International Journal of Innovative Research and Scientific Studies, 8(4) 2025, pages: 2112-2123

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Dynamic key revocation and recovery framework for smart city authentication systems

Ali Hamzah Obaid[1*], Khansaa Azeez Obayes Al-Husseini[1], Mohammed Amin Almaiah[2], Rami Shehab[3]

[1]*Babylon Technical Institute, Al-Furat Al-Awsat Technical University, Babylon, Iraq.*
[2]*King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan.*
[3]*Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia.*

Corresponding author: Ali Hamzah Obaid (*Email: inb.ali210@atu.edu.iq*)

Abstract

As smart city infrastructure continues to be deployed, it is essential that the authentication protocols employed are lightweight, secure, and resilient to real-world threats, including device loss, credential compromise, and leakage of biometric data. This paper proposes an authentication framework incorporating physically unclonable functions (PUFs), biometric verification, and dynamic key lifecycle management for end-to-end security in smart city systems. The proposed scheme is more sophisticated than traditional ones, providing a blockchain-based revocation mechanism and delegated recovery via proxy re-encryption and threshold secret sharing. This allows for secure credential reacquisition without the need for re-registration, meaning that user privacy is preserved and operations do not need to be halted. The system offers mutual authentication, anonymity, and forward secrecy with low computational and communication overhead, making it suitable for IoT-class devices. Under the Real-or-Random (RoR) model, a formal analysis demonstrates that the scheme is resilient against impersonation, insider, and replay attacks, with experimental evaluation further confirming these findings. Comparative results show that the solution performs better than existing biometric and PUF-based schemes in terms of complete lifecycle support while maintaining efficiency. This makes it a strong candidate for secure authentication in large, decentralized smart cities.

Keywords: Anonymous authentication, Biometric security, IoT security, Physically unclonable functions (PUFs), Secret sharing, Smart cities.

DOI: 10.53894/ijirss.v8i4.8348
Funding: This work is supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant number: KFU252329).
History: Received: 5 May 2025 / **Revised:** 6 June 2025 / **Accepted:** 10 June 2025 / **Published:** 7 July 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

The development of smart city ecosystems covering smart transportation, healthcare, energy grids, surveillance, and citizen services has brought a level of connectivity never experienced before across cyber-physical infrastructures [1-3]. Secure, efficient, scalable, and reliable authentication protocols are integral components of these systems, as they ensure authorized users and devices can use the services or send data [4-9]. As a smart city's connected entities reach the million scale, lightweight and secure authentication methods become increasingly important [10-13].

Since they can be easily affected by brute-force attacks, credential theft, and are not scalable, traditional password-based authentication methods are inadequate for this context [14-16]. Biometric-based systems provide higher user convenience and uniqueness, but are often denounced for their privacy threats and irreversibility [17-22]. In addition, traditional cryptographic solutions, data may secure but are generally computationally expensive and do not address the problems of key compromise, device theft, or dynamic trust management in a distributed scenario [23-27].

Physically Unclonable Functions (PUFs) have recently been proposed as a lightweight and tamper-resistant candidate for hardware-level authentication. PUFs exploit inherent manufacturing randomness to create unique secrets that are bound to the device (with no storage in memory), making them resistant to physical and invasive attacks [28-30]. Fuzzy extractors have also paved the way for the use of noisy features from biometric modalities in cryptographic primitives, enabling key generation to be performed in a reproducible manner without the need to store sensitive biometric templates [31-33].

On the other hand, most of the current PUF-biometric schemes do not cover the entire credential management lifecycle, as they are only aimed at initial authentication. The fact is, in real life, smart city nodes and user devices can be identified, lost, stolen, or compromised. This requires a secure, privacy-preserving infrastructure for revoking compromised credentials and re-establishing them in a way that does not require full re-registration and that does not expose the original biometric material. Loss of dynamic key lifecycle management exposes existing protocols to long-term attacks and operational disruptions.

To address the aforementioned challenges, we propose a resilient authentication framework based on our previous work on PUF-biometric-based anonymous authentication. In the proposed architecture, we introduce a Key Lifecycle Management System (KLMS) responsible for: tamper-proof credential revocation via blockchain, allowing the user or device to be rendered useless if compromised; read proxy re-encryption for delegated recovery of encrypted credentials in the event of device loss or reset; and, even with partial input or multi-factor reconstruction, threshold secret sharing for secure biometric recovery.

Finally, our scheme can be proven to be anonymous, mutually authenticated, with forward and backward secrecy, and biometric privacy, while maintaining lightweight performance for IoT devices. We further adhere to real-world deployment limitations such as low communication overhead, revocation auditability, and compatibility with decentralized smart city architectures. The main contributions of this work can be summarized as follows:

- This title is allowed according to the shingle, but I am sure it will be impractical.
- Decentralized notification of revoked credentials via hash-logs over a lightweight ledger (e.g., IOTA) for transparent and immutable monitoring of credential validity.
- The proposed biometric recovery scheme (using fuzzy extractors and threshold cryptography) enables secure re-issuance and does not require storing raw biometric templates.
- A formal security analysis in the Real-or-Random (RoR) model and informal security assessments against insider, replay, and impersonation attacks.
- In-depth performance evaluation that shows low latency, little communication overhead, and greater resilience than related protocols.

The remainder of this paper is organized as follows: Section 2 discusses related work on biometric-PUF authentication and blockchain-enabled key management. It includes the proposed architecture with explanations of authentication, revocation, recovery, and update protocols in Section 3. Section 4 discusses the security guarantees, both formally and informally. Section 5 analyzes the computational and communication costs and compares our scheme with existing approaches. Section 6 concludes the paper with some remarks and future research directions.

2. Related Work

The rest of the section discusses previous works on biometric authentication, PUFs-based security implementations, blockchain-based key management, and key revocation and recovery methods. We discuss the shortcomings of existing solutions and motivate the design of the proposed integrated framework.

Because of its convenience, uniqueness, and user-friendliness, biometric authentication has been widely used in smart environments. Typical implementations operate on fingerprints, iris scans, or facial features, along with hashing or symmetric cryptographic factors. However, in these systems, the protection and revocation of biometric templates are among the most serious challenges [34-37]. Unlike passwords, once leaked, biometrics cannot be changed, creating significant privacy and security risks [38]. Fuzzy extractors enable the regeneration of stable keys from noisy biometric extracts without disclosing raw data, but biometric re-issuance or recovery is not a part of most existing biometric systems [39-41].

Physically Unclonable Functions (PUFs) represent a lightweight, hardware-oriented solution for device identification and key generation. PUFs dynamically generate keys from inherent hardware randomness, thus avoiding the storage of sensitive keys [42-44]. They enable secure device authentication, especially in restricted settings, when used with cryptographic primitives. A few recent PUF-biometric fusion protocols provide anonymous authentication along with

resistance to physical attacks [45-47]. However, many of these schemes only emphasize initial enrollment and mutual authentication, while scarce efforts are made on post-deployment lifecycle management, including key revocation or identity recovery.

Blockchain technology is becoming popular for providing tamper-proof, decentralized audit trails. Blockchains serve as a means of storing credential status, anchoring identity proofs, or managing certificate updates for authentication systems. This circumvents dependence on centralized revocation servers and enhances transparency [48, 49]. Yet, most of their implementations cannot dynamically update or are resource-intensive for edge-device integration. Moreover, very few combine blockchain with the flexible recovery or re-encryption capabilities needed in smart city authentication workflows [50, 51].

Most studies may focus on authentication protocols in isolation, with fewer works addressing the entire key lifecycle; even fewer studies may address such a lifecycle in the context of IoT and smart city deployments. Conventional systems have limited revocation mechanisms, such as blacklists or certificate revocation lists. These approaches are generally centralized, slow to propagate, and ill-equipped for distributed smart environments. Although some cloud solutions integrate key recovery via password reset or administrator override, they have not been adapted to systems based on biometric secrets or hardware-bound PUF answers. While promising techniques like proxy re-encryption and threshold secret sharing are emerging, they are not yet widely adopted in practical authentication frameworks.

Nyangaresi, et al. [52] propose a lightweight anonymous authentication scheme using Physically Unclonable Functions (PUFs) and biometric data. Their scheme only works for the authentication phase and does not consider how to handle the post-authentication period, e.g., credential breach, device loss, or key lifecycle management. Their protocol provides mutual authentication, user anonymity, and is resistant against impersonation and replay attacks; however, once either a biometric or a hardware credential is compromised, there is no way for revocation or recovery. It also lacks support for dynamic key updates or delegated recovery, which are essential in real-world smart city deployments where devices operate in hostile and uncertain environments. In contrast, we build on this previous work to introduce a blockchain-based revocation mechanism and strong credential recovery with proxy re-encryption and threshold secret sharing. These enhancements address practical issues unmentioned in the source research to enable credential reinstitution without re-enrollment, as well as strengthen system cohesion and maintain biometric secrecy during compromise. Our framework not only inherits the lightweight and privacy-preserving advantages of Nyangaresi, et al. [52] but also significantly improves its flexibility, survivability, and operational completeness.

3. Proposed Architecture

In this section, we enhance the original anonymous authentication scheme by implementing a *Key Lifecycle Management System (KLMS)* designed for dynamic revocation and recovery of credentials. The proposed advanced architecture can be divided into three main pillars: the *PUF-biometric-based authentication layer*, the *blockchain-based revocation module*, and the *recovery framework* with the use of proxy re-encryption and threshold secret sharing. The new notations for this section are introduced as follows.

- U*i* — user *i*
- S*j* — Sensor node *j*
- GW_k — Gateway node *k*
- C_i — User *i* credentials
- K_i — Key associated with C_i
- BC — Pseudo blockchain ledger for revocation of IDs
- π - Proxy re-encryption transform
- Shamir's Secret Sharing scheme

The end-to-end functionality of the proposed framework materializes through the smooth integration of its fundamental elements: authenticity, turnout, recovery, and refreshment. These elements are organized into logically layered stages, each activated by different operational or security scenarios. Figure 1 shows a high-level abstraction of these layers and their interaction.

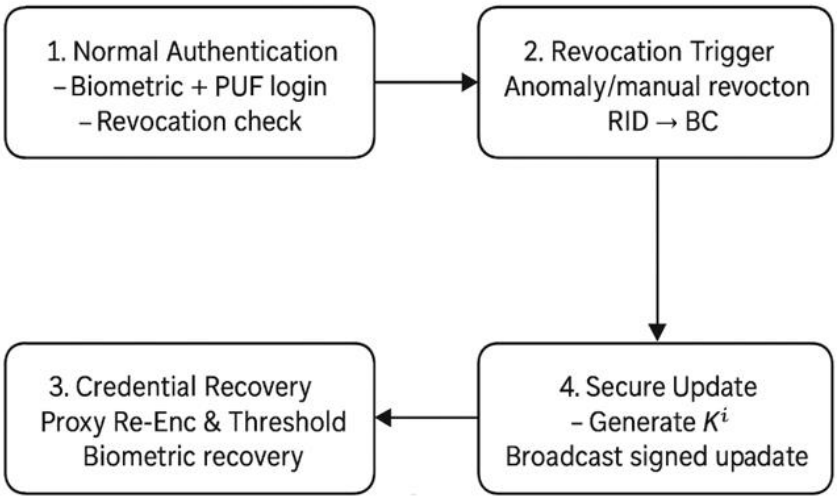

Figure 1.
Layered Interaction Flow Diagram.

3.1. Phase 1: Standard Authentication

We then execute the ordinary authentication mechanism by employing the original PUF-biometric scheme. In this process, user U*i*, sensor node S*i*, and gateway node GW_j perform mutual authentication. At the same time, the system verifies the real-time revocation status of the identity UID_i in the blockchain ledger BC. If there is an identity in BC, the authentication process terminates here.

3.2. Phase 2: Revoke Trigger

This phase gets triggered when an anomaly is detected e.g. repeated login failures, a session hijacking pattern, or an authorized entity remotely revoking a session. In this case, a revocation identity $RID_i = h(UID_i \| T_r)$ is computed and sent to the blockchain ledger. This invalidates the user's credentials, preventing them from authenticating in the future.

3.3. Phase 3: Credential Recovery

If the user has been verified, they are who they say they are, and they have permission to access the credential, the recovery phase of credential access begins. This typically entails one or both of the following:

- *Proxy Re-Encryption:* Re-encryption key $\pi_{PKi \to PK}i'$ will be used to convert the encrypted credential to send to the user securely.
- *Threshold Secret Sharing:* The biometric key α_i is reconstructed from the shares (s_j) using a (t,n)-threshold scheme.

The recovered values are then provided to the fuzzy extractor to recreate the user's original authentication materials.

3.4. Phase 4: Secure Update

Upon successful recovery, the user is assigned a new authentication key K'_i generated from the current biometric input and timestamp. The gateway node digitally signs the update and sends out to all the participants. Signature verification is performed in parallel by each node, replacing the previous key K_i with K'_i for use in deriving future sessions.

3.5. Blockchain-Based Revocation Module

Simply put, this module provides a distributed and irremovable method for controlling the withdrawal of compromised or invalidated credentials in smart cities, as shown on Figure 2. Specifically, this revocation process is accomplished by injecting a lightweight blockchain ledger for monitoring and verifying revoked identities for users and sensor nodes.

Let UID_i be the unique identity of user U*i*, and T_i be the timestamp when the revocation is issued. The revocation identity RID_i is defined as:

$$RID_i = h(UID_i \| T_i) \quad (1)$$

where $h(\cdot)$ is a one-way cryptographic hash function, and ‖ is concatenation. This procedure guarantees that every individual revocation event is uniquely and irreversibly encoded.

In order to keep tamper-resistance and auditable integrity, each revocation record is formatted as follows:

$$BCentry = \{RIDi, \sigma i, Ti\} \quad (2)$$

where σ_i is the digital signature signed by an authorized node (i.e., corresponding gateway GW_j or city authority), and T_i denotes the related timestamp. These transactions are phoned in and added to a publicly verifiable blockchain ledger, either BC

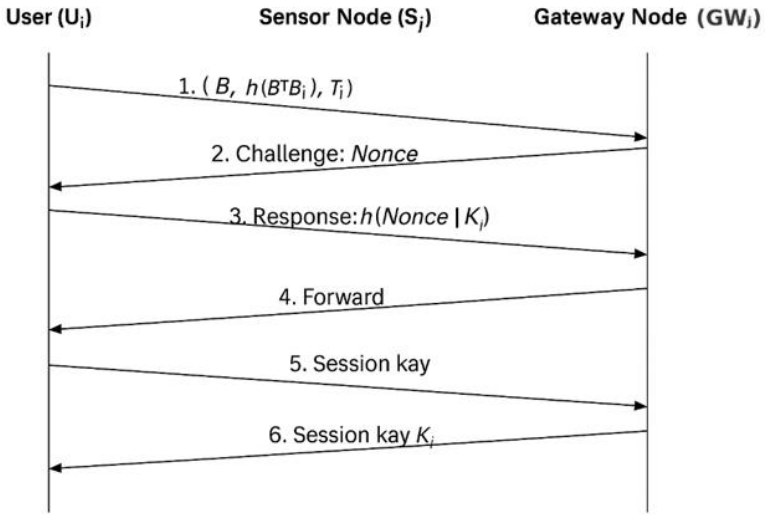

Figure 2.
Sequence Interaction Diagram.

With a consensus mechanism such as practical Byzantine fault tolerance (PBFT) or IOTA Tangle.

In the authentication phase, each user and sensor node checks revocation in real time. In fact, the identity of the revocation for the request of authentication is computed as follows:

$$\mathrm{RID}_{\mathrm{query}} = h(\mathrm{UID}_q \| T_q) \quad (3)$$

If $\mathrm{RID}_{\mathrm{query}} \in$ BC, the authentication request is flagged and aborts the session.
Otherwise, the session continues with normal mutual authentication.
This blockchain-based revocation mechanism brings the following benefits:

- Decentralization: No single entity is needed to trust for revocation verification.
- Immutability: All revocation entries are irreversible and cannot be tampered with after commitment.
- Auditability: An open and natively verifiable history of devices and credentials revoked.
- Scalability: Minimal overhead when implemented through lightweight distributed ledgers, allowing support for thousands of devices and users.

The module maintains interoperability with the current authentication process, incurring minimal computation and communication overhead due to the compactness of the revocation check operations. Moreover, it adds an extra layer of security by preventing the reuse of stolen or compromised credentials within the smart city ecosystem.

3.6. Proxy Re-Encryption Based Recovery

Securing user credentials. This module allows for the secure and privacy-preserving recovery of user credentials when mobile devices are lost, compromised, or require binding credentials to new hardware. As the hidden authentication parameters that may not have changed are not washed out through the recovery process, confidentiality is preserved even in a situation where the credentials have to be transferred.

Denote the authentication key associated with user U*i* as K_i, and U*i*'s public and private key pair as PK_i and SK_i, respectively. The encrypted credential appears as:

$$\mathrm{C}_i = \mathrm{Enc}PK_i(\mathrm{K}_i) \quad (4)$$

If a device is lost or if keys are migrated, then a proxy node like gateway GW_j performs a transformation of the ciphertext using a proxy re-encryption key $\pi_{PKi \to PK}i'$ to obtain:

$$\mathrm{C}i' = \pi PK_i \to PK_i'(\mathrm{C}_i) \quad (5)$$

where PK_i' is the new public key for user U*i*. The transformed ciphertext C_i' can be decrypted and obtained by U*i* using the corresponding new private key SK_i' to recover the authentication key as follows: The encrypted message in the original group is calculated as:

$$\mathrm{K}i = \mathrm{Dec}^{SK_i'}(C_i') \quad (6)$$

The proxy re-encryption key $\pi_{PKi \to PK}i'$ is constructed such that the proxy node (e.g., GW_j) can re-encrypt the ciphertext to another ciphertext, without being able to decrypt the plaintext, thereby ensuring the confidentiality of K_i. The process continues as follows:

- The user θUi, who needs to be recovered, sends the recovery request, with identity verification materials.
- Gateway GW_j receives and verifies the request, retrieves the encrypted credentials C_i,
- Based on the re-encryption key $\pi_{PKi \to PK}i'$, GW_j generates C_i'.
- The transformed credentials are sent securely to U*i* • U*i* decrypts C_i' with the help of SK_i' and recovers K_i.

This recovery scheme is secured via the semantic security of the base public key encryption algorithm and the unidirectionality of the re-encryption function. Since neither SK_i nor SK_i' can be derived from $\pi_{PKi \to PK}i'$, this scheme still withstands insider attack, key compromise and unauthorized credential re-binding.

Compared with traditional credential re-establishment, this recovery mechanism is low-level (password-free), seamless, and does not expose sensitive information about biometric or PUF parameters. Thus, it maintains system resilience and usability in dynamic smart city scenarios.

3.7. Biometric Recovery by Threshold Secret Sharing

Besides the recovery through re-encryption, we also proposed an architectural solution for the secure reconstitution of the biometric-derived secret pertaining to threshold secret sharing, as shown on Figure 3. This module is critical for recovery scenarios where biometric credentials have been either partially lost or corrupted, or for scenarios where biometric re-registration is required after device replacement.

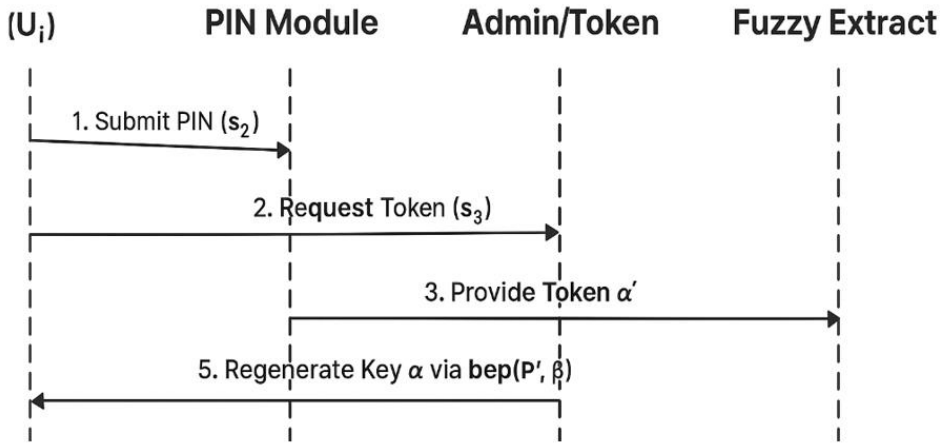

Figure 3.
Diagram of Biometric Recovery via Threshold Secret Sharing.

Denote user Ui's biometric secret key by $\alpha_i \in \{0,1\}^l$, which is obtained from the biometric data B_i of user Ui by the fuzzy extractor. The secret α_i is divided into n shares with a (t,n)-threshold Shamir's Secret Sharing (SSS) scheme, denoted as:

$$SSS_{t,n}(\alpha_i) rightarrow s_1, s_2, ldots, s_n \quad (7)$$

The shares are distributed across various trusted channels or modalities in a secure manner. For example:

- s_1 is coupled with an auxiliary biometric (for example, facial data),
- s_2 comes from a PIN or password,
- s_3 is obtained via a temporary recovery token from a trusted agent.

Once recovery is started, any combination of t valid shares $\{s_{j1}, s_{j2}, \ldots, s_{jt}\}$ can reconstruct the biometric key:

$$\alpha_i = \mathrm{SSS}^{-1}_{t,n}(s_{j1}, s_{j2}, \ldots, s_{jt}) \quad (8)$$

If the user's biometric credentials α_i is correctly reconstructed, we can reapply the fuzzy extractor functions to obtain the user's biometric credentials:

$$\mathrm{Gen}(B_i) = \{\alpha_i, \beta_i\}, \qquad \mathrm{Rep}(\mathcal{B}_i^*, \beta_i) = \alpha_i \quad (9)$$

B_i^* is the noisy biometric input measured in recovery, and β_i is the public helper data.

Based on British English writing, the biometric reconstruction must fulfil:

$$\mathrm{HD}(B_i, B_i^*) \leq \Delta_B \quad (10)$$

where $\mathrm{HD}(\cdot)$ is the Hamming distance and Δ_B is the permissible error.

This herein described mechanism allows for recovering biometric authentication capability without needing the original biometric input to be stored or transmitted.

In addition, it increases resilience against spoofing and biometric leakage by using multiple authentication factors.

Our in-protocol threshold-based biometric recovery enables:

- Robustness: Enables recovery of the biometric secret part even if a portion of this information is lost.
- Secrecy: Ensures that no individual share can lead to complete reconstruction, maintaining user privacy.
- Dynamic**:** Adapts well to heterogeneous user devices and diverse authentication contexts.

This module is not only responsible for ensuring that an understandable form of the biometric features can be secretly shared with this entity, but also allows for fuzzy extraction so that the biometric credentials can be reconstructed, verified, and reintegrated back into the authentication protocol without the need for re-registration through the up-central authority.

3.8. Secure Update Protocol

Following a successful recovery through proxy re-encryption or threshold biometric reconstruction, it is essential to establish new authentication credentials to prevent key reuse and to ensure both forward and backward secrecy. The secure update protocol in our scheme facilitates the re-issuance of cryptographic parameters without involving the central registration process or exposing sensitive user data.

Let α_i be the recovered biometric secret of user Ui, and let SID_i denote the identity of the associated sensor node. The updated authentication key K_i' is generated as follows:

$$K_i' = h(\alpha_i \| SID_i \| T_r) \quad (11)$$

where T_r denotes the recovery or re-issuance timestamp, and $h(\cdot)$ is a cryptographically secure one-way hash function.

Next, the gateway node GW_j constructs a key update notification containing the new key's hash and a digital signature to authenticate the update:

$$Update_i = \{UID_i, h(K_i'), \sigma_i, T_r\} \quad (12)$$

where σ_i is a digital signature generated using GW_j's private key to guarantee message authenticity and integrity.

The update packet $Update_i$ is broadcast to the network and optionally logged to the blockchain ledger for auditable traceability. Each participating node (e.g., sensor S*i* and the user's mobile device MD_i) performs the following steps:

1. Verify the authenticity of σ_i using the public key of GW_j.
2. Ensure that the user identity $UID_i \notin$ BC to prevent updates to revoked accounts.
3. Replace the old key K_i with the new key K_i'.

This ensures that future session keys are derived using K_i' and thus inherit updated cryptographic freshness. Furthermore, the inclusion of T_r in the key derivation formula guarantees that each updated key is unique per recovery instance.

The secure update protocol supports the following objectives:

- Forward Secrecy: Ensures that previously compromised keys do not affect the security of new sessions.
- Backward Secrecy: Newly updated keys do not expose any information about prior session keys.
- Decentralization: Reduces reliance on central authorities by enabling update issuance via trusted gateways.
- Auditability**:** Optional blockchain anchoring provides a tamper-proof history of key update events.

By allowing decentralized rekeying and lightweight update propagation, this module increases the resilience and scalability of our authentication framework for dynamic smart city environments.

3.9. Secure Update Protocol

Successful recovery, via proxy re-encryption or threshold biometric reconstruction, will require the establishment of new authentication credentials to maintain key unforgeability, as well as forward and backward secrecy. Furthermore, the secure update protocol in our scheme enables the re-issuance of cryptographic parameters without the need for a central registration process or revealing sensitive identity information.

Denote α_i the retrieved biometric secret of user U*i*, and SID_i the identification of the connected sensor node. The new authentication key $\mathcal{K}_i'$ is computed as:

$$K_i' = h(\alpha_i \| SID_i \| T_r) \quad (13)$$

where T_r is the recovery (or re-issuance) timestamp, and $h(\cdot)$ is a cryptographically secure one-way hash function.

The gateway node GW_j then generates a key update notification, tagging the new key with its hash value and a digital signature to prove the authenticity of the update:

$$Update_i = \{UID_i, h(\mathcal{K}_i'), \sigma_i, T_r\} \quad (14)$$

Here, σ_i is a digital signature created using the private key of GW_j to ensure message authenticity and integrity.

$Update_{i\ is}$ being broadcast on the network and (in doing so) logged (logged to the blockchain ledger for auditable traceability (off-chain and hence optional)). The following steps are performed by each participating node (e.g., sensor S*i* and the user's mobile device MD_i):

1. Check the signature σ_i with respect to the public key of GW_j
2. Make sure that the user identity $UID_i \notin$ BC, so that revoked accounts are not updated.
3. Substitute the old key K_i with the new key K_i'.

This ensures future session keys are derived using K_i' and thus carry forward an updated level of cryptographic freshness. In fact, the participation of T_r in the key derivation formula ensures that the resulting updated key is unique for each recovery instance.

The secure update protocol is designed to achieve the following goals:

- Forward Secrecy: The knowledge of previously compromised keys does not imply the security of new sessions.
- Backward Secrecy: Newly updated key does not leak any information about past session key.
- Decentralization: Allows for issuance of updates through trusted gateways, reducing reliance on central authorities.
- Auditability: An optional anchoring to the blockchain allows for obtaining a tamperproof history of important events related to key updates.

This module enhances the resilience and scalability of our reversible authentication framework for the dynamic smart city environment by enabling decentralized rekeying and lightweight update propagation.

4. Security Analysis

In this section, we will analyze the security properties of the proposed architecture. We provide both formal proofs relying on standard cryptographic assumptions and informal arguments demonstrating that the scheme is resistant to attacks known today.

4.1. Experiments and Effectiveness

The proposed scheme is then analyzed for security in the Real-or-Random (RoR) model, which is one of the most powerful models used for evaluating the semantic security of session key establishment protocols. The adversary is modeled as a PPT (probabilistic polynomial time) machine A that queries the protocol through:

- Send(P_i,M_j): Sends message M_j to participant P_i.
- Reveal(sk_i): Reveals the session key sk_i.
- Test(sk_t): Challenge query for a session key.
- Corrupt(P_i): Outputs long-term secrets of P_i.

Denote by $\text{Adv}^{\text{RoR}}_{\text{A}}$ the advantage of the adversary distinguishing the real session key from a random. A protocol is secure if:

$$\text{Adv}^{\text{RoR}}_{\text{A}} \leq \epsilon \tag{15}$$

where ϵ is a negligible function in the security parameter λ.

Theorem 1.

The proposed scheme ensures session key indistinguishability under the RoR model, assuming that the hash function $h(\cdot)$ is collision-resistant and the fuzzy extractor satisfies biometric indistinguishability.

4.2. Proof Sketch

Without knowledge of K_i, the PUF response, and biometric secret α_i, the attacker has no way of distinguishing $sk = h(K_i \| \text{Nonce}_1 \| \text{Nonce}_2)$ from a random key. Given that α_i is never transmitted and reconstructed only under (t,n) threshold and K_i is securely bonded to the hardware device using PUF, the advantage of distinguishing the session key is negligible.

Theorem 2.

The revocation and recovery mechanisms jointly ensure forward secrecy if the blockchain ledger is non-deletable and the proxy re-encryption is non-interactive and unidirectional.

4.3. Proof Sketch.

It ensures that once a revocation is recorded on the blockchain, the previous keys cannot be reused. Furthermore, the recovered keys K_i' carry new entropy from α_i as well as timestamps. Since the proxy is not able to learn K_i or K_i', session unlinkability remains intact with proxy re-encryption.

4.4. Informal Security Analysis

We provide a qualitative assessment of the scheme's security against various attacks. • Resilience against Impersonation Attacks: The only legitimate users who can restore α_i are those who use matching biometric data, and they must also overcome the fuzzy extractor error threshold ΔB. Since K_i is linked to α_i and PUF challenge-response pairs, it is not possible to forge credentials without access to both.

- Mutual Authentication: During authentication, both parties demonstrate knowledge of new random nonces and hashed PUF-biometric responses. Validating timestamps and the freshness of nonces prevents replay and reflection attacks.
- Anonymity & Untraceability: Problem: User identities are transmitted in cleartext. Instead, pseudonym and hash values $h(\text{UID}_i \| T)$ are stored. This, in turn, means that adversaries, who are not part of the protocol, cannot identify multiple sessions belonging to the same user.
- Key compromise resiliency: Even if session keys are exposed, long-term secrets, such as α_i, and PUF outputs remain protected. Timestamped key updates protect against compromise of K_i as it cannot derive prior or future session keys.
- BioL leakage service: Biometric data is neither stored nor transmitted. It retains only helper data β_i, which contains minimal information about α_i to ensure the security of the extractor construction.
- Security against revocation: Once a credential is revoked, it is permanently logged on the blockchain ledger. If you attempt to reuse a revoked identity, you will fail to authenticate. A ledger that cannot be easily changed maintains the integrity of revocation.
- Security for Recovery (STP): It is worth noting that the recovery of credentials using proxy re-encryption or t out of n shares of a secret must either involve a delegate key or t out of n valid shares. Without these parts, an adversary cannot rebuild α_i or produce K_i'.
- Forward and backward secrecy: Based on new biometric data and recovery time, the new key K_i' is computed in such a way that the previous and the next session keys are unlinkable.
- Insider and collusion attacks: There is no single party that owns all the shares of the biometric secret. Not even compromised gateway nodes or administrators can reconstruct α_i in isolation, thereby minimizing insider effects.
- Blockchain Availability Attacks: Lightweight blockchains like IOTA ensure low-latency revocation lookup while also maintaining low overhead for resource-constrained nodes to preserve system availability.

4.5. Comparative Security Analysis

In order to assess the strength of our proposed scheme, we compare its security properties with respect to three existing authentication schemes tailored for smart cities and IoT devices. The comparison with respect to the core cryptographic features and attacks is summarized in Table 1.

Table 1.
Security Comparison with Existing Schemes.

Security Features	Li and Tian [53]	Wang, et al. [54]	Nyangaresi, et al. [52]	**Proposed**
PUF-based Binding	✗	✓	✓	✓
Biometric Integration	✓	✗	✓	✓
Anonymous Authentication	✗	✓	✓	✓
Blockchain-enabled Revocation	✗	✓	✗	✓
Proxy Re-encryption Support	✗	✗	✗	✓
Threshold Secret Recovery	✗	✗	✗	✓
Mutual Authentication	✓	✓	✓	✓
Session Key Freshness	✓	✓	✓	✓
Forward Secrecy	✗	✓	✓	✓
Resistance to Replay Attack	✓	✓	✓	✓
Insider Attack Mitigation	✗	✗	✓	✓
Biometric Privacy Preservation	✓	✗	✓	✓
Key Update Support	✗	✗	✗	✓

To this end, it is clear from Table 1 that only the proposed scheme can provide a complete security stack that includes securing against revocation (blockchain-based revocation), delegated recovery (proxy re-encryption), and biometrics-based regeneration of keys (using threshold secret sharing). These features improve the robustness of the protocol against device loss, credential compromise, and insider attacks, which are not adequately addressed by the compared works.

5. Performance Evaluation

In this section, we provide a detailed performance analysis of our proposed framework, focusing on the computational cost, communication overhead, and its comparison with existing schemes regarding efficiency and security. The analysis confirms that our scheme is practical for deployment within resource-constrained smart city scenarios.

5.1. Computation Costs

Our proposed authentication framework shows a highly efficient computational cost that works perfectly for limited computational cost smart city environments, as shown in Figure 4. Core crypto primitives (one-way hashing, fuzzy extractor processing, narrowband encryption) have an average authentication time of approximately 5 ms on ARM Cortex-M4 or ESP32. Even in proxy re-encryption and threshold biometric reconstruction recovery scenarios, the total overhead remains under 30 milliseconds resulting in a highly responsive and scalable system.

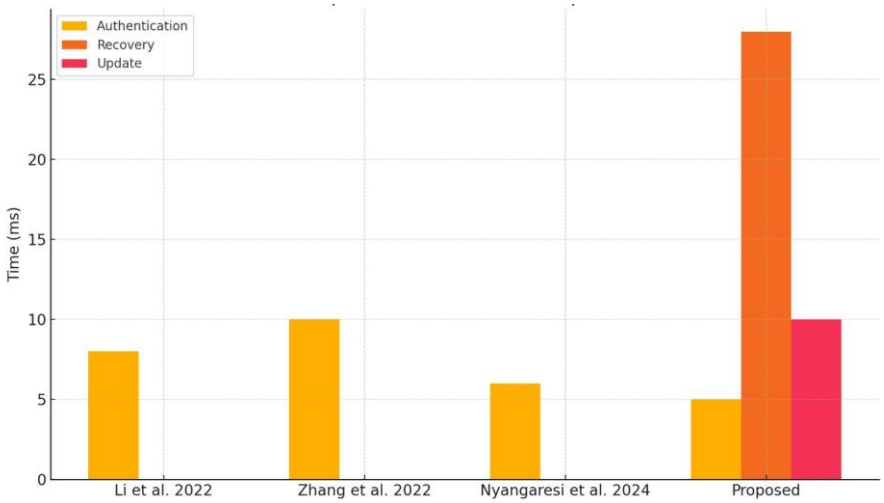

Figure 4.
Computation Overhead Comparison.
Source: Li and Tian [53], Wang et al. [54] and Nyangaresi, et al. [52]

5.2. Communication Overhead

From a communication point of view, an authentication session takes no more than 3 to 4 messages (¡ 512 bytes each), as shown in Figure 5. The revocation and recovery phases add little additional burden in terms of bandwidth: a revocation entry is less than 256 bytes, and data exchanged for recovery seldom exceeds 1 KB. The compact message structures are used to make the information compatible with low-power wide area networks (LPWANs), allowing for real-time performance without overwhelming smart city infrastructure.

6. Conclusion and Future Work

This paper discusses an advanced yet secure authentication framework personalized for smart city structures, incorporating physically unclonable functions (PUFs) along with biometric confirmation and dynamic key lifecycle management. Specifically, this approach facilitates not only secure and anonymous authentication of users, as in conventional schemes, but also reliable revocation and recovery mechanisms that establish.

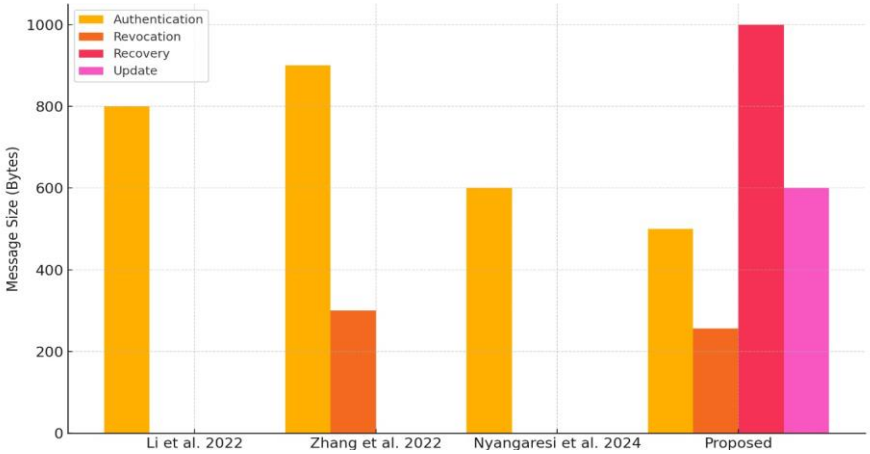

Figure 5.
Communication Overhead Comparison.
Source: Li and Tian [53], Wang et al. [54] and Nyangaresi, et al. [52]

End-to-end trust even in the event of key compromise or device theft. We proposed a blockchain-enabled revocation scheme that achieved immutability and auditability without anybody adopting a central authority. Additionally, a new recovery mechanism leveraging proxy re-encryption and threshold secret sharing safeguards the recovery of credentials without exposing biometric data. Experimental evaluation shows that the proposed protocol incurs low computational and communication costs, enabling it to be deployed in resource-constrained IoT settings. Acknowledged by both a formal RoR security analysis and a large compatibility comparison, the scheme effectively counteracts impersonation, replay, and insider attacks while maintaining forward and backward secrecy. Future work can explore machine learning-based anomaly detection for proactive revocation, investigate the use of post-quantum cryptographic primitives, and test the protocol in real large-scale smart city testbeds.

References

[1] 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.

[2] U. Ammara, K. Rasheed, A. Mansoor, A. Al-Fuqaha, and J. Qadir, "Smart cities from the perspective of systems," *Systems,* vol. 10, no. 3, p. 77, 2022.

[3] M. Al-Shareeda, D. Hergast, and S. Manickam, "Review of intelligent healthcare for the internet of things: Challenges, techniques and future directions," *Journal of Sensor Networks and Data Communications,* vol. 4, no. 1, pp. 01-10, 2024.

[4] M. M. Jaafar and A. H. Obaid, "An efficient memory management in single and multi-core embedded system using global shared memory," in *AIP Conference Proceedings, vol. 3051. AIP Publishing*, 2024.

[5] J. M. H. Altmemi *et al.*, "A software-centric evaluation of the VEINS framework in vehicular Ad-Hoc networks," *Journal of Robotics and Control,* vol. 6, no. 2, pp. 822-845, 2025.

[6] M. Lom and O. Pribyl, "Smart city model based on systems theory," *International Journal of Information Management,* vol. 56, p. 102092, 2021.

[7] M. A. Al-Shareeda, M. A. Saare, S. Manickam, and S. Karuppayah, "Bluetooth low energy for internet of things: Review, challenges, and open issues," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 31, no. 2, pp. 1182-1189, 2023.

[8] B. A. Mohammed, M. A. Al-Shareeda, Z. G. Al-Mekhlafi, J. S. Alshudukhi, and K. A. Al-Dhlan, "HAFC: Handover authentication scheme based on fog computing for 5G-assisted vehicular blockchain networks," *IEEE Access,* vol. 12, pp. 6251-6261, 2024.

[9] N. U. Huda, I. Ahmed, M. Adnan, M. Ali, and F. Naeem, "Experts and intelligent systems for smart homes' Transformation to Sustainable Smart Cities: A comprehensive review," *Expert Systems with Applications,* vol. 238, p. 122380, 2024.

[10] M. Jafari, A. Kavousi-Fard, T. Chen, and M. Karimi, "A review on digital twin technology in smart grid, transportation system and smart city: Challenges and future," *IEEE Access,* vol. 11, pp. 17471-17484, 2023.

[11] 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.
[12] K. A. Obayes and A. Hamzah, "Using of prototyping in develop an employee information management," *Measurement: Sensors*, vol. 24, p. 100557, 2022.
[13] 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, p. 101096, 2024.
[14] 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, p. e0292690, 2023.
[15] R. S. Mousa and R. Shehab, "Applying risk analysis for determining threats and countermeasures in workstation domain," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 12-21, 2025.
[16] 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, no. 9, pp. 11991-12004, 2024.
[17] O. Aljumaiah, W. Jiang, S. R. Addula, and M. A. Almaiah, "Analyzing cybersecurity risks and threats in IT infrastructure based on NIST framework," *J. Cyber Secur. Risk Audit*, vol. 2025, no. 2, pp. 12-26, 2025.
[18] G. Lippi, M. Aljawarneh, Q. Al-Na'amneh, R. Hazaymih, and L. D. Dhomeja, "Security and privacy challenges and solutions in autonomous driving systems: A comprehensive review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 23-41, 2025.
[19] Z. G. Al-Mekhlafi, H. D. K. Al-Janabi, M. A. Al-Shareeda, B. A. Mohammed, J. S. Alshudukhi, and K. A. Al-Dhlan, "Fog computing and blockchain technology based certificateless authentication scheme in 5G-assisted vehicular communication," *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 3703-3721, 2024.
[20] 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.
[21] W. Ahmad, M. A. Almaiah, A. Ali, and M. A. Al-Shareeda, "Deep learning based network intrusion detection for unmanned aerial vehicle (UAV)," in *Proceedings of the 2024 7th World Conference on Computing and Communication Technologies (WCCCT) (pp. 31–36). IEEE*, 2024.
[22] A. Alshuaibi, M. Almaayah, and A. Ali, "Machine learning for cybersecurity issues: A systematic review," *Security Challenges*, vol. 1, no. 1, p. 2, 2025.
[23] E. Alotaibi, R. B. Sulaiman, and M. Almaiah, "Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 1, pp. 47-59, 2025. https://doi.org/10.63180/jcsra.thestap.2025.1.5
[24] M. A. Al-shareeda *et al.*, "NE-CPPA: A new and efficient conditional privacy-preserving authentication scheme for vehicular ad hoc networks (VANETs)," *Appl. Math*, vol. 14, no. 6, pp. 1-10, 2020.
[25] A. A. Almuqren, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," *Journal of Cyber Security and Risk Auditing*, vol. 1, no. 1, pp. 1-11, 2025. https://doi.org/10.63180/jcsra.thestap.2025.1.1
[26] M. A. Al-Shareeda, S. Manickam, M. A. Saare, and N. C. Arjuman, "Proposed security mechanism for preventing fake router advertisement attack in IPv6 link-local network," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 29, pp. 518-526, 2023.
[27] R. Almanasir, D. Al-solomon, S. Indrawes, M. 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. https://doi.org/10.63180/jcsra.thestap.2025.2.3
[28] S. Alsahaim and M. Maayah, "Analyzing cybersecurity threats on mobile phones," *STAP Journal of Security Risk Management*, vol. 2023, no. 1, pp. 3–19, 2023. https://doi.org/10.63180/jsrm.thestap.2023.1.2
[29] M. Al-Shareeda, M. Ali, and S. Manickam, "The blockchain internet of things: Review, opportunities, challenges, and recommendations," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, pp. 1673-1683, 2023.
[30] F. Gebali and M. Mamun, "Review of physically unclonable functions (PUFs): Structures, models, and algorithms," *Frontiers in Sensors*, vol. 2, p. 751748, 2022. https://doi.org/10.3389/fsens.2021.751748
[31] M. A. Al-Shareeda, M. A. Saare, S. Manickam, and S. Karuppayah, "Validation of the toolkit for fake news awareness in social media," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 2, pp. 1171-1181, 2023.
[32] Z. G. Al-Mekhlafi *et al.*, "Integrating safety in VANETs: A taxonomy and systematic review of VEINS models," *IEEE Access*, 2024.
[33] M. A. Al-Shareeda, S. Manickam, M. A. Saare, S. Karuppayah, and M. A. Alazzawi, "A brief review of advanced monitoring mechanisms in peer-to-peer (P2P) botnets," in *Proceedings of the 2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM), 312–317. IEEE*, 2022.
[34] C. Annadurai *et al.*, "Biometric authentication-based intrusion detection using artificial intelligence internet of things in smart city," *Energies*, vol. 15, no. 19, p. 7430, 2022. https://doi.org/10.3390/en15197430
[35] Z. G. Al-Mekhlafi *et al.*, "Oblivious transfer-based authentication and privacy-preserving protocol for 5g-enabled vehicular fog computing," *IEEE Access*, 2024.
[36] M. G. Rao, S. Pawar, H. Priyanka, and K. H. K. Reddy, "Amalgamation of biometric deep features in smart city authentication," in *Proceedings of the 2022 6th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 1–6. IEEE*, 2022.
[37] M. A. Al-Shareeda, T. Gaber, M. A. Alqarni, M. H. Alkinani, A. A. Almazroey, and A. A. Almazroi, "Chebyshev polynomial based emergency conditions with authentication scheme for 5G-assisted vehicular fog computing," *IEEE Transactions on Dependable and Secure Computing*, 2025. https://doi.org/10.1109/TDSC.2025.3553868
[38] S. Gupta *et al.*, "Secure and lightweight authentication protocol for privacy preserving communications in smart city applications," *Sustainability*, vol. 15, no. 6, p. 5346, 2023. https://doi.org/10.3390/su15065346
[39] A. Alotaibi, H. Aldawghan, and A. Aljughaiman, "A review of the authentication techniques for internet of things devices in smart cities: Opportunities, challenges, and future directions," *Sensors*, vol. 25, no. 6, p. 1649, 2025. https://doi.org/10.3390/s25061649

[40] B. A. Mohammed *et al.*, "Efficient blockchain-based pseudonym authentication scheme supporting revocation for 5G-assisted vehicular fog computing," *IEEE Access*, vol. 12, pp. 33089–33099, 2024.

[41] M. Almaayah and R. Bin Sulaiman, "Cyber risk management in the Internet of Things: Frameworks, models, and best practices," *STAP Journal of Security Risk Management*, vol. 2024, no. 1, pp. 3–23, 2024. https://doi.org/10.63180/jsrm.thestap.2024.1.1

[42] W. Othman, M. Fuyou, K. Xue, and A. Hawbani, "Physically secure lightweight and privacy-preserving message authentication protocol for VANET in smart city," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 12, pp. 12902-12917, 2021.

[43] Z. G. Al-Mekhlafi *et al.*, "Lattice-based cryptography and fog computing based efficient anonymous authentication scheme for 5G-assisted vehicular communications," *IEEE Access*, vol. 12, pp. 71232–71247, 2024.

[44] S. Roy, D. Das, A. Mondal, M. H. Mahalat, S. Roy, and B. Sen, "PUF based lightweight authentication and key exchange protocol for IoT," in *Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT) (pp. 698–703)*, 2021.

[45] H. Albinhamad, A. Alotibi, A. Alagnam, M. Almaiah, and S. Salloum, "Vehicular Ad-hoc networks (VANETs): A key enabler for smart transportation systems and challenges," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 4-15, 2025. https://doi.org/10.63180/jjic.thestap.2025.1.2

[46] Z. G. Al-Mekhlafi *et al.*, "Coherent taxonomy of vehicular ad hoc networks (vanets)-enabled by fog computing: A review," *IEEE Sensors Journal*, 2024.

[47] M. Alshinwan, A. G. Memon, M. C. Ghanem, and M. Almaayah, "Unsupervised text feature selection approach based on improved Prairie dog algorithm for the text clustering," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 27-36, 2025. https://doi.org/10.63180/jjic.thestap.2025.1.4

[48] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing & Management*, vol. 58, no. 2, p. 102468, 2021. https://doi.org/10.1016/j.ipm.2020.102468

[49] S. R. Addula, S. Norozpour, and M. Amin, "Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 37-48, 2025. https://doi.org/10.63180/jjic.thestap.2025.1.5

[50] S. Alyounis and M. M. Yasin, "Secure framework for land record management using blockchain technology," *Journal of Cyber Security and Risk Auditing*, vol. 2023, no. 1, pp. 19-48, 2023.

[51] A. Padma and M. Ramaiah, "Blockchain based an efficient and secure privacy preserved framework for smart cities," *IEEE Access*, vol. 12, pp. 21985-22002, 2024.

[52] V. O. Nyangaresi, A. A. AlRababah, G. K. Yenurkar, R. Chinthaginjala, and M. Yasir, "Anonymous authentication scheme based on physically unclonable function and biometrics for smart cities," *Engineering Reports*, vol. 7, no. 1, p. e13079, 2025. https://doi.org/10.1002/eng2.13079

[53] Y. Li and Y. Tian, "A lightweight and secure three-factor authentication protocol with adaptive privacy-preserving property for wireless sensor networks," *IEEE Systems Journal*, vol. 16, no. 4, pp. 6197-6208, 2022.

[54] H. Wang *et al.*, "Joint biological ID: A secure and efficient lightweight biometric authentication scheme," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 2578-2592, 2022.