Journal of Computer Science

Research Article

A Lightweight and Privacy-Preserving Biometric Authentication Framework for Sustainable IoMT Systems

Saima Anwar Lashari[1], Mahmood A. Al-Shareeda[2,3], Mohammed Amin Almaiah[4] and Rami Shehab[5]

[1]*College of Computing and Informatics Saudi Electronic University Riyadh, 11673, Saudi Arabia*
[2]*Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq*
[3]*College of Engineering, Al-Ayen University, Thi-Qar, Iraq*
[4]*Department of Computer Science, King Abdullah the II IT School, The University of Jordan, Amman, Jordan*
[5]*Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa 31982, Saudi Arabia*

Article history
Received: 31-08-2025
Revised: 02-01-2026
Accepted: 05-01-2026

Corresponding Author:
Mahmood A. A. Al-Shareeda
Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
Email: m.almaiah@ju.edu.jo

Abstract: Biometric authentication provides secure, identity-bound access control for the Internet of Medical Things (IoMT), crucial for wearable, implantable, and ambient devices. However, the inherent immutability and sensitivity of biometric data pose severe privacy risks in the event of a breach. Furthermore, conventional public-key cryptography is often too computationally intensive for resource-constrained IoMT hardware. To address these challenges, this paper proposes a lightweight, privacy-preserving authentication framework for sustainable IoMT. Our system integrates cancellable biometrics with fuzzy extractors to generate secure, revocable, and non-invertible templates. We replace elliptic curve cryptography with lightweight symmetric primitives, TinyAES and SPECK, to minimize overhead. The mutual authentication protocol is formally verified using BAN logic, ensuring session security and freshness. Implemented on commercial IoMT devices (ESP32, Raspberry Pi), the framework demonstrates a 3.4× reduction in execution time, 57% lower memory usage, and 66% lower energy consumption compared to ECC-based schemes. In summary, this work presents an efficient, deployable architecture for viable and sustainable biometric authentication in resource-limited e-healthcare.

Keywords: Internet of Medical Things (IoMT), Biometric Authentication, Privacy-Preserving Security, Cancellable Biometrics, Fuzzy Extractors, Lightweight Cryptography, Sustainable IoT Systems

Introduction

Biometric authentication in the Internet of Medical Things (IoMT) has emerged as one of the most promising approaches to secure sensitive healthcare data while ensuring real-time patient identity in IoMT environments (Khan and Kabir, 2024; Adil et al., 2024; Robert et al., 2024). Internet of Medical Things (IoMT) systems, including wearable, implantable, and ambient medical devices, are becoming more popular in collecting, transmitting, and analyzing physiological data for remote diagnosis, chronic disease treatment, and emergency services (Rahmani et al., 2022; Dwivedi et al., 2022; Al-Shareeda et al., 2025b); Du et al., 2023; Rajawat et al., 2023). Nevertheless, these devices have extremely limited energy, memory, and computational capacity (Addula et al., 2025; Alshinwan et al., 2025; Albinhamad et al., 2025). Traditional authentication mechanisms be it password-based or using public key cryptography are insufficient or impractical in such environments, creating the need for more effective/efficient, usable, and privacy preserving alternatives (Mahamuni, 2024; Al-Mekhlafi et al., 2024b; Sarker et al., 2023; Ramya and Pradeep, 2024).

In this context, biometric authentication has a variety of advantages (Hussain et al., 2018; Saare et al., 2019a; 2019b; Alattas et al., 2023). Biometric traits (e.g., fingerprints, iris patterns, Electrocardiogram (ECG) signals) are unique, persistent and cannot be forgotten or entered by hand unlike passwords or tokens (Irkham et al., 2022; Al-Shareeda et al., 2025c; Majeed et al., 2023; Almazroi et al., 2024a). Nevertheless, biometric data is inherently sensitive and immutable; once compromised, it cannot be retired or replaced like a password (Jaafar et al., 2026; Alalisalem and Rahman, 2026; Ang et al., 2026). Moreover, most biometrics based authentication protocols store raw or static biometric templates, making users vulnerable to serious privacy threats in case of a breach (Akilan et al., 2023; Al-Shareeda et al., 2025a; Hadiyanto et al., 2023; Al-Mekhlafi et al., 2024a). This comes in addition to the heavy computational load of these common cryptographic operations (like elliptic curve encryption) that dramatically restrict use cases of any of such protocols for low-power medical devices (Bughio et al., 2024; Mohammed et al., 2024; Arefin et al., 2024).

The current IoMT schemes use either of the two manipulation-resistant design objectives, namely biometric template protection and cryptographic strengthening. However, most of the existing solutions are based on computationally expensive public-key schemes like ECC, that introduce significant delay, memory overhead and energy consumption to resource-constrained medical devices. Other schemes adopt lightweight cryptography while static biometric templates are still saved, providing only weak security protection against template exposure, cross-matching and long term identity theft. Therefore, the existing solutions are unable to simultaneously guarantee both biometric revocation and privacy preservation with full sustainability in practical IoMT scenarios.

To overcome drawbacks of existing schemes, this paper proposes the design and evaluation of a lightweight privacy preserving biometric authentication framework for IoMT. By this, the system makes use of cancellable biometrics transformations and fuzzy extractors to secure templates, allowing for compromising data to be securely revocable and substitutable. It integrates lightweight symmetric encryption (e.g., TinyAES, SPECK) interleaved in order to provide confidentiality over the channel with little overhead. We demonstrate the framework at low device level in a constrained real-world IoMT hardware setting and validate the practical feasibility by benchmarking the framework. This study makes the following contributions:

- We propose a unified biometric authentication framework for the Internet of Medical Things (IoMT) that achieves biometric template revocability, non-invertibility, and unlinkability through the combined use of cancellable biometric transformations and fuzzy extractors
- We design a lightweight security architecture that replaces computationally intensive ECC-based authentication mechanisms with efficient symmetric cryptographic primitives, making the framework suitable for resource constrained IoMT devices
- We formally analyze the proposed authentication protocol using Burrows Abadi Needham (BAN) logic to verify mutual authentication and session freshness under standard cryptographic assumptions
- We implement and experimentally evaluate the proposed framework on representative IoMT hardware platforms, including ESP32 microcontrollers and Raspberry Pi devices, demonstrating substantial reductions in execution time, memory footprint, and energy consumption compared to ECC-based schemes
- We introduce a sustainability-oriented authentication design that minimizes computational and storage overhead, thereby supporting scalable and long-term deployment in continuous remote healthcare monitoring environments

Related Work

The use of biometric authentication in conjunction with the Internet of Medical Things (IoMT) has become a point of interest due to the technology's ability to improve security and tailor healthcare services. Yet, the nature of IoMT devices themselves, have constraints like limited power, memory, and processing capacity which require the formulation of lightweight, secure, and privacy-aware authentication mechanisms. This includes authentication, template security, and system sustainability, yet many research efforts did not provide a holistic way to improve all three dimensions.

Biometric authentication techniques are particularly suitable for medical IoT systems as these systems involve a challenging context where traditional password or token-based solutions are impractical (Praveen and Pabitha, 2023; Al-Shareeda et al., 2024; Wu et al., 2023; Almazroi et al., 2023; Kabel et al., 2024). Various biometric modalities such as ECG, fingerprints, iris scan, and facial recognition have also been used in several schemes to verify patient identity (Aldaghlawy and Al-Shareeda, 2025; Hernandez-Jaimes et al., 2024; Abu Laila et al., 2025). These systems improve usability and identity assurance, but most of them still involve raw or hashed biometric data and therefore expose the system to unrecoverable compromises if breached (Jain et al., 2024; Almazroi et al., 2024b; Al-Na'amneh et al., 2025; Rajput et al., 2024).

Researchers have thus suggested different template protection mechanisms like cancellable biometrics, biometric hashing, and fuzzy extractors in order to mitigate biometric data breach risks (Sharma and Sharma, 2022; Al-Mekhlafi et al., 2024c; Musikawan et al., 2024). Cancellable biometrics apply noninvertible transformations to the raw features so that templates can be revoked and re-issued on the condition that some templates are compromised (Zeledon-C´ Ordoba et al., 2022); Al-Shareeda et al., 2025b; Yachongka et al., 2021). Unlike the above techniques, fuzzy extractors create stable cryptographic keys from noisy biometric inputs, without the need to store the original biometric vector. Despite benefits, few works embed these mechanisms in end-to-end IoMT frameworks or assess them on constrained medical devices (Wang et al., 2022; Mohammed et al., 2024b; Sumalatha et al., 2024; Mageshbabu and Mohana, 2024).

Sharma and Sharma (2022) presented an Internet of Medical Things e-Health architecture based on a blockchain. Combining decentralized communication, biometric identification and bio-key generation, the framework also takes account of data security, privacy protection and trust relationship while attending to limited resource environments and addressing threats including eavesdropping and denial of service. Khan et al. (2023) provided a feature oriented evaluation method of selecting secure authentication protocols on IoHT devices. By the integration of AHP with TOPSIS in multicriteria decision-making, the proposed mechanism found out a proper authentication scheme to improve security and trustworthiness in healthcare IoT. Goh et al. (2022) presented IoM hashing along with alignment free hashing and feature level fusion for multimodal biometric authentication framework. The technique preserves the biometric templates and works for heterogeneous features and competitive performance, with guaranteed privacy in state-of-the-art levels. Dalal (2025) presented an overview of the authentication and authorization systems for IoT in medicine. It explores conventional and advanced methods, offering user perspectives on such concepts as biometrics, multifactor authentication, AI techniques, blockchain applications and zero-trust modeling, as well implementation challenges and success factors essential for striking a balance between security considerations versus the operational realities required to provide quality patient care. Jain et al. (2024) presented a secure IoMT architecture comprising blockchain, cloud computing, and digital twins with lightweight authentication. Leveraging session keys and decentralized ledgers, the framework ensures the privacy of patients, integrity of data, and resistance to attacks while making health care monitoring efficient and secure based on formal proof. Prajapati et al. (2025) presented a qualitative analysis of authentication schemes applied for IOMT. It reviews the strengths and limitations of current solutions, presents best practices, and provides direction to select robust authentication mechanisms for secure communication, patient safety, and trustworthy IoMT functioning. Baniya et al. (2024) introduced the Internet of Medical Things and we investigate blockchainbased methods for secure device authentication and data security. It covers IoMT architecture, challenges and blockchain technologies for IoMT to advance the security, privacy, and efficiency in smart healthcare systems. The protocol presented by Byeon (2025) proposes a strong multifactor authentication scheme using ECC, biometrics and PUFs, it has some drawbacks regarding practical implementation in resource-constrained IoMT applications. Though ECC provides a higher level of security at lower key sizes, the scheme will impose high computational and memory overhead and is therefore not suitable for real-time deployment in low-power wearable or implantable devices. In addition, the protocol does not provide revoke-ability and unlink-ability for the biometric template, so the identity of a user cannot be securely reissued once disclosed and cross-platform correlation cannot be prevented. Also, the biometric data protection mechanism uses static storage instead of a cancellable or dynamically regenerable template, so it will be susceptible to long-term privacy-oriented attacks. The proposal also has no energy efficiency analysis and it does not use real IoMT hardware to test its performance. In contrast, the proposed framework resolves all the afore-mentioned issues by adopting lightweight symmetric encryption, cancellable biometric transformations and fuzzy extractors to ensure revokability, non-invertibility and low resource consumption which makes it fairly applicable to sustainable, secure IoMT authentication.

While there have been many works on biometric authentication for IoMT, the majority of them focus on security, template protection and computational complexity separately. Accordingly, they do not offer a comprehensive protection guaranteeing at the same time biometric privacy, revocability and sustainable operation under very tight resource constraints of medical IoT devices. Although the proposed model provides substantial advancement over IoMT authentication security and sustainability, it has several limitations. First, the experimental evaluation is performed on a representative biometric modalities (such as ECG and fingerprint) and simulated data of the biometric inputs instead of using clinical big datasets, which may make limitation in generalization of the characteristic properties of biometric performance. Second, hardware validation is based on the ESP32 (microcontroller) and Raspberry Pi (mini-computer) platforms; while these platforms are popular for prototyping within the IoMT domain, further evaluation on multiple device implementations with medical-grade standards and ultra-low power solutions would decisively reinforce respectively the relevance of the demonstrated results. Third, we consider system level sustainability metrics execution time, memory footprint and energy consumption instead of biometric recognition accuracy ones: FAR, FRR or EER. Last, the large-scale and long-term deployment sustainability have not been investigated thus far, an interesting direction for future research. As summarized in Table 1, existing IoMT authentication schemes typically address biometric security, cryptographic protection, or efficiency in isolation. In contrast, the proposed framework simultaneously ensures biometric template protection with revocability, lightweight cryptographic operation, real-hardware validation, and energy-aware design, addressing key limitations identified in prior studies.

Table 1: Qualitative comparison of representative IoMT authentication approaches

Scheme	Biometric Protection	Template Security	Revocability	Lightweight Crypto	Hardware Validation	Energy Analysis
Sharma and Sharma (2022)	Yes	Partial	No	No	No	No
Goh et al. (2022)	Yes	Yes	Partial	No	No	No
Jain et al. (2024)	Yes	Partial	No	Partial	No	No
Prajapati et al. (2025)	Yes	–	–	–	–	–
Byeon (2025)	Yes	Static	No	No (ECC)	No	No
Proposed Framework	Yes	Strong	Yes	Yes	Yes	Yes

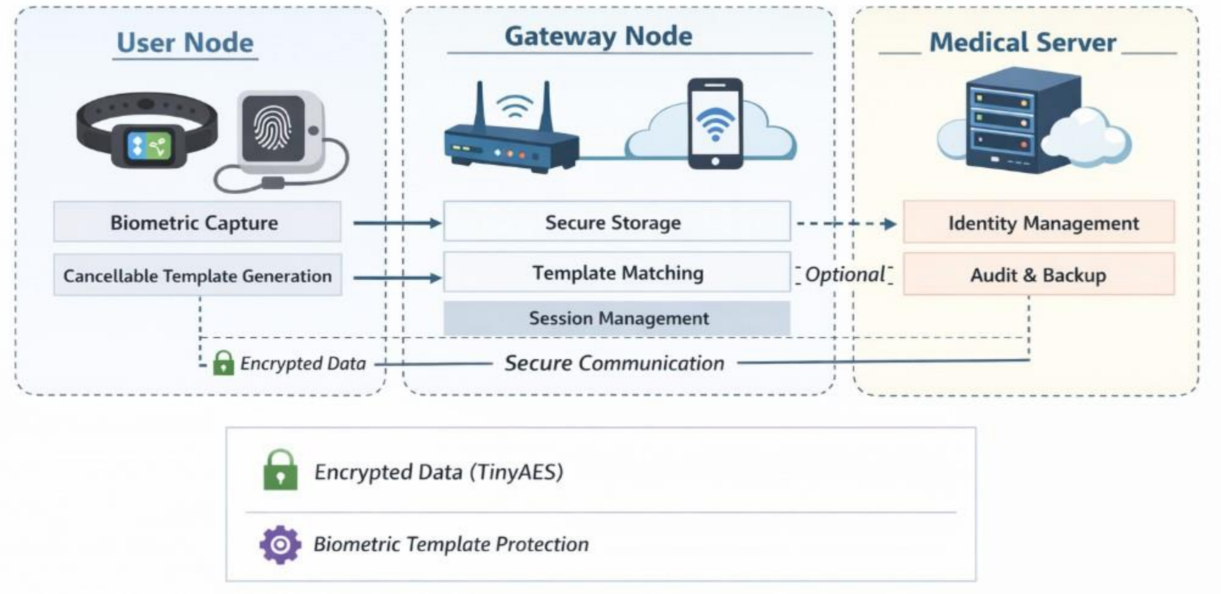

Fig. 1: Overview of the proposed biometric authentication framework for IoMT

Background

This section introduces the basic ideas and assumptions of the biometric authentication scheme. It presents the IoMT system model and threat assumptions; principle of biometric template protection, as well as significance of lightweight cryptography in memory constrained healthcare scenario are discussed.

System Overview

The proposed framework consists of two main phases, Secure Enrollment and Biometric Authentication, where lightweight cryptography is used along with the biometric template protection techniques, as shown in Figure 1. It runs with three primary entities:

- User Node (UN): The User Node is where the biometric data is collected and processed within the IoMT network. The UN that is usually a wearable device (e.g., smart band, smart ring), or implantable sensor (e.g., pacemaker, glucose monitor), is in the responsible for collecting the user's biometric characteristics including a fingerprint, iris pattern, or ECG signal. Because of the device's computational constraints and severe energy caveats, aside from the lightweight biometric transformation and encryption mechanism, everything occurs on the local device. The User Node protects against any unprotected sensitive raw biometric data from leaking off-device. Instead, a template of the biometric that's transformed into a cancellable template is created and transmitted to the Gateway Node securely. It ensures continued secure access by requiring a periodic re-authentication of the user
- Gateway Node (GWN): The Gateway Node is a trusted third party between User Node and Medical Server. The GWN is virtually deployed as mobile device, edge hub or embedded controller, and performs lite authentication processing, ephemeral storage of encrypted biometric data and cryptographic session management. The storage securely stores the encrypted biometric templates and helper data, performs the matching algorithm, and returns the authentication results in the local environment. It is more powerful than the User Node computationally, it can do things like compare the

stored tempate with the User and the stored timestamps vs. the current time, as well as handshakes for challenge/responses. Privacy-aware implementations treat the gateway as the last point of verification, which prevents biometrics from being transmitted to external servers that offer storage space. It also serves as the first line of defense against attacks from the outside world and allows for offloading processing work from more limited edge devices

- Medical Server (MS): An optional framework component for long term storage, identity management and audit logging. The MS can reside in the cloud or within a secure healthcare IT infrastructure and may what is in there? Encrypted biometric templates, authentication logs, backup copies of helper data, etc. Depending on privacy concerns, the MS can be configured to act as a secondary verification point or central authority for dealing with template revocation and the enforcement of policy. However, in privacy-preserving deployments the MS takes a passive role and only queries encrypted authentication records and metadata. This modular architecture enables the framework to tailor itself to varied operational modes centralized hospital networks, decentralized home care networks, or federated telemedicine networks

All messages are encrypted through lightweight symmetric ciphers such as TinyAES, while biometric templates are transformed using cancellable biometric transformations or fuzzy extractors before storage or transmission.

Biometric Template Protection Technique

Physiological features fingerprints, iris patterns, and electrocardiograms (ECG) are unique and universal, which gives biometric authentication the strong identity assurance that each user associated with the transaction is who they claim to be. Unlike tokens or passwords, biometric traits are permanent and non-replaceable (Champaneria et al., 2024; Sardar et al., 2024). If biometric templates are leaked, users cannot change. (invalidate/reset) their fingerprint or retina. Therefore, protecting biometric templates against unauthorized access is a crucial requirement for IoMT systems in healthcare settings where privacy violations can lead to serious damage (Rachapalli et al., 2024). To mitigate this proposal proposes a new framework which combines cancellable biometrics and fuzzy extractors, two common methodology to protect biometric templates such that revocation, unlinkability, and efficient processing are supported (Sardar et al., 2023; Segun et al., 2023).

Threat Model

The security of the framework is proven in the well-known Dolev-Yao threat model, where adversaries can intercept, replay, and modify any message over the network, but not to break cryptographic primitives. Threats considered include:

- Eavesdropping: Adversaries may eavesdrop on communication between the User Node (UN) and Gateway Node (GWN) to extract biometric templates, session identifiers, or helper data (Vo et al., 2023). Since either raw biometric data or its transformed version may be used to recover sensitive traits about identity, the framework makes sure that all transmissions are done using symmetric encryption (e.g., TinyAES, SPECK) with lightweight performance, such that unprotected biometric information never leaks out (Tolba and Derdour, 2021; Salem and Mehaoua, 2022)
- Biometric Template Theft: Stored biometric templates are indeed an attractive target for attackers if adequate measures for secure protection are not adopted. There is also a risk that a biometric template that has been stolen can be used to impersonate the user, not only in the compromised system, but if templates are reused in many systems, on multiple platforms (Liang et al., 2020). To overcome this, cancellable biometrics and fuzzy extractors are used by the system to safeguard the stored templates. Moreover, the non-invertible nature of these approaches means that even if an attacker were to steal the stored data, they would be unable to reconstruct the original biometric without significant computational resources (Khan and AbaOud, 2023)
- Replay Attacks: In a replay attack, an attacker (adv) reuses the defined ciphertext of the encrypted messages captured previously, such as enrollment templates or authentication requests, to access secure resources without proper authorization (Asif et al., 2025; Masud et al., 2021). The framework achieves this by introducing session-bound timestamps (T_i) and a mechanism of challenge-response to bind each authentication session to unique and time sensitive states. Rejection of stale or duplicate communication is enforced based on timestamp validation, or freshness checks of a nonce (Hegde et al., 2025)
- Cross-Matching and Linkability Attack: If the same biometric template or transformation is used across multiple services or sessions, an adversary could correlate these identities at least across different platforms, which is a severe violation of privacy (Li et al., 2021). However, various cancellable transformations over a variable number of rounds each introduces dynamic and user-specific keys, allowing proofs of unlinkability: any individual biometric template retains statistical independence (albeit imperfect) from all other templates, even if the templates were generated from identical sources (Xu et al., 2025; Poudel et al., 2024)
- Key Compromise and Insider Attacks: There is always a likelihood for adversaries to attack the

transformation keys (K_T) or encryption Keys (K) using side-channel attacks, memory leakage, or an insider attack. To counter such threats, transformation keys can be refreshed periodically, and compromised templates can be revoked and reissued with a new key (Ahn et al., 2011; Ghazal et al., 2022). On top of that, it is assumed that keys are either stored in trusted zones on the device or derived dynamically through need using trusted key-derivation schemes, minimizing persistent attack surfaces (Liu et al., 2024; Otorkpa et al., 2024)

The goal of the system is to build one or more core security properties guided by the threat model: Intensive registries: All biometric data in transit and at rest is encrypted by lightweight symmetric ciphers. Integrity: Data in template injections or tampering is prevented by binding it to session metadata and freshness values. Authentication: Users are verified to be who they say they are via privacy preserving matching techniques with secured templates. Non-invertible and Revocable: Compromised templates do not leak original biometric and are replaceable.

Lightweight Cryptography for IoMT

IoMT devices operate under strict constraints in terms of processing capability, memory size, and energy availability. Let Di denote an IoMT device with computational capacity Ci, memory Mi, and energy budget Ei, where Ci,Mi,Ei ≪ those of conventional computing systems. Cryptographic mechanisms deployed on such devices must therefore satisfy:

Otime(Enc,Dec) ≤ Ci,, Ospace(K,S) ≤ Mi,E(Enc,Dec) ≤ Ei, where Enc(·) and Dec(·) denote encryption and decryption operations, K is the secret key, and S represents internal state variables.

The public key cryptographic structures RSA and elliptic curve cryptography (ECC) are not conforming to these limits because of the expensive modulo exponential or scalar multiplication operations. Therefore, lightweight symmetric cryptography has been considered as a realization of security communication for the IoMT.

Symmetric Encryption Model: Let m ∈ {0,1}n be a plaintext message (e.g., protected biometric template or authentication data), and let k ∈ {0,1}λ be a symmetric secret key. A lightweight cipher computes: C = Enck(m), m = Deck(c), where Enck(·) and Deck(·) are designed to minimize round complexity, memory usage, and energy consumption while maintaining computational indistinguishability under standard security assumptions.

Representative Lightweight Cryptographic Algorithms

Table 2 presents representative cryptographic algorithms based on whether they are suitable for IoMT settings. Public- key systems such as RSA and ECC have high computational costs for expensive arithmetic operations, which are not suitable for resource-limited medical equipment. Compared to TinyAES and SPECK, lightweight symmetric ciphers require a much shorter computation cost but remain secure enough, thus making them more appropriate for long-term IoMT authentication and secure data transmission.

Key advantages of lightweight symmetric cryptography for IoMT:

- Low computational complexity: Encryption and decryption rely on simple operations (XOR, addition, bit rotation), significantly reducing execution time
- Minimal memory footprint: Small key sizes and limited internal state allow deployment on microcontrollers with constrained RAM and flash memory
- Energy efficiency: Reduced instruction count directly lowers energy consumption, which is critical for battery powered or implantable devices
- Compatibility with biometric protection: Lightweight encryption securely protects cancellable biometric templates and fuzzy extractor outputs during transmission and storage

Table 2: Comparison of cryptographic primitives for IoMT environments

Scheme	Type	Key Size	Computation Cost	IoMT Suitability
RSA	Public-key	2048 bits	Very High	No
ECC	Public-key	256 bits	High	Limited
AES	Symmetric	128 bits	Medium	Moderate
TinyAES	Symmetric	128 bits	Low	Yes
SPECK	Symmetric	64–128 bits	Very Low	Yes

In the proposed framework, lightweight symmetric cryptographic primitives such as TinyAES and SPECK are employed to secure authentication messages and protected biometric data. This design choice ensures confidentiality and integrity while preserving system-level sustainability, making the framework suitable for long-term IoMT deployment.

Materials and Methods

This paper introduces the lightweight and privacy-preserving biometric-based authentication for sustainable IoMT (Internet of Medical Things) systems. The framework solves the significant problem of maintaining immutable biometric credentials in medical environments where once biometric data is compromised, it suffers from an irrevocability not found in passwords or cryptographic tokens as used for password derived keys. As illustrated in Fig. 2, the proposed framework combines cancellable biometric transformations, fuzzy extractors and lightweight symmetric cryptography for security and privacy preserving, revocability, energy efficiency in a single authentication pipeline.

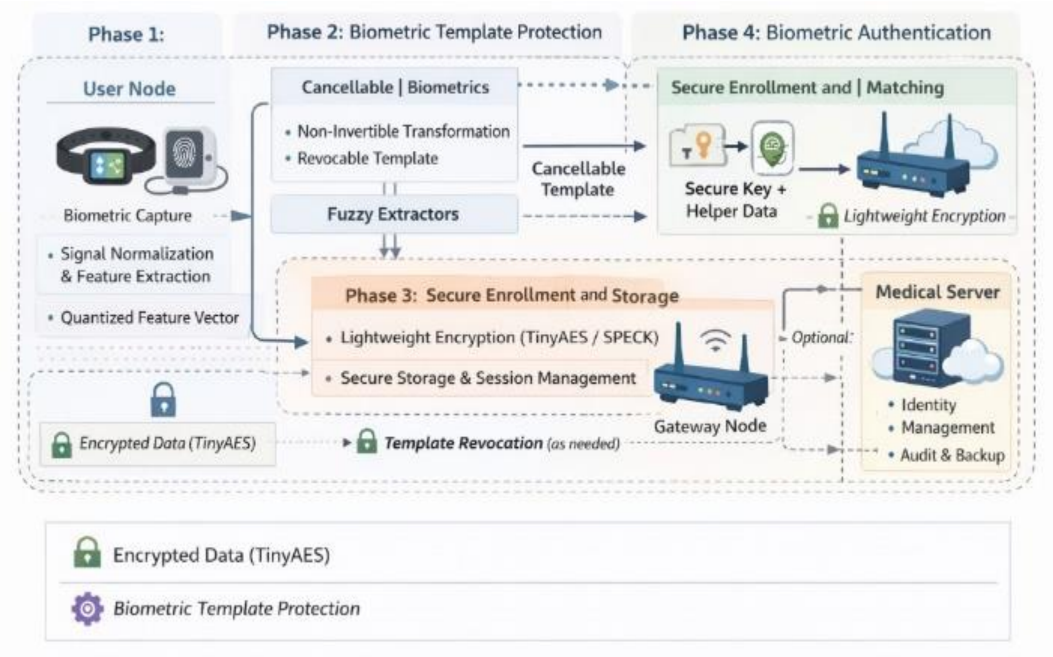
Phase 1:
Phase 2: Biometric Template Protection
Phase 4: Biometric Authentication
User Node
Biometric Capture
• Signal Normalization & Feature Extraction
• Quantized Feature Vector
Cancellable | Biometrics
• Non-Invertible Transformation
• Revocable Template
Fuzzy Extractors
Cancellable Template
Secure Enrollment and | Matching
Secure Key + Helper Data
Lightweight Encryption
Phase 3: Secure Enrollment and Storage
• Lightweight Encryption (TinyAES / SPECK)
• Secure Storage & Session Management
Gateway Node
Optional:
Medical Server
• Identity
• Management
• Audit & Backup
Encrypted Data (TinyAES)
Template Revocation (as needed)
Encrypted Data (TinyAES)
Biometric Template Protection

Fig. 2: Operational phases of the proposed framework with core activities

The system runs through four stages namely biometric acquisition and pre-processing, biometric template protection, secure enrollment and storage, search; biometric authentication and matching. Each phase is meticulously constructed to reduce the computing and communication cost, and yet retain biometric privacy protection as well as support template revocation in constrained IoMT environments.

Biometric Acquisition and Preprocessing

In the first phase, User Node (UN) obtains biometric signal (fingerprint, ECG signal and iris pattern of the user). Because of noise and randomness in sensing biometric information, the raw signal is preprocessed that includes normalizing (scale adjusting), filtering and feature extracting etc. according to preprocessing methods so as to have stable and reproducible representation of a biometric.

Algorithm 1 describes the preprocessing pipeline. The original biometric signal is preprocessed (normalization) to compensate for sensor noise and environmental factors, then features are extracted specifically in the domain (e.g., frequency of ECG or minutiae for fingerprints). Quantization is then used to convert the features into a fixed-length biometric token for further cryptographic operations.

Algorithm 1: Biometric Acquisition and Preprocessing

```
Input: Raw biometric signal $B$
Output: Quantized biometric feature vector $Q_B$
$B' \leftarrow$ Normalize($B$) ;
$F_B \leftarrow$ Feature Extract($B'$) ; // e.g., edges, peaks
$Q_B \leftarrow$ Quantize($F_B$) ;
return $Q_B$
```

Biometric Template Protection

In order to avoid leakage of raw biometric data, the extracted feature vector is secured by a cancellable biometric transformation, or alternatively, by a fuzzy extractor when the system configuration requires so. These servomechanisms provide for templates to be irrevocably hacked by an attacker or to have their content mis-used across apps.

Cancellable biometrics apply a non-invertible transformation of data dependent on a key in the template generation process to obtain revocable templates that can be re-issued if needed. By contrast, Fuzzy Extractors produce a secure key and related helper data from "better-than-random" biometric readings and a noisy reader by not storing biometric templates in the clear.

Algorithm 2 outlines both protection mechanisms. In both of these cases, the raw biometric data is not recoverable from the obfuscated outputs, thus providing non-invertibility and unlinkability at scale while keeping it inexpensive in terms of computational cost for IoMT devices.

Algorithm 2: Biometric Template Protection

```
Input: Quantized biometric vector $Q_B$, transformation key $K_T$
Output: Cancellable template $B_T$ or key $R$ and helper data $H$
Option A – Cancellable Biometrics;
BT ← Transform(QB,KT) ;// Apply BioHashing or projection
return $B_T$;
Option B – Fuzzy Extractor;
$(R,H) \leftarrow$ Gen($Q_B$) ;// Generate key + helper
return $(R,H)$
```

Secure Enrollment and Storage

After template protection, the cancellable template obtained or the fuzzy extractor output is forced to be encrypted with a low complexity symmetric cipher (TinyAES, SPECK) consort. The encrypted data is then sent to the Gateway Node (GWN) or, optionally, the Medical Server (MS) as per deployment configuration.

Finally, in Algorithm 3, we describe the secure enrollment. The secured biometric data are combined with the user's identifiers and session-related information, encrypted through a symetric key at GWN and saved securely. This approach reduces communication overhead and provides confidentiality of data, even when the data is intercepted or storage systems are compromised.

Algorithm 3: Secure Enrollment

```
Input: $B_T$ or $(R,H)$, symmetric key $K$
Output: Encrypted template $C$ stored at GWN
$M \leftarrow BT \,//\, H \,//\, IDU \,//\, T1$ ;
  C ← EncK(M) ;                  // Lightweight cipher
TinyAES, SPECK
Send $C$ to GWN or MS;
Store $C$ with session metadata (timestamp, ID);
```

Biometric Authentication and Matching

In the authentication phase a new biometric sample is obtained by and processed in accordance with the same Algorithm 3. Processing and protection schemes as were applied during enrollment. The newly computed protected representation is compared with the stored one in a privacy preserving way. In this case, the authentication can be based on matching of cancelable biometric templates or the reconstruction and verification of cryptographic keys generated by fuzzy extractors as in Algorithm 4. Authentication is validated if the matching measure exceeds a predetermined threshold or key reconstruction succeeds. In case of any compromise, the system also provides support for revoking templates by regenerating transformation parameters and then re-enrolling.

Algorithm 4: Biometric Authentication and Matching

```
Input: New biometric $B*$, stored $C$, key $K_T$, cipher key $K$
Output: Authentication result $B^{*'} \leftarrow$ Normalize($B*$) ;
$F_{B*} \leftarrow$ Feature _Extract($B^{*'}$) ;
$Q_{B*} \leftarrow$ Quantize($F_{B*}$) ;
Option A – Cancellable Biometrics: ;
$B_T^* \leftarrow$Transform($Q_{B*}$,$K_T$) ;
$(B_T,H) \leftarrow$ Dec$_K$($C$) ;
score ← Compare$(B_T^*, B_T)$ ;
Option B – Fuzzy Extractor: ;
$(R', \_) \leftarrow \mathrm{Rep}(Q_{B^*}, H)$ ;
Match ← $(R' == R)$ ;
if $score \geq threshold$ or $Match$ is $True$ then
    Accept authentication;
else
    Reject authentication;
```

Security Analysis

This section examines the security of the biometric authentication framework under practical adversarial model. The analysis is centered around biometric privacy preservation, resiliency to typical network and system level attacks, and template revocation taking into account the computational and energy requirements of IoMT environments.

Formal Security Analysis (BAN Logic)

To formally analyze the authentication correctness and session key agreement of the proposed framework, we employ Burrows Abadi Needham (BAN) logic, as shown in Figure 3. BAN logic is widely used to verify whether communicating entities can mutually authenticate each other and establish a shared secret under cryptographic assumptions.

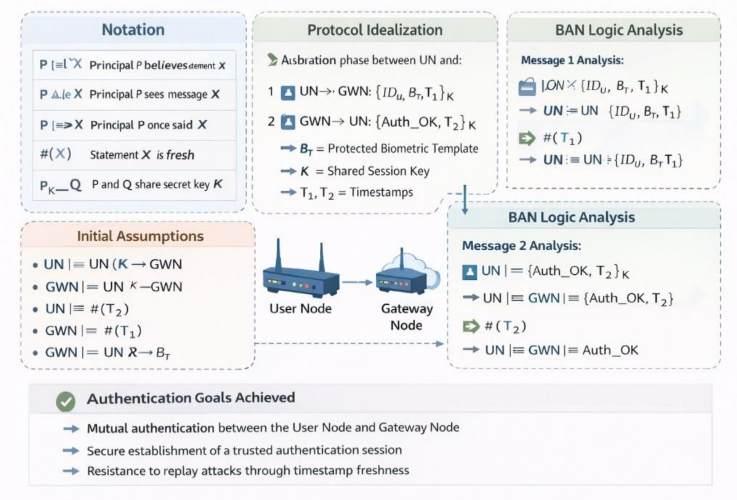
Notation
P |≡ X Principal P believes statement X
P ◁ X Principal P sees message X
P |~ X Principal P once said X
#(X) Statement X is fresh
P K— Q P and Q share secret key K
Protocol Idealization
Aısbration phase between UN and:
1 UN→ GWN: {ID_u, B_T, T_1}K
2 GWN→ UN: {Auth_OK, T_2}K
B_T = Protected Biometric Template
K = Shared Session Key
T_1, T_2 = Timestamps
BAN Logic Analysis
Message 1 Analysis:
|ON ⨯ {ID_U, B_T, T_1}K
UN |≡ UN {ID_U, B_T, T_1}
#(T_1)
UN |≡ UN ⊧ {ID_U, B_T T_1}
Initial Assumptions
UN |≡ UN (K → GWN
GWN |≡ UN K—GWN
UN |≡ #(T_2)
GWN |≡ #(T_1)
GWN |≡ UN R→ B_T
User Node
Gateway Node
BAN Logic Analysis
Message 2 Analysis:
UN |≡ {Auth_OK, T_2}K
UN |≡ GWN |≡ {Auth_OK, T_2}
#(T_2)
UN |≡ GWN |≡ Auth_OK
Authentication Goals Achieved
Mutual authentication between the User Node and Gateway Node
Secure establishment of a trusted authentication session
Resistance to replay attacks through timestamp freshness

Fig. 3: Formal security analysis of the proposed biometric authentication framework using BAN logic

1) *Notation:* The following BAN logic notations are used:

- $P \mid\equiv X$: Principal P believes statement X
- $P \triangleleft X$: Principal P sees message X
- $P \mid\sim X$: Principal P once said X
- $P \Rightarrow X$: Principal P has jurisdiction over X
- $\#(X)$: Statement X is fresh
- $P \leftrightarrow^{K} Q$: P and Q share secret key K
- $\{X\}_K$: Message X encrypted under key K

2) *Protocol Idealization:* The authentication phase between the User Node (UN) and Gateway Node (GWN) is abstracted into the following idealized message exchange:

$$UN \rightarrow GWN : \{ ID_U , B_T , T_1 \}_K \quad (1)$$

$$GWN \rightarrow UN : \{ Auth\_OK , T_2 \}_K \quad (2)$$

where B_T denotes the protected biometric template (or derived key), K is the shared symmetric session key, and T_1, T_2 are timestamps ensuring freshness:

3) *Initial Assumptions:* The following assumptions hold prior to protocol execution:

- $UN \mid\equiv UN \overset{K}{\leftrightarrow} GWN$
- $GWN \mid\equiv UN \overset{K}{\leftrightarrow} GWN$
- $UN \mid\equiv \#(T_2)$
- $GWN \mid\equiv \#(T_1)$
- $GWN \mid\equiv UN \Rightarrow B_T$

These assumptions indicate that both entities believe in the secrecy of the shared key, trust timestamp freshness, and that the Gateway Node trusts the User Node regarding ownership of biometric data:

4) *BAN Logic Analysis:* Message 1 Analysis:

Upon receiving Message 1, the Gateway Node observes: $GWN \triangleleft \{ID_U, B_T, T_1\}_K$, Using the message-meaning rule and the shared key assumption: $GWN \mid\equiv UN \mid\sim (ID_U, B_T, T_1)$. Since T_1 is fresh: $GWN \mid\equiv \#(T_1)$. Applying the nonce verification rule: $GWN \mid\equiv UN \mid\equiv (ID_U, B_T)$. Thus, the gateway Node believes that the biometric authentication request originated from the legitimate User Node.

Message 2 Analysis:

Upon receiving Message 2, the User Node observes: $UN \triangleleft \{Auth\ OK, T_2\}_K$. Applying the message-meaning rule: $UN \mid\equiv GWN \mid\sim (Auth\ OK, T_2)$. Given freshness of T_2:

$UN \mid\equiv \#(T_2)$. By nonce-verification: $UN \mid\equiv GWN \mid\equiv$

Auth OK. Therefore, the User Node believes that the authentication confirmation was generated by the legitimate Gateway Node:

5) *Authentication Goals:* The formal analysis confirms that the following security goals are achieved:

- Mutual authentication between the User Node and Gateway Node
- Secure establishment of a trusted authentication session
- Resistance to replay attacks through timestamp freshness

Consequently, under BAN logic assumptions and standard cryptographic primitives, the proposed framework satisfies the authentication correctness and session validity requirements for secure IoMT deployments.

Informal Security Analysis

In this paper, we model the adversary using the Dolev Yao threat model where it is assumed that the attacker has full control over a communication channel but cannot break any cryptographic primitive:

- Resilience to Theft of the Biometric Templates: The framework uses cancellable biometrics and fuzzy extractors, so that the original raw biometric data is not stored or transmitted. The template is rather transformed through a non-invertible function or used as a basis for deriving a key through a helper. If the attacked template is a protected template, we simply regenerate a new protected template with the same transformation key, thus revocable and unreusable. This ensures that attackers cannot use the biometric trait to recover the template (i.e., reverse engineer), or reuse the same template in another session or application
- Defense in Depth against Replay Attacks: In order to thwart replay attacks, all enrollment and authentication messages in the proposed framework are stamped with a timestamp and session-based identifier. Every authentication request is associated to a specific session context and the Gateway Node checks message freshness prior to its treatment. As a result, this prevents play back of previously-recorded messages or replay attacks since the stale timestamp and session id are rejected
- Protection of Biometric Data in Transit: Before data is sent from one node to another, all sensitive data (biometric templates, helper data and encrypted session metainformation) is encrypted using lightweight symmetric encryption algorithms such as TinyAES or SPECK. The rationale behind these two ciphers is their selection for compatibility with resource-limited hardware, but with sufficient strength to prevent interception of data or leakage of plaintext through a common communication channel
- Non-invertibility and Unlinkability: Let the cancellable template be defined as $B_T = f(Q_B, K_T)$, where Q_B is the quantized biometric feature vector and K_T is a user-specific secret transformation key. We

assume $f(\cdot)$ is a one-way transformation in the sense that for any PPT adversary A observing B_T (and public system parameters), the probability of recovering a valid preimage Q_B is negligible: $\Pr(A(B_T) = Q_B \wedge f(Q_B, K_T) = B_T) \leq \mathrm{negl}(\lambda)$. For the fuzzy extractor path $(R,H) \leftarrow \mathrm{Gen}(Q_B)$, H reveals negligible information about Q_B, and the derived key R is pseudorandom, i.e., $R \approx U$ given H

- Allow Exposure to Be Revoked: Specifically, if the transformation key is compromised (K_T), the proposed framework allows the template to be revoked and re-issued without requiring the user to modify their biometric trait. You may issue a new transformation key and derive a new cancellable template from the same biometric input. This property offers a strengthening for long-term resilience, in line with the tenets of forward secrecy, ensuring that the compromise of a session will not lead to compromising future sessions
- Confidentiality of Data in Transit: Sensitive data, such as protected biometrics templates, helper data and session metadata is encrypted through lightweight symmetric key primitives (TinyAES/SPECK). These algorithms achieve the goal of confidentiality and integrity with low computation cost and low energy consumption. Therefore, even if the communication path is eavesdropped, the adversaries cannot infer meaningful biometric or authentication information from these intercepted ciphertexts
- Resistance to Brute-force and Template Guessing: High entropy physiological signals are used to generate the biometric templates which are then transformed with keys or extractors. The output of these operations also tends to be very random and unpredictable. In addition to this, symmetric encryption prevents interception of ciphertext from revealing hints about the underlying biometric or helper values. Thus, a brute-force or dictionary attack on the encrypted template or helper data is computationally intractable
- Resistance to Biometric Template Compromise: The framework guarantees that raw biometric data is never saved or transmitted. Instead, biometric characteristics are secured by means of cancellable biometric transforms or fuzzy extractors. In cancellable biometric, a non-invertible key-dependent transformation is used to map the biometric feature vector and it is impossible to get back the original biometric template without learning the transformation key. This fuzzy extractor based method only stores fresh helper data along with a pseudorandom key that does not contain enough information to recover the original biometric input. If protected template is compromised, new template can be re-issued by changing transform key or extractor parameters with no need of user to change the biometric trait. This characteristic provides revocability and confines long-term privacy exposure
- Ethical and Privacy Considerations. The system adopts a privacy-by-design approach, ensuring that raw biometric data is neither stored nor transmitted and that the use of revocable, non-invertible, unlinkable biometric representations is enforced. Whenever feasible, biometric processing takes place locally on user devices and communication is done with only protected templates or cryptographically derived metadata. Accordingly, the framework is compliant with heavily adopted regulations and ethical considerations in healthcare for data protection including GDPR and HIPAA it reduces data exposure, making it possible to support user's consent through template revocation process, as well as long-term privacy risks of biometric immutability

Qualitative Comparison

Qualitative comparison between the proposed framework and the ECC-based biometric authentication scheme by Byeon (2025) is presented in Table 3, based on security properties specifically tailored for biometric-based IoMT systems. Instead of directly applying cryptographic verification, the comparison is mediated via analytical review of protocol design decisions. Although both schemes meet the basic security services, including confidentiality, integrity and authentication, our framework also realizes some biometric-related protections such as template revocability, non-invertibility and unlinkability which are not supported obviously in the compared ECC-based scheme. These are essential properties to address long-term privacy risks, as well as facilitate sustainable deployment in resource limited IoMT settings.

Table 3: Qualitative security property comparison between the proposed framework and an ECC-based IoMT authentication scheme

Security Property	Proposed Framework	(Byeon, 2025)
Confidentiality	⍰	⍰
Integrity	⍰	⍰
Authentication	⍰	⍰
Replay attack resistance	⍰	⍰
Biometric template revocability	⍰	⍰
Template non-invertibility	⍰	⍰
Session unlinkability	⍰	⍰
Key exposure mitigation	⍰	⍰
Low computational overhead	⍰	⍰

In this regard, the new framework achieves complete satisfaction of biometric template revocability, non-invertibility and unlinkability, where these properties have either been claimed but not realized in the original work. Most importantly, this has become possible with the coupling of cancellable biometrics and fuzzy extractors, which allow for privacy-preserving and revocable templates in cases of compromise. In contrast, the framework presented by Byeon (2025) stores biometric data in static form which makes them vulnerable to cross-matching and identity theft.

In addition, the proposed system has been proven secure against replay attacks and key exposure threats using timestamp validation, ephemeral session tokens, and the possibility to re-issue templates with a different transformation key. Byeon (2025) addresses these attacks somewhat but require smart card storage and expensive ECC operations, i.e., high overhead and low revocability.

Instead, it is fully implemented and shown to have a clear computational gain. The system's lightweight symmetric cryptography is designed for IoMT platforms, maximizing the energy efficiency and functionality of devices while implementing biometric authentication. This load comes from most data being cryptographically strong, requiring ECC operations and multistepped faction verification methods that are intensive by nature.

In summary, the presented framework provides a more extensive, adaptable, and sustainable security solution for biometric authentication in resource-constrained Internet of Medical Things (IoMT) environments, consequently bridging several gaps created by existing solutions.

Results and Discussion

In this section, we discuss the performance of our biometric authentication scheme in terms of execution time, memory usage, and energy. The evaluation is designed to evaluate the applicability of our framework with resource constrained IoMT devices, and the efficiency comparison against ECC-based authentication protocol for biometrics introduced by Byeon (2025). All the experiments aim to illustrate system-level efficiency, rather than biometric recognition accuracy, which is beyond the scope of this study.

Experimental Setup

All experiments have been performed on popular IoMT hardware platforms for prototyping and edge deployment. In this paper User Nodes ran on a ESP32 microcontroller (dual-core, 160 MHz, 520 KB SRAM), whereas the gateway operations were performed using a Raspberry Pi 3B (quadcore, 1.2 GHz, 1 GB RAM). The model-based design was realized in embedded C and MicroPython. Biometric inputs were created by simulated fingerprint and ECG signals, thus making them repeatable in their experiments. All reported statistics are averaged over multiple authentication runs under the same conditions.

Execution Time Analysis

Figure 4 shows the execution time for enrolling and verification of a user, comprising biometric template protection, encryption and matching. The average execution time per authentication session of the proposed framework is 6.7 ms, while that of the ECC-based protocol in Byeon (2025) at before, which corresponds to a reduction of about 3.4×. This performance boost is largely thanks to the utilization of lightweight symmetric primitives (TinyAES) and efficient biometric template protection techniques that bypass computationally-intensive public key operations.

Memory Footprint Analysis

The memory usage of the proposed framework is compared with ECC-based method in Fig. 5. The proposed implementation uses around 6.5 KB of memory, while the ECCbased scheme takes over 15.2 KB because of elliptic-curve operations, biometric hashing and PUF related blocks. This represents approximately a 57% decrease in memory. This memory efficiency can be especially valuable for embedded medical devices that have constraints on the amount of RAM and flash storage, allowing for more flexible deployment options and better system responsiveness.

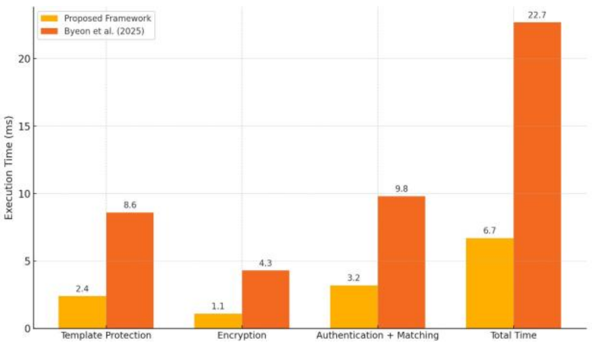

Fig. 4: Execution time comparison per operation

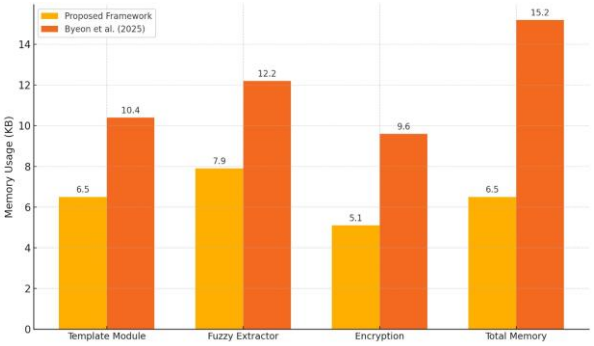

Fig. 5: Memory footprint comparison per component

Energy Consumption Analysis

The energy usage per authentication session is presented in Fig. 6. The proposed design uses around 0.74 mWh/session (compared to 2.18 mWh for the ECC-based approach) resulting into 66% savings in energy overhead. Reduced energy consumption comes mostly from the reduction in execution time but also by excluding costly public-key cryptographic operations. This enhancement is especially important for the wearable, battery-operated IoMT devices that will perform authentications continuously or many times a day.

All these results, when taken together, confirm that the proposed framework indeed provides strong biometric security, while at the same time low time, memory and energy overhead. Its practicality makes it a suitable option for real-world IoMT deployments, namely in remote, battery-limited or low supervision environments.

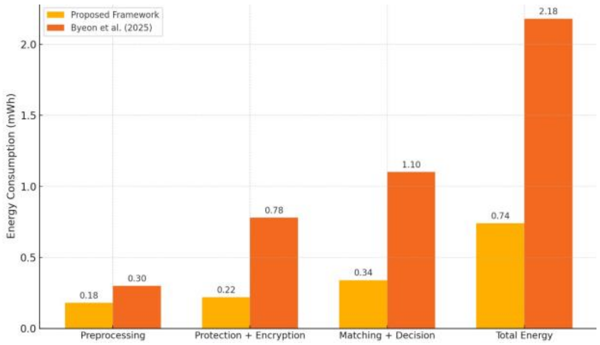

Fig. 6: Energy consumption comparison per phase

Conclusion

In this paper, we introduced a lightweight and privacy preserving biometric authentication scheme designed for resource-limited Internet of Medical Things (IoMT) systems. By combining cancellable biometric transformations with the concept of Fuzzy Extractor, it ensures that immutable biometric credentials are immune to long-term privacy risks caused by identity leakage due to use of un-revoked and non-invertible representations. For practical deployability, the framework uses small symmetric cryptographic building blocks (e.g., TinyAES and SPECK) rather than costly public-key primitives (e.g., elliptic curve cryptography). Performance evaluation on representative IoMT hardware platforms shows that the proposed approach can greatly reduce the execution time, memory overhead and energy consumption compared with an ECC-based baseline, with about 3.4× faster authentication speed, and reducing memory usage and saving energy by 57 and 66%. We also show from efficiency comparison that the proposed framework enjoys essential biometric-specific security properties, such as template revocability and non-invertibility, unlinkability etc., which have been ignored in most of the previous biomedical authentication protocols. Both informal and formal security analyses also demonstrated the correctness of authentication process, as well as the resilience to typical network-level attacks. In summary, the proposed protocol is a balance tradeoff among security, privacy and sustainability, which can be applied to potential real IoMT environments where wearable healthcare device and remote patient monitoring system are worked. Future developments will include the extension of the evaluation on clinical biometric datasets, integration of postquantum cryptographic primitives and validation in large-scale health infrastructures.

Acknowledgment and Funding Information

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. Grant No. KFU260074)

Authors' Contributions

Saima Anwar Lashari: Conceptualization, methodology, software, writing original draft.

Mahmood A. Al-Shareeda: Conceptualization, formal analysis, software, validation, writing review and edited.

Mohammed Amin Almaiah: Methodology, validation, formal analysis, supervision, writing review and edited.

Ethics

This study does not involve human participants, patients, clinical trials, or animal subjects. All biometric data used were synthetically generated or simulated. Therefore, ethical approval and informed consent were not required.

Conflict of Interest

The authors declare that there are no commercial or financial relationships that could be construed as a potential conflict of interest.

References

Al-Shareeda, M., Mohammed Ali, A., Adel Hammoud, M., Haider Muhammad Kazem, Z., & Aqeel Hussein, M. (2025a). Secure IoT-Based Real-Time Water Level Monitoring System Using ESP32 for Critical Infrastructure. *Journal of Cyber Security and Risk Auditing*, *2025*(2), 44–52. https://doi.org/10.63180/jcsra.thestap.2025.2.4

Al-Shareeda, M. A., Gaber, T., Alqarni, M. A., Alkinani, M. H., Almazroey, A. A., & Almazroi, A. A. (2025b). Chebyshev Polynomial Based Emergency Conditions with Authentication Scheme for 5G-Assisted Vehicular Fog Computing. *IEEE Transactions on Dependable and Secure Computing*, *22*(5), 4795–4812. https://doi.org/10.1109/tdsc.2025.3553868

Al-Shareeda, M. A., Obaid, A. A., & Almajid, A. A. H. (2025c). The Role of Artificial Intelligence in Bodybuilding: A Systematic Review of Applications, Challenges, and Future Prospects. *Jordanian Journal of Informatics and Computing*, *2025*(1), 16–26. https://doi.org/10.63180/jjic.thestap.2025.1.3

Al-Shareeda, M. A., Jafer, A. N., Hashem, M. T., & Fajr, M. S. (2024). Secure Offline Smart Office Automation System Using ESP32 and Bluetooth Control Architecture. *Journal of Cyber Security and Risk Auditing*, *2024*(1), 3–13. https://doi.org/10.63180/jcsra.thestap.2024.1.2

Abu Laila, D., Aljawarneh, M., Al-Na'amneh, Q., & Bin Sulaiman, R. (2025). Optimizing Intrusion Detection Systems through Benchmarking of Ensemble Classifiers on Diverse Network Attacks. *STAP Journal of Security Risk Management*, *2025*(1), 71–84. https://doi.org/10.63180/jsrm.thestap.2025.1.4

Addula, S. R., Norozpour, S., & Amin, M. (2025). Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing. *Jordanian Journal of Informatics and Computing*, *2025*(1), 38–48. https://doi.org/10.63180/jjic.thestap.2025.1.5

Adil, M., Khan, M. K., Kumar, N., Attique, M., Farouk, A., Guizani, M., & Jin, Z. (2024). Healthcare Internet of Things: Security Threats, Challenges, and Future Research Directions. *IEEE Internet of Things Journal*, *11*(11), 19046–19069. https://doi.org/10.1109/jiot.2024.3360289

Ahn, R.-S., Yoon, E.-J., Bu, K.-D., & Nam, I.-G. (2011). Secure and Efficient DB Security and Authentication Scheme for RFID System. *The Journal of Korea Information and Communications Society*, *36*(4C), 197–206.https://doi.org/10.7840/kics.2011.36c.4.197

Alalisalem, D., & Rahman, H. (2026). Securing Healthcare Digital Twin with Blockchain: A Systematic Review of Architecture, Threats and Evaluation. *STAP Journal of Security Risk Management*, *2026*(1), 46–66. https://doi.org/10.63180/jsrm.thestap.2026.1.3

Alattas, A. H. A., Al-Shareeda, M. A., Manickam, S., & Saare, M. A. (2023). Enhancement of NTSA Secure Communication with One-Time Pad (OTP) in IoT. *Informatica*, *47*(1). https://doi.org/10.31449/inf.v47i1.4463

Albinhamad, H., Alotibi, A., Alagnam, A., Almaiah, M., & Salloum, S. (2025). Vehicular Ad-hoc Networks (VANETs): A Key Enabler for Smart Transportation Systems and Challenges. *Jordanian Journal of Informatics and Computing*, *2025*(1), 4–15. https://doi.org/10.63180/jjic.thestap.2025.1.2

Aldaghlawy, H. J., & Al-Shareeda, M. A. (2025). The Role of Simulating Digital Threats through Interactive Theater Performances. *Journal of Cyber Security and Risk Auditing*, *2025*(4), 276–286. https://doi.org/10.63180/jcsra.thestap.2025.4.7

Almazroi, A. A., Alkinani, M. H., Al-Shareeda, M. A., & Manickam, S. (2024a). A Novel DDoS Mitigation Strategy in 5G-Based Vehicular Networks Using Chebyshev Polynomials. *Arabian Journal for Science and Engineering*, *49*(9), 11991–12004. https://doi.org/10.1007/s13369-023-08535-9

Almazroi, A. A., Alqarni, M. A., Al-Shareeda, M. A., & Manickam, S. (2023). L-CPPA: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system. *PLOS ONE*, *18*(10), e0292690. https://doi.org/10.1371/journal.pone.0292690

Almazroi, A. A., Alqarni, M. A., Al-Shareeda, M. A., Alkinani, M. H., Almazroey, A. A., & Gaber, T. (2024b). FCAVBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network. *Internet of Things*, *25*, 101096. https://doi.org/10.1016/j.iot.2024.101096

Al-Mekhlafi, Z. G., Al-Janabi, H. D. K., Khalil, A., Al-Shareeda, M. A., Mohammed, B. A., Alsadhan, A. A., Alayba, A. M., Shamsan Saleh, A. M., Al-Reshidi, H. A., & Almekhlafi, K. (2024a). Lattice-Based Cryptography and Fog Computing Based Efficient Anonymous Authentication Scheme for 5G-Assisted Vehicular Communications. *IEEE Access*, *12*, 71232–71247. https://doi.org/10.1109/access.2024.3402336

Al-Mekhlafi, Z. G., Anwar Lashari, S., Al-Shareeda, M. A., Abdulkarem Mohammed, B., Sulaiman Alshudukhi, J., Al-Dhlan, K. A., & Manickam, S. (2024b). Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs) Enabled by Fog Computing: A Review. *IEEE Sensors Journal*, *24*(19), 29575–29602. https://doi.org/10.1109/jsen.2024.3436612

Al-Mekhlafi, Z. G., Anwar Lashari, S., Mohammed Hachim Altmemi, J., Al-Shareeda, M. A., Abdulkarem Mohammed, B., Sallam, A. A., Ali Al-Qatab, B., Alshammari, M. T., & Alayba, A. M. (2024c). Oblivious Transfer-Based Authentication and Privacy-Preserving Protocol for 5G-Enabled Vehicular Fog Computing. *IEEE Access*, *12*, 100152–100166. https://doi.org/10.1109/access.2024.3429179

Al-Na'amneh, Q., Aljawarneh, M., Alhazaimeh, A. S., Hazaymih, R., Shah, S. M., & Dhifallah, W. (2025). Securing Trust: Rule-Based Defense Against On/Off and Collusion Attacks in Cloud Environments. *STAP Journal of Security Risk Management*, *2025*(1), 85–114. https://doi.org/10.63180/jsrm.thestap.2025.1.5

Alshinwan, M., Memon, A. G., Ghanem, M. C., & Almaayah, M. (2025). Unsupervised text feature selection approach based on improved Prairie dog algorithm for the text clustering. *Jordanian Journal of Informatics and Computing*, *2025*(1), 27–36. https://doi.org/10.63180/jjic.thestap.2025.1.4

Ang, S., Ho, M., Huy, S., & Janarthanan, M. (2026). A Multi-Layered Adaptive Cybersecurity Framework for the Banking Sector Integrating Next-Gen Firewalls with AI-Driven IDPS. *STAP Journal of Security Risk Management*, *2026*(1), 67–76. https://doi.org/10.63180/jsrm.thestap.2026.1.4

Arefin, Md. S., Rahman, M. M., Hasan, Md. T., & Mahmud, M. (2024). A Topical Review on Enabling Technologies for the Internet of Medical Things: Sensors, Devices, Platforms, and Applications. *Micromachines*, *15*(4), 479. https://doi.org/10.3390/mi15040479

Asif, M., Abrar, M., Salam, A., Amin, F., Ullah, F., Shah, S., & AlSalman, H. (2025). Intelligent two-phase dual authentication framework for Internet of Medical Things. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-024-84713-5

Akilan, U, H., Prakash, I. B., and Rajkumar, K. (2023). Exploring the Impact and Potential of the Internet of Medical Things (IoMT): A Comprehensive Review. *Proceedings of the International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 967–972. https://doi.org/10.1109/icac3n60023.2023.10541669

Baniya, P., Agrawal, A., Nand, P., Bhushan, B., & Bhattacharya, P. (2024). Blockchain-Based Security Sustainable Framework for IoMT Applications and Industry 5.0. *Soft Computing in Industry 5.0 for Sustainabilit*, 377–406. https://doi.org/10.1007/978-3-031-69336-6_17

Bughio, K. S., Cook, D. M., & Shah, A. (2024). Investigating the intersections of vulnerability detection and Internet of Medical Things (IoMT) in healthcare, a scoping review protocol for Remote Patient Monitoring. *Research, Society and Development*, *13*(6), e11313646080. https://doi.org/10.33448/rsd-v13i6.46080

Byeon, H. (2025). Vulnerability Analysis of Privacy-Preserving Four-Factor Authentication for Medical IoT Environments and Sustainable Development Goals. *Journal of Lifestyle and SDGs Review*, *5*(4), e05225. https://doi.org/10.47172/2965-730x.sdgsreview.v5.n04.pe05225

Champaneria, V. H., Zaveri, M. A., & Patel, S. J. (2024). A Secure Template Protection Technique for Robust Biometric Systems. *Proceedings of the IEEE Students Conference on Engineering and Systems (SCES)*. 2024 IEEE Students Conference on Engineering and Systems (SCES), Prayagraj, India. https://doi.org/10.1109/sces61914.2024.10652322

Dalal, A. (2025). Secure authentication and authorization in the internet of medical things. *CRC Press*, 35–54. https://doi.org/10.1201/9781003640325-3

Du, H., Wang, J., Niyato, D., Kang, J., Xiong, Z., Guizani, M., & Kim, D. I. (2023). Rethinking Wireless Communication Security in Semantic Internet of Things. *IEEE Wireless Communications*, *30*(3), 36–43. https://doi.org/10.1109/mwc.011.2200547

Dwivedi, R., Mehrotra, D., & Chandra, S. (2022). Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *Journal of Oral Biology and Craniofacial Research*, *12*(2), 302–318. https://doi.org/10.1016/j.jobcr.2021.11.010

Ghazal, T. M., Hasan, M. K., Abdallah, S. N. H., & Abubakkar, K. A. (2022). Secure IoMT Pattern Recognition and Exploitation for Multimedia Information Processing using Private Blockchain and Fuzzy Logic. *ACM Transactions on Asian and Low-Resource Language Information Processing*, *21*, 2375–4699. https://doi.org/10.1145/3523283

Goh, Z. H., Wang, Y., Leng, L., Liang, S.-N., Jin, Z., Lai, Y.-L., & Wang, X. (2022). A Framework for Multimodal Biometric Authentication Systems With Template Protection. *IEEE Access*, *10*, 96388–96402. https://doi.org/10.1109/access.2022.3205413

Hadiyanto, H., Sukamto, S., Suryono, S., & Kurnianingsih, K. (2023). A Review on Internet of Medical Things (IoMT): A Case Study for Preeclampsia. *E3S Web of Conferences*, *448*, 02058. https://doi.org/10.1051/e3sconf/202344802058

Hegde, M., M., K., Hegde, V., Rao, R. R., Mantoor, V. M., & Bhat, R. (2025). PLASMA-Privacy-Preserved Lightweight and Secure Multi-level Authentication scheme for IoMT-based smart healthcare. *Open Computer Science*, *15*(1), 20250024. https://doi.org/10.1515/comp-2025-0024

Hussain, A., Saare, M. A., Jasim, O. M., & Mahdi, A. A. (2018). A heuristic evaluation of iraq e-portal. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC*, *10*(1–10), 103–107.

Hernandez-Jaimes, M. L., Martínez-Cruz, A., Ramírez-Gutiérrez, K. A., & Guevara-Martínez, E. (2024). Enhancing Machine Learning Approach Based on Nilsimsa Fingerprinting for Ransomware Detection in IoMT. *IEEE Access*, *12*, 153886–153897. https://doi.org/10.1109/access.2024.3480889

Irkham, I., Ibrahim, A. U., Nwekwo, C. W., Al-Turjman, F., & Hartati, Y. W. (2022). Current Technologies for Detection of COVID-19: Biosensors, Artificial Intelligence and Internet of Medical Things (IoMT): Review. *Sensors*, *23*(1), 426. https://doi.org/10.3390/s23010426

Jaafar, H. S., Abed, A. A., & Al-Shareeda, M. A. (2026). A Secure Industrial Internet of Things (IIoT) Framework for Real-Time PI Control and Cloud-Integrated Industrial Monitoring. *STAP Journal of Security Risk Management*, *2026*(1), 77–86. https://doi.org/10.63180/jsrm.thestap.2026.1.5

Jain, A., Garg, M., Gupta, A., Batra, S., & Narwal, B. (2024). IoMT-BADT: A blockchain-envisioned secure architecture with a lightweight authentication scheme for the Digital Twin environment in the Internet of Medical Things. *The Journal of Supercomputing*, *80*(11), 16222–16253. https://doi.org/10.1007/s11227-024-06026-8

Khan, H. U., Ali, Y., & Khan, F. (2023). A features-based privacy preserving assessment model for authentication of internet of medical things (iomt) devices in healthcare. *Mathematics*, *11*(5), 1197. https://doi.org/10.3390/math11051197

Khan, L., & Kabir, F. (2024). In-depth Analysis on Secure and Privacy-Preserving Smart Care Homes based on Internet of Medical Things (IoMT). *Proceedings of the IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, 1–6. https://doi.org/10.1109/iatmsi60426.2024.10503242

Khan, M. F., & Abaoud, M. (2023). Blockchain-Integrated Security for Real-Time Patient Monitoring in the Internet of Medical Things Using Federated Learning. *IEEE Access*, *11*, 117826–117850. https://doi.org/10.1109/access.2023.3326155

Kabel, S. A. E.-M., El-Banby, G. M., Abou Elazm, L. A., El-Shafai, W., El-Bahnasawy, N. A., El-Samie, F. E. A., Elazm, A. A., Siam, A. I., & Abdelhamed, M. A. (2024). Securing Internet-of-Medical-Things networks using cancellable ECG recognition. *Scientific Reports*, *14*(1). https://doi.org/10.1038/s41598-024-54830-2

Li, W., Meng, W., & Yang, L. T. (2021). Enhancing trust-based medical smartphone networks via blockchain-based traffic sampling. *Proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 122–129. https://doi.org/10.1109/trustcom53373.2021.00034

Liang, H., Wu, J., Zheng, X., Zhang, M., Li, J., & Jolfaei, A. (2020). Fog-based Secure Service Discovery for Internet of Multimedia Things. *ACM Transactions on Multimedia Computing, Communications, and Applications*, *16*(3s), 1–23. https://doi.org/10.1145/3415151

Liu, G., Xie, H., Wang, W., & Huang, H. (2024). A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. *Journal of Cloud Computing*, *13*(1), 44. https://doi.org/10.1186/s13677-024-00608-w

Mageshbabu, M., & Mohana, J. (2024). Enhancing Biometric Security: A Machine Learning Approach to ECG-Based Authentication. *Proceedings of the Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI)*, 1654–1659. https://doi.org/10.1109/icoici62503.2024.10696328

Mahamuni, C. V. (2024). Improving Cardiopulmonary Resuscitation (CPR): Integrating Internet of Medical Things (IoMT) and Machine Learning (ML) - A Review. *Recent Research Reviews Journal*, *3*(1), 70–87. https://doi.org/10.36548/rrrj.2024.1.005

Majeed, F., Nazir, M., & Schneider, J. (2023). ISA: Internet of Medical Things (IoMT) in Smart Healthcare and its Applications: A Review. *Proceedings of the International Conference on Artificial Intelligence (ICAI)*, 129–135. https://doi.org/10.1109/icai58407.2023.10136661

Masud, M., Gaba, G. S., Alqahtani, S., Muhammad, G., Gupta, B. B., Kumar, P., & Ghoneim, A. (2021). A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care. *IEEE Internet of Things Journal*, *8*(21), 15694–15703. https://doi.org/10.1109/jiot.2020.3047662

Mohammed, B. A., Al-Shareeda, M. A., Al-Mekhlafi, Z. G., Alshudukhi, J. S., & Al-Dhlan, K. A. (2024). HAFC: Handover Authentication Scheme Based on Fog Computing for 5G-Assisted Vehicular Blockchain Networks. *IEEE Access*, *12*, 6251–6261. https://doi.org/10.1109/access.2024.3351278

Musikawan, P., Kongsorot, Y., Aimtongkham, P., & So-In, C. (2024). Enhanced Multigrained Scanning-Based Deep Stacking Network for Intrusion Detection in IoMT Networks. *IEEE Access*, *12*, 152482–152497. https://doi.org/10.1109/access.2024.3480011

Otorkpa, O. J., Olaniyan, O. E., & Onifade, A. A. (2024). Protecting patient privacy in the age of smart healthcare: practical cybersecurity measures for individuals and healthcare providers. *World Journal of Advanced Research and Reviews*, *23*(1), 3047–3050. https://doi.org/10.30574/wjarr.2024.23.1.2334

Poudel, A., Mohanty, S., & Pradhan, M. (2024). Design of Lightweight Authentication Scheme for Low Power Internet of Medical Things (IoMT). *Proceedings of the International Conference on Smart Power Control and Renewable Energy (ICSPCRE)*, 1–6. https://doi.org/10.1109/icspcre62303.2024.10675052

Prajapati, S. K., Kulkarni, P., & Balaji, C. G. (2025). Qualitative Analysis of Authentication Mechanisms for Secure Communication in the Internet of Medical Things. *Internet of Medical Things for Healthcare Applications*, 133–164. https://doi.org/10.4018/979-8-3373-4332-7.ch005

Praveen, R., & Pabitha, P. (2023). A secure lightweight fuzzy embedder based user authentication scheme for internet of medical things applications. *Journal of Intelligent & Fuzzy Systems*, *44*(5), 7523–7542. https://doi.org/10.3233/jifs-223617

Rahmani, M. K. I., Shuaib, M., Alam, S., Siddiqui, S. T., Ahmad, S., Bhatia, S., & Mashat, A. (2022). Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review. *Computational Intelligence and Neuroscience*, *2022*, 1–14. https://doi.org/10.1155/2022/9766844

Rajawat, A. S., Goyal, S. B., Bedi, P., Jan, T., Whaiduzzaman, M., & Prasad, M. (2023). Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT). *Future Internet*, *15*(8), 271. https://doi.org/10.3390/fi15080271

Rajput, A., Ahmed, S., & Kasher, L. (2024). Patients' Mental Health Data and Internet of Medical Things (IoMT) Safety: Analyzing Raspberry pi vulnerabilities. *Rawal Medical Journal*, *49*(1), 1. https://doi.org/10.5455/rmj.20240506101607

Ramya, M., & Pradeep, S. (2024). A review on security issues and attack detection in Internet of Medical Things (IoMT). *AIP Conference Proceedings*, 020037. https://doi.org/10.1063/5.0217101

Rachapalli, D., Dondeti, V., & Kalluri, H. K. (2024). Multimodal Cancellable Biometric Template Protection and Person Verification in Transformed Domain. *IEEE Access*, *12*, 173557–173582. https://doi.org/10.1109/access.2024.3501368

Robert, W., Denis, A., Thomas, A., Samuel, A., Kabiito, S. P., Morish, Z., & Ali, G. (2024). A Comprehensive Review on Cryptographic Techniques for Securing Internet of Medical Things: A State-of-the-Art, Applications, Security Attacks, Mitigation Measures, and Future Research Direction. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, *2024*, 135–169. https://doi.org/10.58496/mjaih/2024/016

Saare, M. A, Hussain, A., & Seng Yue, W. (2019a). Relationships between the Older Adult's Cognitive Decline and Quality of Life: The Mediating Role of the Assistive Mobile Health Applications. *International Journal of Interactive Mobile Technologies (IJIM)*, *13*(10), 42. https://doi.org/10.3991/ijim.v13i10.11288

Saare, M. A., Hussain, A., & Seng Yue, W. (2019b). 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 (IJIM)*, *13*(04), 130. https://doi.org/10.3991/ijim.v13i04.10525

Salem, O., & Mehaoua, A. (2022). A Secure Framework for Remote Healthcare Monitoring using the Internet of Medical Things. *Proceeding of the IEEE International Conference on Communications*, 1233-1238. https://doi.org/10.1109/icc45855.2022.9839025

Sardar, A., Umer, S., Rout, R. K., & Khan, M. K. (2023). A Secure and Efficient Biometric Template Protection Scheme for Palmprint Recognition System. *IEEE Transactions on Artificial Intelligence*, *4*(5), 1051–1063. https://doi.org/10.1109/tai.2022.3188596

Sardar, A., Umer, S., Rout, R. K., Sahoo, K. S., & Gandomi, A. H. (2024). Enhanced Biometric Template Protection Schemes for Securing Face Recognition in IoT Environment. *IEEE Internet of Things Journal*, *11*(13), 23196–23206. https://doi.org/10.1109/jiot.2024.3374229

Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions. *Mobile Networks and Applications*, *28*(1), 296–312. https://doi.org/10.1007/s11036-022-01937-3

Segun, O. F., Seyi, B. R., & Alagbe, G. K. (2023). Framework on Enhancing Biometric Template Protection Transformation Scheme Using Residue Number System. *Proceeding of the International Conference on Science, Engineering and Business for Sustainable Development Goals (SEB-SDG)*, 1–11. https://doi.org/10.1109/seb-sdg57117.2023.10124538

Sharma, I., & Sharma, S. (2022). Blockchain Enabled Biometric Security in Intemet-of-Medical-Things (IoMT) Devices. *Proceedings of the International Conference on Augmented Intelligence and Sustainable Systems (ICAISS)*, 971–979. https://doi.org/10.1109/icaiss55157.2022.10010716

Sumalatha, U., Prakasha, K. K., Prabhu, S., & Nayak, V. C. (2024). A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection. *IEEE Access*, *12*, 64300–64334. https://doi.org/10.1109/access.2024.3395417

Tolba, Z., & Derdour, M. (2021). Deep learning for cryptanalysis attack on IoMT wireless communications via smart eavesdropping. *Proceedings of the International Conference on Networking and Advanced Systems (ICNAS)*, 1–6. https://doi.org/10.1109/icnas53565.2021.9628924

Vo, V. N., Nguyen, L.-M.-D., Tran, H., Dang, V.-H., Niyato, D., Cuong, D. N., Luong, N. C., & So-In, C. (2023). Outage Probability Minimization in Secure NOMA Cognitive Radio Systems With UAV Relay: A Machine Learning Approach. *IEEE Transactions on Cognitive Communications and Networking*, *9*(2), 435–451. https://doi.org/10.1109/tccn.2022.3226184

Wang, W., Chen, Q., Yin, Z., Srivastava, G., Gadekallu, T. R., Alsolami, F., & Su, C. (2022). Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks. *IEEE Internet of Things Journal*, *9*(11), 8883–8891. https://doi.org/10.1109/jiot.2021.3117762

Wu, S., Zhang, A., Chen, J., Peng, G., & Gao, Y. (2023). A Blockchain-Assisted Lightweight Anonymous Authentication Scheme for Medical Services in Internet of Medical Things. *Wireless Personal Communications*, *131*(2), 855–876. https://doi.org/10.1007/s11277-023-10457-6

Xu, S., Chen, X., Guo, Y., Yiu, S.-M., Gao, S., & Xiao, B. (2025). Efficient and Secure Post-Quantum Certificateless Signcryption With Linkability for IoMT. *IEEE Transactions on Information Forensics and Security*, *20*, 1119–1134. https://doi.org/10.1109/tifs.2024.3520007

Yachongka, V., Yagi, H., & Oohama, Y. (2021). Biometric Identification Systems with Noisy Enrollment for Gaussian Sources and Channels. *Entropy*, *23*(8), 1049. https://doi.org/10.3390/e23081049

Zeledon-C´ Ordoba, M., Pe´ naranda, C. P., and˜ Coto-Jimenez, M. (2022). An experimental study on footsteps sound recognition as biometric under noisy conditions. *Revista Tecnología En Marcha*, ág-153. https://doi.org/10.18845/tm.v35i8.6467