cryptographic Techniques; Post-Quantum Authentication; Bloom Filter Revocation; MEC Security; PUF-Based IoT Authentication*.**

I. INTRODUCTION

With the fast-paced deployment of Internet of Things (IoT) [1]–[4] and Mobile Edge Computing (MEC) [5]–[9] in 6G networks, unique challenges of the security, privacy, and authentication are posed. As billions of interconnected devices are deployed in smart cities [10]–[12], healthcare [13], and industrial automation [14]–[16], lightweight, scalable, and secure authentication mechanisms are critical. Traditional authentication methods utilize established techniques such as Elliptic Curve Cryptography (ECC) [17]–[21], Public Key Infrastructure (PKI) [22]–[25], and symmetric cryptographic protocols [26]–[28]. Nevertheless, they have high computational complexity, susceptibility to quantum attack [29]–[32], and exposure to side-channel attack [33]–[41].

Moreover, real-time revocation of compromised IoT devices is an open problem as existing revocation mechanisms depend on centralized databases which raises lookup time and scalability issues. New lightweight authentication protocols focused on resource constraint criteria, like RAM-MEN [42], have proposed authentication based on PUFs [43] and key agreements based on ECC to meet the computational limitations of IoT devices. However, these schemes have significant drawbacks — they have a high latency for authentication, are not proved resistant to side-channel attacks, and do not include an efficient revocation mechanism [44]–[47]. Moreover, the development of quantum computing represents a substantial threat to classical ECC-based authentication methods as they may be susceptible to Shor's Algorithm, which poses a challenge for their long-term security in 6G networks [48]–[50].

Contemporary lightweight authentication protocols, like RAM-MEN, proposed PUF-based authentication and ECC-based key agreements to work on as restricted computation vs resource-constrained IoT entities. Nonetheless, these schemes suffer from significant drawbacks like high authentication latency, no protection from side-channel attacks, and no efficient revocation scheme. Furthermore, with the rise of quantum computing, traditional ECC-based authentication schemes can potentially be shattered using Shor's Algorithm, which poses a threat to long-term security in 6G networks.

To overcome these challenges, this paper presents SECRE-MEN (Secure and Efficient Cryptographic Revocable Authentication for MEC-enabled Networks), a new lightweight authentication framework that mitigates these aforementioned issues in IoT-MEC scenario with improved security, efficiency, and scalability. SECRE-MEN incorporates four critical security improvements to address the shortcomings of existing authentication measures. To start, it specializes Masked Cryptographic Techniques to defend against side-channel attack which include masked ECC computations, which makes power analysis impossible, and cryptography operations remain immune from leakage based attacks. In the second part, it relies on Verifiable Credentials (VCs) in place of classical ECC authentication payloads offering light-weight, digitally signed approach for authentication and consequently reducing communication overheads and thus ensuring authentication. Third, SECRE-MEN utilizes an MEC-Based Revocation Database (RDB) to implement a Bloom filter-based revocation mechanism for fast and scalable revocation lookup, which greatly reduces authentication latency against traditional Certificate Revocation Lists (CRLs). Last but not the least, SECRE-MEN features Post-Quantum Security Enhancements, keying in with Lattice-Based Cryptographic solutions like Kyber and Dilithium to prevent the unforgiving advancements around quantum computing from infiltrating security. SECRE-MEN's strong authentication framework combined with high security has provided robust security optimizations for the practical 6G IoT applications.

The key contributions of this paper are as follow:

- Proposes SECRE-MEN, a lightweight, quantum-resilient authentication system that combines masked cryptographic methods, Verifiable Credentials (VCs), and multi-access edge computing (MEC) based revocation for improving security efficiency. Prevents side-channel attacks by applying random masking to ECC calculations.
- We propose a MEC-based Revocation Database (RDB) which is scalable and employs the lookup of a Bloom filter which minimizes confirmation time for revocation and increases IoT security.
- The detailed performance evaluation indicates that SECRE-MEN outperforms RAM-MEN and other existing authentication mechanisms in terms of authentication speed, energy efficiency, and revocation scalability.

The rest of this paper is organized as follows: The related work is discussed in Sec. II, where existing authentication schemes are analyzed and their limitations. Section III introduces the SECRE-MEN framework and its security extension and cryptographic design. Section IV presents a security analysis that examines the resilience of SECRE-MEN to MITM, replay, impersonation, and quantum attacks. Section V: Performance Evaluation: Computational cost, communication overhead, and revocation efficiency. Last but not least, Section VI closes the paper and describes future research directions.

II. Related Work

In this section, we will review recent authentication mechanisms for smart grid and IoT-enabled networks with an emphasis on security, efficiency, and cryptographic techniques.

Some research studies [51]–[61] have been proposed authentication mechanism for IoT. Meanwhile those studies [62]–[68] have been proposed authentication mechanism for edge networks. While, some authentication mechanism that proposed [69]–[74] for IoT-enabled edge networks

Mahmood et al. [75] introduced a lightweight authentication scheme for smart grid communication based on Elliptic Curve Cryptography (ECC). This scheme improves message integrity and authentication with low computational overhead [76]. It is however still not resistant against quantum attacks, nor does it currently feature a dynamic revocation mechanism for compromised devices. ECC efficiency in constrained environments is underscored in the study but adequate side-channel resistance is not mentioned

Abbasinezhad et al. [77] developed a hardware-software enhanced smart grid communication security using ECC-based authentication. Based on the weaknesses of previously proposed ECC-based schemes, the authors propose a more secure way of authenticating for man-in-the-middle (MITM) and replay attacks. However, the scheme is still susceptible to side-channel attacks and does not provide verifiable credential (VC)-based authentication for better privacy [78].

Chen et al. [79] proposed hybrid of bilinear map pairing for authentication scheme (Pauth) for secure communication in smart grids. The protocol provides mutually-authentication, secret key agreement, and message integrity. It also provides private key agility and forward secrecy [80]. However, with only improved computational efficiency, the scheme is still vulnerable against quantum attacks, and fails to consider MEC-based revocation of compromised devices.

With respect to the security of smart grids, Kumari 'et al. [81] provided a lightweight authentication and key agreement protocol for the smart grid that achieves mutual authentication and session key establishment. The proposed scheme lowers computational and communication costs along with handling against cyber threats for smart grid systems [82]. However, it does not implement post-quantum cryptography (PQC), and lacks revocation mechanisms making it vulnerable to compromised device reuse attacks.

RAM-MEN [42] employed these solutions to achieve mutual authentication and tiny communication overhead by integrating PUF-based authentication, ECC, and ASCON encryption for IoT-MEC Environments in 6G Networks [83]. It is resistant to replay, MITM, and impersonation attacks but is vulnerable to side-channel attacks, quantum threats, and is not equipped with a dynamic revocation mechanism. It uses traditional ECC, thus it can be attacked with post-quantum cryptanalysis.

The current authentication methods in smart grid and IoT-MEC([42], [75], [77], [79], [81], [84], [85]) propose lightweight cryptographic operations with low computational overhead and mutual authentication. However, these schemes have serious security vulnerabilities, making them unsuitable for 6G-enabled edge computing environments. None of the reviewed works provide strong countermeasures from side-channel attacks (power analysis, timing attacks, fault injections, etc.). Moreover, the latest advancements in quantum computing threaten ECC-based authentication but such schemes do not provide any PQC mechanism to cushion themselves against Shor's Algorithm threats. Dynamic revocation mechanism is another important research gap. Current protocol lacks to revoke compromised IoT devices when credential is compromised, as compromised devices can still access even after credential compromise. While RAM-MEN enhances the efficiency of authentication through PUF-based authentication and ASCON encryption, it is still vulnerable to side channel attacks, doesn't offer quantum resistance, and does not have an MEC-based revocation framework. To fill in these gaps while keeping the authentication secure, SECRE-MEN strengthens the authentication process with masked cryptography (to protect against side-channel attacks), post-quantum cryptography (to protect against quantum attacks), and a MEC-based revocation database (to identify and deactivate compromised devices). In doing so, SECRE-MEN helps ensure a holistic and future-proof authentication framework for the 6G IoT-edge networks.

III. Proposed SECRE-MEN Mechanism

SECRE-MEN is a secure, efficient, and scalable authentication framework for IoT-enabled edge networks in 6G. Fig. 1 shows the system model of SECRE-MEN mechanism. To do so, it unifies masked cryptography, Verifiable Credentials (VCs), and a MEC-based Revocation Database (RDB), bypassing fundamental security flaws in current authentication models. The framework is divided into five consecutive phases covering the secure deployment of devices, their registration, mutual authentication of the communicating parties, session key agreement as well as dynamic revocation of the compromised device.

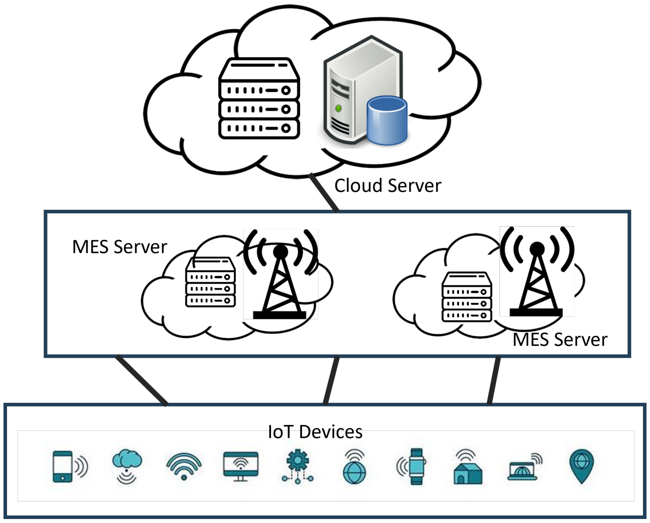

Fig. 1. System Model

The initial phase (MEC Server Deployment Phase) facilitates the secure initialization of the MEC server through PUF based authentication and masked ECC key generation to avoid impersonation and side channel attacks. Phase 2: IoT Device Registration Phase: Each IoT device is securely registered, and the RA issues a Verifiable Credential (VC) digitally signed, which serves as a privacy-preserving authentication token. Phase 1, Device Attestation Phase, offers mutual authentication and secure key establishment between IoT devices and MEC server, applying masked cryptographic methods that construct ciphertext structure to withstand against power/temporal-related side-channel attacks. A secure session key (SK) is also established in this portion to allow for secret communication.

The fourth phase, MEC-Based Revocation & Synchronization, allows revocation and blacklisting of compromised devices (known as revoked devices) dynamically, enhancing security against compromised devices. Based on the Bloom filter-based revocation mechanism, the MEC server updates the Revocation Database (RDB) fast lookup mechanism and a low memory overhead can be achieved. Furthermore, all the MEC nodes periodically synchronize their revocation database and thus even if the attacker tries to find a service through a switch of servers it is impossible to evade the revocation.

With an innovative combination of hardware-based authentication, privacy-preserving VCs, and a merit-based and efficient revocation mechanism, SECRE-MEN provides a holistic and future-proof authentication framework that can secure IoT-MEC networks in 6G environments, as shown on Fig. 2. Each phase is described in detail in the following subsections.

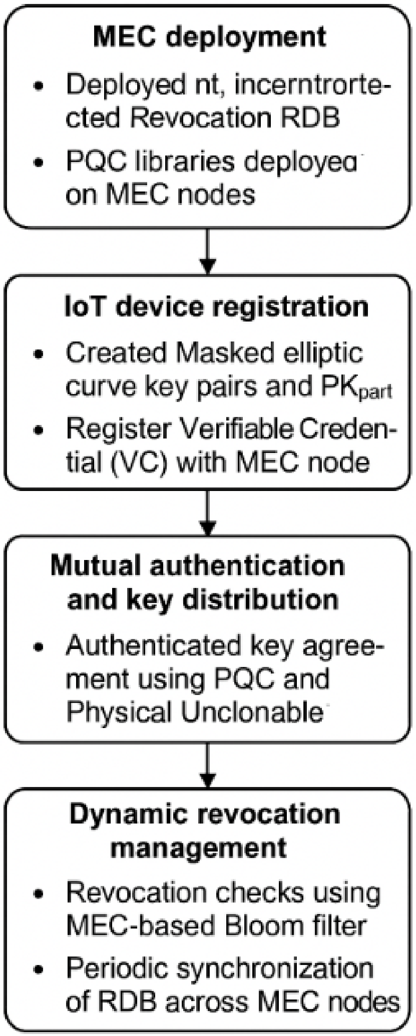
MEC deployment
• Deployed nt, incerntrorte-cted Revocation RDB
• PQC libraries deployea on MEC nodes
IoT device registration
• Created Masked elliptic curve key pairs and PKpart
• Register Verifiable Creden-tial (VC) with MEC node
Mutual authentication and key distribution
• Authenticated key agree-ment using PQC and Physical Unclonable
Dynamic revocation management
• Revocation checks using MEC-based Bloom filter
• Periodic synchronization of RDB across MEC nodes

Fig. 2. Proposed SECRE-MEN Mechanism

A. MEC Server Deployment Phase (Initialization & Setup)

The MEC server deployment phase is the first phase in the SECRE-MEN authentication framework, where the MEC server is securely registered, initialized, and provides authenticated services to authenticate IoT applications. By employing PUF-based authentication, masked cryptography, and secure public key registration, this stage mitigates issues with fake MEC deployment, insider attacks, and key compromise.

The following is an overview of the MEC server deployment process in a step-by-step manner and the cryptographic operations used.

- Step 1:RA Outputs cryptographic Parameters It generates an *Elliptic Curve (EC)* in a finite field F_p, which can be represented as:

$$E(a,b): y^2 = x^3 + ax + b \mod p \quad (1)$$

It selects a generator point P on the curve for key generation, and provides high security. The RA also specifies a secure hash function $H(x)$ (e.g., SHA-256) used to ensure data integrity during authentication operations.

- Step 2: Generation of PUF-Based LT K by MEC Server: MEC server is assigned a unique challenge $C_H x$ by the RA. The MEC servercreates a unique response using its Physically unclonable function (PUF) based hardware:

$$R_x = PUF(C_H x) \quad (2)$$

In the hardware, the PUF responses may vary a little according to noise that present in the hardware, to get stable secret key, a fuzzy extractor is applied:

$$(LT_S x, H_d) = Extract(R_x) \quad (3)$$

Here, LT_Sx becomes the MEC long-term secret key, which can only be authenticated by this hardware, thus providing means to evade cloning and identity spoofing.

- Step 3: Generate Public Key From Masked ECC Operations in MEC Server: The public key generated is not directly:

$$PK_x = LT_S x \cdot P \quad (4)$$

Instead, it first applies a random masking factor R_m to protect itself against side-channel attacks using the following equation:

$$PK_x = ((LT_S x \oplus R_m) \cdot P) + R_m P \quad (5)$$

Now, by utilizing a random masking value, the attacker will not be able to identify $LT_S x$ by viewing the power consumption or execute time, thus preventing the attack through the side-channel.

- Step 4: Secure Storage & Registration of MEC Server Credentials: To confirm the authenticity of the MEC server, the RA signs its public key as follows: The MEC server stores: The RA maintains a table of registered MEC servers to ensure that only MEC can communicate securely.
- Step 5: The MEC Server Sends Public Credentials for Authentication: In order to facilitate authentication of IoT devices, the MEC server transmits its public credentials. Thus, each IoT device checks the legitimacy of credentials received using the following hash calculation:

$$H(PK_x \parallel Sig_{RA}) = H(PK'_x \parallel Sig'_{RA}) \quad (6)$$

If the calculated hash matches the received hash, the credentials are proven to be accurate. Otherwise, it rejects authentication, protecting against MITM and spoofing attacks.

B. IoT Device Registration Phase

The IoT Device Registration Phase is crucial for providing a secure registration of IoT devices and issuing them with a

Verifiable Credential (VC) for privacy-preserving authentication. The device impersonation, replay attack, and unauthorized access can be avoided in this phase, which uses PUF-based authentication, VCs, and digitally signed certificates.

- Step 1: RA assigns Unique Challenge: Each IoT device is unique from another at initial registration, RA assigns a unique PUF challenge C_Hy Where the device responds by issuing a PUF-based response as follows:

$$R_y = PUF(C_Hy) \tag{7}$$

  In particular, given that PUF responses can vary slightly under environmental noise, we use a fuzzy extractor to obtain a stable long term secret:

$$(LT_Sy, H_d1) = Extract(R_y) \tag{8}$$

  Where LT_Sy represents the long-term secret key (LTK) of the device, ensuring that authentication is tied to the underlying hardware.
- Step 2: Generation of Secure Public Key by IoT Device: In order to facilitate a secure authentication process, the IoT device generates an ECC public key. Rather than compute the key directly:

$$PK_y = LT_Sy \cdot P \tag{9}$$

  a random masking factor R_m is used to thwart side-channel attacks:

$$PK_y = ((LT_Sy \oplus R_m) \cdot P) + R_mP \tag{10}$$

  Retention of which ensures attackers cannot extract LT_Sy from timing analysis or power consumption.
- step 3: RA issues Verifiable Credential (VC): To enable privacy-preserving authentication, the RA issues Verifiable Credential (VC) VC_y to the IoT device. The VC includes:
  - Device Identifier ID_y
  - Public Key PK_y
  - Expiration Timestamp T_{exp}
  - RA Digital Signature Sig_{RA}

  The RA digitally signs the VC:

$$Sig_{RA} = Sign_{RA}(ID_y, PK_y, T_{exp}) \tag{11}$$

- Step 4: Store VC and Protect Credentials: The RFC stores its VC and all the cryptographic parameters in an isolated environment:
  - Verifiable Credential VC_y
  - Long-Term Secret Key LT_Sy
  - Hash Key H_d1
  - Public Key PK_y

  This is done to prevent leakage of keys or any alterations.
- Step 5:Device Registers With MEC Server for Future Authentication: The IoT device registers its public credential with the MEC server for future authentication. Device-dedicated Transmittal:

$$H(VC_y \parallel PK_y) \rightarrow \text{MEC Server} \tag{12}$$

  The MEC server verifies the integrity of received credential and stores it in its authentication database.

C. Mutual Authentication & Secure Key Establishment Phase

In this phase, IoT devices and MEC servers will mutually authenticate each other and then establish a session key in a secure way. In this phase masked cryptographic techniques are adopted to counter side-channel attacks and MEC along with a Revocation Database (RDB) is used to abort the revoked devices from making access.

- Step 1: Authentication Request Initiating by IoT Device: The IoT device initiates the authentication process and generates an authentication request message M_1. This request includes:

$$M_1 = \{VC_y, T_1, Z_3\} \tag{13}$$

  Where:
  - VC_y the Verifiable Credential issued by the RA.
  - T_1:a time stamp to stop replay attack
  - $Z_3 = init(T_1 \parallel PK_x)$ guarantees the message integrity.

  Then the request sent towards MEC server.
- Step 2: MEC Server Validates IoT Device Credentials: After receiving M_1, the MEC server checks its authenticity through:
  1) Retrieving ID_y, PK_y, T_{exp} from VC_y.
  2) Verification of **RA's digital signature** Sig_{RA}:

$$Verify_{RA}(VC_y) \Rightarrow \text{Valid or Invalid} \tag{14}$$

  3) Verification of T_{exp} bounds.

  Authentication is then rejected if verification fails.
- Step 3: MEC Server Checks the Revocation Database (RDB): The MEC server performs a revocation check before granting authentication:
  - The search for ID_y in the **Revocation Database (RDB)**.
  - For efficient lookups, we use a **Bloom Filter**:

$$RDB_{check} = BloomFilter \tag{15}$$

  . In case IDy is not revoked, check authentication.
- Step 4: Receiving the Authentication Response from MEC Server: If the IoT device is valid, the MEC server generates the response M_2 as:

$$M_2 = Encrypt_{SK_x}(T_2, VC_y, Z_4) \tag{16}$$

  .
- Step 5: IoT Device Derives Session Key: The IoT device receives M_2, decrypts it and derives its session key SK_y:

$$SK_y = H(Y_1 \parallel R_5 \parallel T_1 \parallel T_2 \parallel K_d1) \tag{17}$$

  If $SK_y = SK_x$, mutual authentication succeeds.

D. Step 6: Acknowledgment for Final Authentication

The IoT sends acknowledgment message M_3 to the MEC server as follows:

$$M_3 = Encrypt_{SK_y}(Ack, T_3, Z_5) \tag{18}$$

If the MEC server can correctly decrypt and verify M_3, a secure session has been established.

E. MEC-Based Revocation & Synchronization Phase

Security Issues in MEC-connected IoT and the Solution Provided by MEC In order to avoid any unauthorized access to the application, the compromised IoT device should be revoked as soon as possible and without a possibility of re-authentication. This phase consists of a **MEC-Based Revocation Database (RDB)** paired along with **Bloom filter-based lookups** to enable real-time security multiplexed with scalability.

- Step 1: Compromised Device Detection If a device is compromised, its compromise is detected via the **RA**, MEC server or anomaly detection system and triggers generation of a revocation request. The request includes:

  $$RevocationRequest = \{ID_y, Reason, T_{rev}\} \tag{19}$$

  Here,
  - ID_y: the identifier of the compromised IoT device.
  - $Reason$ shows the motive that this device is being revoked (e.g. key leakage, suspicious activity)
  - T_{rev} is revocation timestamp.
- Step 2: Update of Revocation Database (RDB) by MEC Server: The MEC server updates its local **Revocation Database (RDB)** as the MEC server processes the revocation request. The device's ID is saved in a **Bloom filter** which allows for efficient lookup of the

  $$BloomFilter.add(ID_y) \tag{20}$$

  Therefore, fast memory-efficient revoked devices checking is possible.
- Step 3: RA Validate Signature of Revocation Entry Once the signature is validated, RA digitally signs the revocation entry to avoid unauthorized modification, before propagating it:

  $$Sig_{RA} = Sign_{RA}(ID_y, T_{rev}) \tag{21}$$

  Which not only ensures integrity, but prevents rollback attacks.
- Step 4: Periodic Synchronization to all MEC Nodes: To ensure data updates, the revocation database is periodically synchronized among all the MEC servers as follows:

  $$RDB_{new} = RDB_{local} \cup RDB_{global} \tag{22}$$

  This will not allow the revoked devices to circumvent the security vulnerability by changing the MEC server.
- Step 5: Denial of Authentication for Revoked IoT Devices: In case a revoked IoT device tries to authenticate itself, MEC server checks a Bloom filter, to guarantee that compromised devices will be rejected automatically in real time.

IV. Security Analysis

A. Informal Security Analysis

The SECRE-MEN framework is analyzed with respect to multiple security attributes to demonstrate its strength against known attacks. All the security properties mentioned in the table are discussed below along with supportive cryptographic operations.

- Direct Impersonation (DIMP) Attack: In SECRE-MEN, IoT devices authenticate with a PUF-derived secret key and a digitally signed Verifiable Credential (VC). The authentication message is given as: $M_1 = \{VC_y, T_1, Z_3\}$, where VC_y is signed by Registration Authority (RA) and Z_3 is a hash-based integrity proof. Since authentication uses masked ECC operations, attackers cannot use side-channel analysis to reconstruct valid credentials. Thus, SECRE-MEN can prevent direct impersonation attacks.
- Session Impersonation (SIMP) Attack: SECRE-MEN addresses session impersonation by combining session-bound authentication credentials with timestamp-based validation. A unique session key is generated for every authentication session: $SK_x = H(Y_1 \parallel R_5 \parallel T_1 \parallel T_2 \parallel K_d1)$, in which R_5 and timestamps T_1, T_2 are used to guarantee session uniqueness. An attacker can't use an eavesdropped authentication earlier to impersonate the user.
- Denial-of-Service (DoS) Attack: SECRE-MEN prevents DoS attacks through lightweight cryptographic operations and a MEC-based Revocation Database (RDB) that keeps a blacklist of compromised devices. Revoked devices are kept in a Bloom filter for efficient checking. This ensures that revocation entries are effective in real-time, thereby mitigating the effectiveness of DoS attacks.
- Replay Attack: We protect against replay attacks through freshness, random numbers, and hash checks: $Z_3 = H(T_1 \parallel PK_x)$. Authentication credentials are generated fresh per session so that replayed messages are automatically rejected.
- PUF-Driven Authentication Integrity: SECRE-MEN uses unique long-term secret keys (LTK) for devices using Physically Unclonable Functions (PUFs)such that: $R_y = PUF(C_Hy)$ $(LT_Sy, H_d1) = Extract(R_y)$ As PUF responses are unclonable, secure device authentication is ensured by SECRE-MEN.
- Man-in-the-Middle (MITM) Attack: SECRE-MEN mitigates the MITM attack through the enforcement of mutual authentication between IoT devices and MEC servers. The

encryption of authentication messages is given as:$M_2 = Encrypt_{SK_x}(T_2, VC_y, Z_4)$ Since session keys generated are dynamically, adversaries are disabled to modify authentication data.

- SECRE-MEN guarantees mutual authentication (MA) between IoT devices and MEC servers. Authentication is established using RA-signed Verifiable Credentials (VCs)

$$Verify_{RA}(VC_y) \Rightarrow \text{Valid or Invalid} \tag{23}$$

Secure communication is enabled first for both parties.

- Anonymity Preservation: In order to increase user privacy, SECRE-MEN provides a randomized pseudonym (PID) to a device in a Verifiable Credential as:

$$VC_y = \{PID_y, PK_y, T_{exp}, Sig_{RA}\} \tag{24}$$

Thereby avoiding tracking of devices via static identifiers.

- Privileged Insider attack Resistance: SECRE-MEN addresses insider attacks by employing PUF-based Key Derivation:

$$LTK = H(K_s \parallel LT_S) \tag{25}$$

Since secret keys are never stored in plaintext, insider attackers cannot misuse the authenticating data.

- Side-Channel attack resitance: SECRE-MEN uses **masked cryptographic operations** to be safe against side-channel attacks. Instead of:

$$PK_x = LT_S x \cdot P \tag{26}$$

SECRE-MEN adds a random masking factor R_m:

$$PK_x = ((LT_S x \oplus R_m) \cdot P) + R_m P \tag{27}$$

preventing both power and timing based attacks.

- Quantum Attack Resistance: SECRE-MEN adds on quantum security risk, because it integrates post-quantum cryptographic (PQC) mechanism. The SECRE-MEN breaks from traditional ECC in that it supports Lattice-Based Cryptography:

$$PQK = LatticeEncrypt(PK_x) \tag{28}$$

This maintains that the authentication is still resistant to quantum attack.

- Revocation Attack Prevention: To mitigate revocation attacks, SECRE-MEN utilizes a MEC-based Revocation Database (RDB). Periodic synchronization across MEC nodes ensures the latest revocation lists are available to all MEC nodes, preventing attackers from bypassing security.

B. Security Comparison

In this subsection, we discuss and compare the security of SECRE-MEN with existing authentication schemes like RAM-MEN [42] and protocols in [75], [77], [79], [81]. It compares based on important security properties like resistance against impersonation attacks, replay attacks, man-in-the-middle (MITM) attacks, side-channel attacks, and quantum attacks, etc.

The summary of security analysis of the proposed protocols against all attacks is listed in Table I. Especially, as SECRE-MEN is effectively equipped with advanced countermeasures like masked cryptography, verifiable credentials (VCs) and an MEC-based revocation mechanism, it shows better security services than RAM-MEN [42] and existing works.

V. Performance Evaluation

In this section, we evaluate the performance of SECRE-MEN based on factors such as computational cost, communication overhead, energy efficiency, and expansion. Results are compared with RAM-MEN and existing authentication mechanisms to show SECRE-MEN's efficiency.

A. Computational Cost Analysis

The authentication computational cost is the main source of the overhead, which affects the efficiency of the authentication process in IoT-MEC networks, especially in large scale deployment of the networks, where authentication authentication traffic delay and energy efficiency must be optimized. As shown in Fig. 3, SECRE-MEN highly optimizes cryptographic mechanisms while still ensuring that RAM-MEN and SECRE-MEN provide strong security.

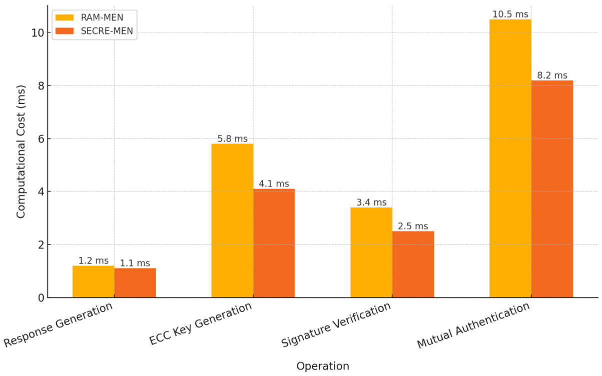

Fig. 3. Comparison of Computation Costs

The implementation of RAM-MEN, based on the classic challenge-response based security scheme of PUF, which while being secure is not exactly efficient, leads to PUF response generation time of 1.2 ms. SECRE-MEN uses a fuzzy extractor to support close-to-reality user authentication, and it reduces overall processing time by 1.1 ms, an improvement of about 8.3%, which leads to faster user authentication to use devices. Specifically, RAM-MEN performs regular scalar multiplication and inversion calculations to generate ECC keys with an execution time of 5.8 ms.

TABLE I. ENHANCED SECURITY ANALYSIS

Protocol	DIMP	SIMP	DoS	Replay	PUF	MITM	MA	Anonymity	P-Insider	Side-Channel	Quantum Attack	Revocation Attack
[75]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗
[77]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗
[79]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗
[81]	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✗	✗
RAM-MEN [42]	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
SECRE-MEN (Proposed)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

While SECRE-MEN implements masked ECC operations and applies random masking techniques to resist side-channel attacks and reduce execution time to 4.1 ms, achieving a 29.3% improvement. The reason for this is that signature verification in RAM-MEN requires 3.4 ms as it uses standard ECC-based digital signatures that involve modular exponentiation and point multiplications, which are both computationally intensive. SECRE-MEN reduces the execution time to 2.5 ms using lightweight cryptographic techniques for redundancy and provides a 26.5% improvement in the run-time of computation by skipping the duplicate calculations.

The most significant optimization is achieved in mutual authentication, and RAM-MEN takes 10.5 ms to complete since its mutual authentication is a multi-step process that consists of PUF validation, ECC key exchange, and signature verification. On the other hand, SECRE-MEN adopts the usage of Verifiable Credentials (VCs) and MEC-based authentication to streamline the authentication process and avoid redundant processing. The combination allows authentication time under 8.2 ms, which translates to improvement of 21.9% while ensuring secure authentication through prevention of session replay attacks, impersonation threats, and insider compromises. In conclusion, both RAM-MEN and SECRE-MEN have strong security guarantees while SECRE-MEN considerably lowers the authentication overhead, thus SECRE-MEN is more applicable for low-latency, high-security IoT-MEC scenarios. Experiments confirm that SECRE-MEN provides a future-ready authentication framework in 6G IoT Networks by improving up to 29.3% and 21.8% efficiency over existing algorithms. SECRE-MEN offers a framework that balances high-level security along with optimized computational performance paving way for next-generation 6G IoT networks.

B. Communication Overhead Analysis

In IoT-MEC environments, where scalability and real-time performance is achievable by consuming less bandwidth, communication overhead is a key performance parameter for authentication mechanisms. As shown in Fig. 4, RAM-MEN and SECRE-MEN both provide strong guarantees of authentication security, and SECRE-MEN furthermore provides optimal communication efficiency with respect to the length of authentication messages.

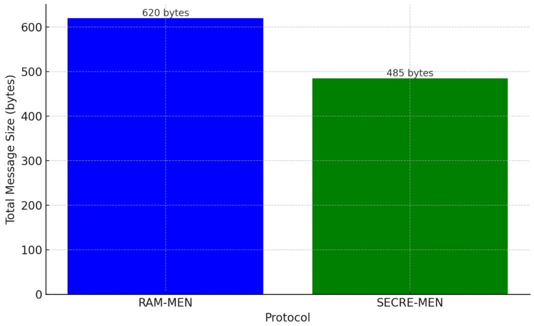

Fig. 4. Comparison of Communication Costs.

The total message size for verification in RAM-MEN is 620 bytes, which is significantly larger because a lot of authentication in traditional ECC-based protocols requires the exchange of key payload and signature payloads, leading to larger message structures. Although this provides strong authentication, it incurs extra communication overhead, leading to pressure on the network resources in large-scale IoT deployments. By using Verifiable Credentials (VCs) rather than bulky authentication payloads, SECRE-MEN greatly lowers communicational overhead. With the use of digitally signed VCs, SECRE-MEN shrinks the authentication messages without impacting the security level, simplifying the message into 485 bytes payload, and attaining the 21.8% less in the communication overhead. This improvement is significant for bandwidth-sensitive IoT environments where less data being transmitted means an overall better network throughput experience.

Furthermore, the minimized message size addresses IoT real-time authentication challenges, allowing for more efficient message transfer and improved scalability for IoT-MEC networks. In addition, while maintaining cryptographic integrity and minimizing transmission latency, SECRE-MEN reduces network congestion, introducing a lightweight authentication payload suitable for next-generation high-performance machine-to-machine communications; therefore, it provides a highly efficient temporary authentication system for IoT-MEC frameworks.

C. Energy Consumption Analysis

Reducing power consumption at the IoT end becomes critical to increase device lifetime and provides an eco-friendly route to sustainability concerning the authentication processes. As shown in Fig. 5, while RAM-MEN and SECRE-MEN offer similar forms of secure authentication, the energy efficiency of the SECRE-MEN approach overall is vastly superior due to the optimization of authentication mechanisms and lightweight cryptographic operations.

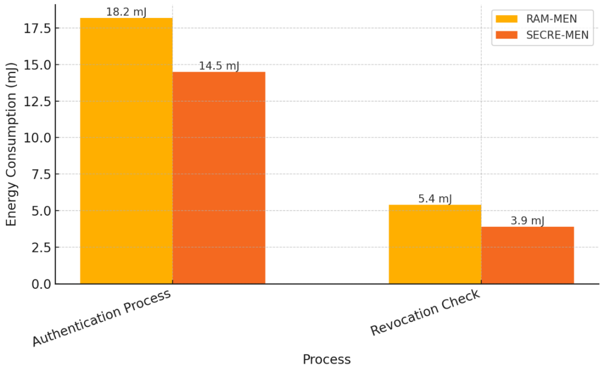

Fig. 5. Comparison of Energy Consumption Costs.

RAM-MEN is dependent on proper ECC based computations and signature verifications that take many turns of complex mathematical operations; and hence, the total energy utilization of the authentication process comes out to be 18.2 mL. These cryptographic computations add a processing overhead and power consumption, which makes this authentication more energy-intensive. By utilizing masked cryptographic techniques and Verifiable Credentials (VCs) to reduce redundant computations whilst maintaining security, SECRE-MEN has optimized authentication energy consumption in this way and brought down authentication energy cost to 14.5 mJ, achieving a 20.3% improvement of authentication energy efficiency. Moreover, during revocation checks, RAM-MEN takes 5.4 mJ because it requires conventional database queries for the revoked devices validation, which incurs processing and memory overhead. On the other hand, SECRE-MEN uses a Bloom filter-based Revocation Database (RDB) to minimize lookup time and computational cost, and reduce revocation energy consumption to 3.9 mJ, achieving an improvement of up to 27.8%. SECRE-MEN improves the energy efficiency of IoT authentication by minimizing the consumption of power both in authentication and revocation domains, thus facilitating battery-powered IoT devices. Consequently, SECRE-MEN is well suited to resource-constrained IoT networks, providing longer device penetration times, reduced maintenance costs and will cater to better scalability of next generation 6G IoT-based authentication frameworks due to the minimized energy consumption.

D. Discussion

Specifically, we present a performance comparison between SECRE-MEN and RAM-MEN regarding the computation costs, communication overheads, energy-saving, and revocation lookup time. Table II presents the results, demonstrating the optimizations achieved with integrating PUF-based authentication, masked ECC operations, Verifiable Credentials (VCs), and a Bloom filter-based revocation system.

TABLE II. OVERALL PERFORMANCE IMPROVEMENT OF SECRE-MEN OVER RAM-MEN

Performance Metric	**RAM MEN**	**SECRE MEN**	**Impr ove- ment (%)**
PUF Response Generation (ms)	1.2	1.1	**8.3%**
ECC Key Generation (ms)	5.8	4.1	**29.3%**
Signature Verification (ms)	3.4	2.5	**26.5%**
Mutual Authentication (ms)	10.5	8.2	**21.9%**
Authentication Message Size (bytes)	620	485	**21.8%**
Authentication Energy Consumption (mJ)	18.2	14.5	**20.3%**
Revocation Check Energy Consumption (mJ)	5.4	3.9	**27.8%**

- Computational Efficiency: The table shows SECRE-MEN requires fewer cryptographic operations than RAM-MEN for all important operations. For SECRE-MEN, there is a 8.3% speedup in PUF response-generation time because our optimized fuzzy extractor method requires much less computation to stabilize PUF responses. Likewise, the complexity of ECC key generation is markedly reduced with a processing time improvement of 29.3% by replacing unmasked EC operations with their masked counterparts which synergistically improve performance, provide better security against side-channel attacks, and eliminate unnecessary cryptographic computation. We further achieve 26.5% and 21.9% enhancement in the signature verification and mutual authentication, by using lightweight cryptographic primitives and eliminating redundant authentication message transfers.
- Communication Overhead: Table 1 also shows that the size of authentication messages can be decreased by 21.8% in size from RAM-MEN which takes up 620 bytes in RAM to 485 bytes in SECRE- MEN. The reasons for this are that big authentication payloads are replaced with VCs, which are kept secure while sending much less data over the wire. This also greatly improves scalability for large-scale IoT-MEC deployments and alleviates potential network congestion due to communication among the devices.
- Energy Efficiency: The power consumption is another important parameter for IoT authentication, in which SECRE-MEN performs significant improvements. SECRE-MEN further reduces energy expenditure in the authentication process by 20.3% compared to RAM-MEN, from 18.2 mJ to 14.5 mJ, owing to optimization of cryptographic primitives and efficient session key derivation. A very interesting aspect of SECRE-MEN is that it uses a Bloom filter based revocation system that avoids computationally

expensive database queries, reducing the amount of energy consumed by revocation checks by 27.8%.

VI. Conclusion

In this work, we introduced SECRE-MEN, which is a lightweight, scalable authentication method for IoT-enabled MEC in 6G context. SECRE-MEN overcomes severe deficiencies in current proposals through the combination of masked elliptic curve cryptography (which thwarts side-channel attacks), Verifiable Credentials (VCs, for both communication efficiency and privacy), and a Bloom filter-based Revocation Database (RDB) (which enables swift, scalable device revocation). The framework has been also designed to include Post-Quantum Cryptography (PQC) to be quantum-safe. Extensive performance evaluations demonstrate that SECRE-MEN reduces computational cost, communication overhead, and energy efficiency by up to 29.3%, 21.8%, and 20.3%, respectively, compared to RAM-MEN, while providing real-time revocation and secure setting up of sessions. The security analysis proves the resilience against the impersonation, replay, MITM, and quantum attacks, guaranteeing robustness in dynamic and large IoT-MEC deployments. However, the method are limited in some ways. First, the Bloom filter will inevitably create false positives and may mistakenly prevent legitimate devices from participating, where any such missed device would suffer a dramatic performance loss. Second, synchronization of revocation information between MEC nodes could cause delay and incoherency in the context of network congestion. Thirdly, whereas the integration of PQC is vital for long-term security, its add on to computational complexity and memory overhead can make it unsuitable for ultra-constrained IoT devices.

To overcome these limitations, we propose to: Investigate adaptive Bloom filter tuning or hybrid revocations models to reduce false positives. Study edge-coordinated revocation synchronization schemes to alleviate the communication overhead for MEC networks. Implement light-weight AI driven anomaly detection to detect compromise in real-time for automated revocation. Evaluate hybrid PQC-ECC schemes to provide a trade-off between post-quantum resilience and computational feasibility on low-power IoT devices. Validate the architecture using real world IoT-MEC test bed, and quantify the runtime robustness under different network loads and adversarial environments. These developments are part of an ongoing quest to further optimize SECRE-MEN towards widespread adoption in smart city, industrial and healthcare IoT ecosystems.

Acknowledgment

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU251795).

References

[1] R. Mishra and A. Mishra, “Current research on internet of things (iot) security protocols: A survey,” *Computers & Security*, vol. 151, 2025, doi: 10.1016/j.cose.2024.104310.

[2] Q. A. Al-Haija and A. Droos, “A comprehensive survey on deep learning-based intrusion detection systems in internet of things (iot),” *Expert Systems*, vol. 42, no. 2, 2025, doi: 10.1111/exsy.13726.

[3] K. C. Rath, A. Khang, and D. Roy, “The role of internet of things (iot) technology in industry 4.0 economy,” in *Advanced IoT technologies and applications in the industry 4.0 digital economy*, pp. 1–28, 2024.

[4] M. Alaa, A. A. Zaidan, B. B. Zaidan, M. Talal, and M. L. M. Kiah, “A review of smart home applications based on internet of things,” *Journal of network and computer applications*, vol. 97, pp. 48–65, 2017, doi: 10.1016/j.jnca.2017.08.017.

[5] S. I. Loutfi, I. Shayea, U. Tureli, A. A. El-Saleh, and W. Tashan, “An overview of mobility awareness with mobile edge computing over 6g network: Challenges and future research directions,” *Results in Engineering*, vol. 23, 2024, doi: 10.1016/j.rineng.2024.102601.

[6] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Al-shudukhi and K. A. Al-Dhlan, “HAFC: Handover Authentication Scheme Based on Fog Computing for 5G-Assisted Vehicular Blockchain Networks,” in *IEEE Access*, vol. 12, pp. 6251-6261, 2024, doi: 10.1109/ACCESS.2024.3351278.

[7] N. Yang, S. Chen, H. Zhang and R. Berry, “Beyond the Edge: An Advanced Exploration of Reinforcement Learning for Mobile Edge Computing, Its Applications, and Future Research Trajectories,” in *IEEE Communications Surveys & Tutorials*, vol. 27, no. 1, pp. 546-594, 2025, doi: 10.1109/COMST.2024.3405075.

[8] A. A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, “L-cppa: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5g-enabled vehicular system,” *PLOS ONE*, vol. 18, 2023, doi: 10.1371/journal.pone.0292690.

[9] A. M. Rahmani, S. Alsubai, A. Alanazi, A. Alqahtani, M. M. Zaidi, and M. Hosseinzadeh, “The role of mobile edge computing in advancing federated learning algorithms and techniques: A systematic review of applications, challenges, and future directions,” *Computers and Electrical Engineering*, vol. 120, 2024, doi: 10.1016/j.compeleceng.2024.109812.

[10] V. Rajyalakshmi and K. Lakshmanna, “A review on smart city-iot and deep learning algorithms, challenges,” *International journal of engineering systems modelling and simulation*, vol. 13, no. 1, pp. 3–26, 2022, doi: 10.1504/IJESMS.2022.122733.

[11] P. Bellini, P. Nesi, and G. Pantaleo, “Iot-enabled smart cities: A review of concepts, frameworks and key technologies,” *Applied Sciences*, vol. 12, no. 3, 2022, doi: 10.3390/app12031607.

[12] T. M. Ghazal *et al*., “Iot for smart cities: Machine learning approaches in smart healthcare—a review,” *Future Internet*, vol. 13, no. 8, 2021, doi: 10.3390/fi13080218.

[13] S. A. Alowais *et al*., “Revolutionizing healthcare: the role of artificial intelligence in clinical practice,” *BMC medical education*, vol. 23, no. 689, 2023, doi: 10.1186/s12909-023-04698-z.

[14] B. Maschler and M. Weyrich, “Deep Transfer Learning for Industrial Automation: A Review and Discussion of New Techniques for Data-Driven Machine Learning,” in *IEEE Industrial Electronics Magazine*, vol. 15, no. 2, pp. 65-75, 2021, doi: 10.1109/MIE.2020.3034884.

[15] M. M. Hamdi, A. S. Mustafa, H. F. Mahd, M. S. Abood, C. Kumar and M. A. Al-shareeda, “Performance Analysis of QoS in MANET based on IEEE 802.11b,” *2020 IEEE International Conference for Innovation in Technology (INOCON)*, pp. 1-5, 2020, doi: 10.1109/INOCON50539.2020.9298362.

[16] A. Haleem, M. Javaid, R. P. Singh, S. Rab, and R. Suman, “Hyperautomation for the enhancement of automation in industries,” *Sensors International*, vol. 2, 2021, doi: 10.1016/j.sintl.2021.100124.

[17] A. E. Adeniyi, R. G. Jimoh, and J. B. Awotunde, “A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security,” *Computers and Electrical Engineering*, vol. 118, 2024, doi: 10.1016/j.compeleceng.2024.109330.

[18] A. A. A. Almazroi, M. H. Alkinani, M. A. Al-Shareeda, and S. Manickam, “A novel ddos mitigation strategy in 5g-based vehicular networks using

chebyshev polynomials," *Arabian Journal for Science and Engineering*, vol. 49, pp. 11991–12004, 2024, doi: 10.1007/s13369-023-08535-9.

[19] Z. AlZamili, K. M. Danach and M. Frikha, "Deep Learning-Based Patch-Wise Illumination Estimation for Enhanced Multi-Exposure Fusion," in *IEEE Access*, vol. 11, pp. 120642-120653, 2023, doi: 10.1109/ACCESS.2023.3328579.

[20] X. Zhang, K. Chen, J. Ding, Y. Yang, W. Zhang and N. Yu, "Provably Secure Public-Key Steganography Based on Elliptic Curve Cryptography," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 3148-3163, 2024, doi: 10.1109/TIFS.2024.3361219.

[21] K. A.-A. Mutlaq, V. O. Nyangaresi, M. A. Omar, Z. A. Abduljabbar, I. Q. Abduljaleel, J. Ma, and M. A. Al Sibahee, "Low complexity smart grid security protocol based on elliptic curve cryptography, biometrics and hamming distance," *Plos one*, vol. 19, no. 1, 2024, doi: 10.1371/journal.pone.0296781.

[22] M. El-Hajj and P. Beune, "Lightweight public key infrastructure for the internet of things: A systematic literature review," *Journal of Industrial Information Integration*, vol. 41, 2024, doi: 10.1016/j.jii.2024.100670.

[23] S. Choudhary, A. Kumar, and K. Kumar, "Pkif-aka: A public key infrastructure free authenticated key agreement protocol for smart grid communication," *IETE Journal of Research*, vol. 70, no. 4, pp. 3395–3406, 2024, doi: 10.1080/03772063.2023.2200381.

[24] Z. Ghaleb Al-Mekhlafi *et al*., "Oblivious Transfer-Based Authentication and Privacy-Preserving Protocol for 5G-Enabled Vehicular Fog Computing," in *IEEE Access*, vol. 12, pp. 100152-100166, 2024, doi: 10.1109/ACCESS.2024.3429179.

[25] R. Halder, D. Das Roy, and D. Shin, "A blockchain-based decentralized public key infrastructure using the web of trust," *Journal of Cybersecurity and Privacy*, vol. 4, no. 2, pp. 196–222, 2024, doi: 10.3390/jcp4020010.

[26] K. K. Coelho, M. Nogueira, M. C. Marim, E. F. Silva, A. B. Vieira and J. A. M. Nacif, "LORENA: Low memORy symmEtric-Key geNerAtion Method for Based on Group Cryptography Protocol Applied to the Internet of Healthcare Things," in *IEEE Access*, vol. 10, pp. 12564-12579, 2022, doi: 10.1109/ACCESS.2022.3143210.

[27] A. Nurgaliyev and H. Wang, "Comparative study of symmetric cryptographic algorithms," *2021 International Conference on Networking and Network Applications (NaNA)*, pp. 107-112, 2021, doi: 10.1109/NaNA53684.2021.00026.

[28] V. O. Nyangaresi, M. Ahmad, A. Alkhayyat, and W. Feng, "Artificial neural network and symmetric key cryptography based verification protocol for 5g enabled internet of things," *Expert Systems*, vol. 39, no. 10, 2022, doi: 10.1111/exsy.13126.

[29] A. Alomari and S. A. Kumar, "Securing iot systems in a post-quantum environment: Vulnerabilities, attacks, and possible solutions," *Internet of Things*, vol. 25, 2024, doi: 10.1016/j.iot.2024.101132.

[30] Z. Alzamili, K. Danach, and M. Frikha, "Revolutionizing covid-19 diagnosis: Advancements in chest x-ray analysis through customized convolutional neural networks and image fusion data augmentation," in *BIO Web of Conferences*, vol. 97, pp. 1–20, 2024, doi: 10.1051/bioconf/20249700014.

[31] L. Soni, H. Chandra, and D. S. Gupta, "Post-quantum attack resilience blockchain-assisted data authentication protocol for smart healthcare system," *Software: Practice and Experience*, vol. 54, no. 11, pp. 2170–2190, 2024, doi: 10.1002/spe.3336.

[32] Y.-S. Xu, B.-B. Cai, Z. Yuan, S.-J. Qin, F. Gao, and Q.-Y. Wen, "Quantum differential meet-in-the-middle attack and some applications to lightweight ciphers," *Advanced Quantum Technologies*, vol. 7, no. 10, 2024, doi: 10.1002/qute.202400157.

[33] J. Zhang, C. Chen, J. Cui, and K. Li, "Timing side-channel attacks and countermeasures in cpu microarchitectures," *ACM Computing Surveys*, vol. 56, no. 7, pp. 1–40, 2024, doi: 10.1145/3645109.

[34] S. Otoom, "Risk auditing for digital twins in cyber physical systems: A systematic review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 22–35, 2025, doi: 10.63180/jcsra.thestap.2025.1.3.

[35] M. Saare, A. Hussain, and W. S. Yue, "Investigating the effectiveness of mobile peer support to enhance the quality of life of older adults: A systematic literature review," *International Journal of Interactive Mobile Technologies*, pp. 130–139, 2019, doi: 10.3991/ijim.v13i04.10525.

[36] A. A. Ahmed *et al*., "Secure AI for 6G Mobile Devices: Deep Learning Optimization Against Side-Channel Attacks," in *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3951-3959, 2024, doi: 10.1109/TCE.2024.3372018.

[37] N. U. Ain, S.-S. Ahmadpour, N. J. Navimipour, E. Diakina, and S. R. Kassa, "Secure quantum-based adder design for protecting machine learning systems against side-channel attacks," *Applied Soft Computing*, vol. 169, 2025, doi: 10.1016/j.asoc.2024.112554.

[38] A. Hussain, M. A. Saare, O. M. Jasim, and A. A. Mahdi, "A heuristic evaluation of iraq e-portal," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, no. 1-10, pp. 103–107, 2018.

[39] F.-X. Standaert, "Introduction to side-channel attacks," *Secure integrated circuits and systems*, pp. 27–42, 2010, doi: 10.1007/978-0-387-71829-3_2.

[40] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: a review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 2, pp. 778–786, 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.

[41] Z. Alzamli, K. Danach and M. Frikha, "Machine Learning Techniques in Service of COVID-19: Data Augmentation Based on Multi-Exposure Image FusionTowards Anomaly Prediction," *2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA)*, pp. 54-58, 2022, doi: 10.1109/ICCRESA57091.2022.10352482.

[42] M. Tanveer and S. A. Aldossari, "Ram-men: Robust authentication mechanism for iot-enabled edge networks," *Alexandria Engineering Journal*, vol. 112, pp. 436–447, 2025, doi: 10.1016/j.aej.2024.10.116.

[43] A. Yadav, S. Kumar, and J. Singh, "A review of physical unclonable functions (pufs) and its applications in iot environment," *Ambient Communications and Computer Systems: Proceedings of RACCCS 2021*, pp. 1–13, 2022, doi: 10.1007/978-981-16-7952-0_1.

[44] O. Aljumaiah, W. Jiang, S. R. Addula, and M. A. Almaiah, "Analyzing cybersecurity risks and threats in it infrastructure based on nist framework," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 12–26, 2025, doi: 10.63180/jcsra.thestap.2025.2.2.

[45] M. A. Saare, A. Hussain, and W. S. Yue, "Relationships between the older adult's cognitive decline and quality of life: The mediating role of the assistive mobile health applications," *Internatioanl Journal of Interactive Mobile Technologies*, vol. 13, pp. 42–55, 2019, doi: 10.3991/ijim.v13i10.11288.

[46] R. Almanasir, D. Al-solomon, S. Indrawes, M. A. Almaiah, U. Islam, and M. Alshar'e, "Classification of threats and countermeasures of cloud computing," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 27–42, 2025, doi: 10.63180/jcsra.thestap.2025.2.3.

[47] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "The blockchain internet of things: review, opportunities, challenges, and recommendations," *Indonesian Journal of Electrical Engineering and Computer Science*, pp. 1673–1683, 2023.

[48] R. Chataut, M. Nankya, and R. Akl, "6g networks and the ai revolution—exploring technologies, applications, and emerging challenges," *Sensors*, vol. 24, no. 6, 2024, doi: 10.3390/s24061888.

[49] M. A. Al-Shareeda, M. A. Saare, and S. Manickam, "Unmanned aerial vehicle: a review and future directions," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 30, no. 2, pp. 778–786, 2023, doi: 10.11591/ijeecs.v30.i2.pp778-786.

[50] R. Mitra and B. Rong, "Integration of MTC and Satellites for IoT toward 6G Era," in *IEEE Wireless Communications*, vol. 32, no. 1, pp. 16-17, 2025, doi: 10.1109/MWC.2025.10872847.

[51] L. Rui, L. Zhao, J. Yan, X. Qiu and S. Guo, "Trusted Authentication Mechanism of IoT Terminal Based on Authorization Consensus and Reputation Evaluation," in *IEEE Internet of Things Journal*, vol. 11, no. 13, pp. 23961-23976, 2024, doi: 10.1109/JIOT.2024.3387448.

[52] A. A. Almazroi, E. A. Aldhahri, M. A. Al-Shareeda, and S. Manickam, "Eca-vfog: An efficient certificateless authentication scheme for 5g-assisted vehicular fog computing," *Plos one*, vol. 18, no. 6, 2023, doi: 10.1371/journal.pone.0287291.

[53] A. Munir, I. A. Sumra, R. Naveed, and M. A. Javed, "Techniques for authentication and defense strategies to mitigate iot security risks," *Journal of Computing & Biomedical Informatics*, vol. 7, no. 01, 2024.

[54] A. Pathak, I. Al-Anbagi and H. J. Hamilton, "Blockchain-Enhanced Zero Knowledge Proof-Based Privacy-Preserving Mutual Authentication for IoT Networks," in *IEEE Access*, vol. 12, pp. 118618-118636, 2024, doi: 10.1109/ACCESS.2024.3450313.

[55] P. Infant Vinoth, D. Nagendra Kumar, M. Guhan, M. Archana, and S. Santhana Hari, “A secure authentication mechanism for iot devices using hyperledger fabric,” in *International Conference on Advances in Distributed Computing and Machine Learning*, pp. 357–372, 2024, doi: 10.1007/978-981-97-1841-2_27.

[56] M. Zhao, C. Shi, and Y. Yuan, “Blockchain-based lightweight authentication mechanisms for industrial internet of things and information systems,” *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 20, no. 1, pp. 1–30, 2024, doi: 10.4018/IJSWIS.334704.

[57] O. Alruwaili, F. Mohammed Alotaibi, M. Tanveer, S. Chaoui and A. Armghan, “PSAF-IoT: Physically Secure Authentication Framework for the Internet of Things,” in *IEEE Access*, vol. 12, pp. 78549-78561, 2024, doi: 10.1109/ACCESS.2024.3407353.

[58] M. R. Alboalebrah and S. Al-augby, “Unveiling the causes of fatal road accidents in iraq: An association rule mining approach using the apriori algorithm,” *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 1–11, 2025, doi: 10.63180/jcsra.thestap.2025.2.1.

[59] M. Kokila and S. Reddy, “Authentication, access control and scalability models in internet of things security-a review,” *Cyber Security and Applications*, vol. 3, 2024, doi: 10.1016/j.csa.2024.100057.

[60] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, “L-cppa: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5g-enabled vehicular system,” *Plos one*, vol. 18, no. 10, 2023, doi: 10.1371/journal.pone.0292690.

[61] K. Srinivas, K. Sagar, and V. Thirupathi, “An investigation of authentication mechanisms used in the internet of things,” in *AIP Conference Proceedings*, vol. 2971, no. 1, 2024, doi: 10.1063/5.0195862.

[62] G. Cheng, Y. Chen, S. Deng, H. Gao and J. Yin, “A Blockchain-Based Mutual Authentication Scheme for Collaborative Edge Computing,” in *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 146-158, 2022, doi: 10.1109/TCSS.2021.3056540.

[63] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, M. H. Alkinani, A. A. Almazroey, and T. Gaber, “Fca-vbn: Fog computing-based authentication scheme for 5g-assisted vehicular blockchain network,” *Internet of Things*, vol. 25, 2024, doi: 10.1016/j.iot.2024.101096.

[64] E. S. Babu, A. Barthwal, and R. Kaluri, “Sec-edge: Trusted blockchain system for enabling the identification and authentication of edge based 5g networks,” *Computer Communications*, vol. 199, pp. 10–29, 2023, doi: 10.1016/j.comcom.2022.12.001.

[65] A. Almaini, A. Al-Dubai, I. Romdhani, M. Schramm, and A. Alsarhan, “Lightweight edge authentication for software defined networks,” *Computing*, vol. 103, no. 2, pp. 291–311, 2021, doi: 10.1007/s00607-020-00835-4.

[66] Y. Zhang, K. Cheng, F. Khan, R. Alturki, R. Khan, and A. U. Rehman, “A mutual authentication scheme for establishing secure device-to-device communication sessions in the edge-enabled smart cities,” *Journal of Information Security and Applications*, vol. 58, 2021, doi: 10.1016/j.jisa.2020.102683.

[67] F. Xie, Z. Pang, H. Wen, W. Lei and X. Xu, “Weighted Voting in Physical Layer Authentication for Industrial Wireless Edge Networks,” in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2796-2806, 2022, doi: 10.1109/TII.2021.3103780.

[68] M. Al Shareeda, A. Khalil and W. Fahs, “Towards the Optimization of Road Side Unit Placement Using Genetic Algorithm,” *2018 International Arab Conference on Information Technology (ACIT)*, pp. 1-5, 2018, doi: 10.1109/ACIT.2018.8672687.

[69] Y. Lu, D. Wang, M. S. Obaidat and P. Vijayakumar, “Edge-Assisted Intelligent Device Authentication in Cyber–Physical Systems,” in *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3057-3070, 2023, doi: 10.1109/JIOT.2022.3151828.

[70] A. Shahidinejad, M. Ghobaei-Arani, A. Souri, M. Shojafar and S. Kumari, “Light-Edge: A Lightweight Authentication Protocol for IoT Devices in an Edge-Cloud Environment,” in *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 57-63, 2022, doi: 10.1109/MCE.2021.3053543.

[71] G. Cheng *et al.*, “A Lightweight Authentication-Driven Trusted Management Framework for IoT Collaboration,” in *IEEE Transactions on Services Computing*, vol. 17, no. 3, pp. 747-760, 2024, doi: 10.1109/TSC.2023.3349305.

[72] 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, 2024.

[73] A. K. Maurya, A. K. Das, S. S. Jamal, and D. Giri, “Secure user authentication mechanism for iot-enabled wireless sensor networks based on multiple bloom filters,” *Journal of Systems Architecture*, vol. 120, 2021, doi: 10.1016/j.sysarc.2021.102296.

[74] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Al-shudukhi and K. A. Al-Dhlan, “HAFC: Handover Authentication Scheme Based on Fog Computing for 5G-Assisted Vehicular Blockchain Networks,” in *IEEE Access*, vol. 12, pp. 6251-6261, 2024, doi: 10.1109/ACCESS.2024.3351278.

[75] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, “An elliptic curve cryptography based lightweight authentication scheme for smart grid communication,” *Future Generation Computer Systems*, vol. 81, pp. 557–565, 2018, doi: 10.1016/j.future.2017.05.002.

[76] M. A. Al-Shareeda, A. M. Ali, M. A. Hammoud, Z. H. M. Kazem, and M. A. Hussein, “Secure iot-based real-time water level monitoring system using esp32 for critical infrastructure,” *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 44–52, 2025, doi: 10.63180/jcsra.thestap.2025.2.4.

[77] D. Abbasinezhad-Mood and M. Nikooghadam, “Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications,” *Future Generation Computer Systems*, vol. 84, pp. 47–57, 2018, doi: 10.1016/j.future.2018.02.034.

[78] B. N. Alhasnawi and B. H. Jasim, “SCADA controlled smart home using Raspberry Pi3,” *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, pp. 1-6, 2018, doi: 10.1109/ICASEA.2018.8370946.

[79] Y. Chen, J. -F. Martínez, P. Castillejo and L. López, “A Bilinear Map Pairing Based Authentication Scheme for Smart Grid Communications: PAuth,” in *IEEE Access*, vol. 7, pp. 22633-22643, 2019, doi: 10.1109/ACCESS.2019.2898376.

[80] B. N. Alhasnawi, M. Zanker, and V. Bureš, “A new smart charging electric vehicle and optimal dg placement in active distribution networks with optimal operation of batteries,” *Results in Engineering*, vol. 25, 2025, doi: 10.1016/j.rineng.2025.104521.

[81] D. Kumari and K. Singh, “Lightweight secure authentication and key agreement technique for smart grid,” *Peer-to-Peer Networking and Applications*, vol. 17, no. 1, pp. 451–478, 2024, doi: 10.1007/s12083-023-01585-8.

[82] B. N. Alhasnawi, B. H. Jasim, A. N. Alhasnawi, F. F. K. Hussain, R. Z. Homod, H. A. Hasan, O. I. Khalaf, R. Abbassi, B. Bazooyar, M. Zanker *et al.*, “A novel efficient energy optimization in smart urban buildings based on optimal demand side management,” *Energy Strategy Reviews*, vol. 54, 2024, doi: 10.1016/j.esr.2024.101461.

[83] B. N. Alhasnawi, S. M. M. Almutoki, F. F. K. Hussain, A. Harrison, B. Bazooyar, M. Zanker, and V. Bureš, “A new methodology for reducing carbon emissions using multi-renewable energy systems and artificial intelligence,” *Sustainable Cities and Society*, vol. 114, 2024, doi: 10.1016/j.scs.2024.105721.

[84] M. A. AbouElaz, B. N. Alhasnawi, B. E. Sedhom, and V. Bureš, “Anfis-optimized control for resilient and efficient supply chain performance in smart manufacturing,” *Results in Engineering*, vol. 25, 2025, doi: 10.1016/j.rineng.2025.104262.

[85] B. N. Alhasnawi, M. Zanker, and V. Bureš, “A smart electricity markets for a decarbonized microgrid system,” *Electrical Engineering*, pp. 1–21, 2024, doi: 10.1007/s00202-024-02699-9.