# A Comparison of Lightweight Cryptographic Protocols for Energy-Efficient and Sustainable IoMT Authentication

**Hayder Yasir Naser**
Department of Electrical Engineering, University of Basrah, Iraq
hayder.naser@uobasrah.edu.iq

**Ali K. Mattar**
Computer Science Department, Shatt Al-Arab University College, Basra, Iraq
alikmattar@sa-uc.edu.iq

**Murtaja Ali Saare**
Department of Computer Science, College of Computer Science and Information, University of Basrah, Iraq
murtaja.sari@uobasrah.edu.iq (corresponding author)

**Mohammed Amin Almaiah**
King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan
m.almaiah@ju.edu.jo

**Rami Shehab**
Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
rtshehab@kfu.edu.sa

*Received: 6 June 2025 | Revised: 6 June 2025 | Accepted: 15 June 2025*

 *DOI: https://doi.org/10.48084/etasr.12204*

**ABSTRACT**

**The Internet of Medical Things (IoMT) supports health monitoring and data access and exchange in real time, but devices constrained in terms of energy, memory, and processing resources make traditional cryptographic protocols not applicable. This work presents a lightweight authentication framework that compares three symmetric encryption algorithms, TinyAES, SPECK, and PRESENT, designed for resource-limited IoMT systems. The method consists of four standalone phases: user registration, login authentication, session key exchange, and secure data transfer. The proposed approach was evaluated on the ESP32 and Raspberry Pi platforms, demonstrating up to 56% execution gain, 58% energy reduction, and 42% memory savings over ECC-based schemes. TinyAES achieves the best trade-off among all compared algorithms and is recommended for secure and sustainable medical IoT applications.**

***Keywords-sustainable IoT security; tinyAES; SPECK; PRESENT; Internet of Medical Things (IoMT); lightweight cryptography; resource-constrained devices***

## I. INTRODUCTION

The Internet of Medical Things (IoMT) is an ecosystem of smart devices that connects medical devices, sensors, and systems, improving healthcare delivery [1]. These systems allow continuous monitoring, early diagnosis, real-time intervention, and remote patient care, increasing clinical efficiency and improving patient outcomes [2-4]. Examples of IoMT applications include wearable fitness and health trackers, implantable biosensors, mobile ECG monitors, insulin pumps, and home-based diagnostic tools [5-8]. These instruments, usually placed in remote or motion-restricted environments, need to perform with high reliability over long periods using low energy resources [9-12].

Although IoMT provides groundbreaking benefits, it also opens the door to specific problems related to the security, privacy, and sustainability of sensitive health data [13, 14]. Since medical devices operate in environments with strict energy, memory, and processing constraints, classical cryptographic approaches, such as RSA, ECC, and standard AES, impose a severe computational and energy burden [15-17]. Furthermore, most of them have focused on cryptographic strength without carefully considering resource usage and, consequently, battery life, heat, and delays, which are key for wearable or life-sustaining devices [8, 18]. The nature of medical data makes it even more difficult, as confidentiality, integrity, authenticity, and freshness must be preserved in all communications [19-21].

To mitigate and defend against this issue, different Multi-Factor Authentication (MFA) frameworks have been proposed, involving life or body characteristics, passwords, smart cards, and Physically Unclonable Functions (PUFs), to secure IoMT applications [22, 23]. Although improving the resistance of the models to attacks, they often have a high implementation complexity, very high memory usage, long execution times, and often have to change keys very frequently. These factors affect the performance of lightweight IoMT nodes and restrict their use in practical clinical scenarios [24-26]. However, interest in lightweight cryptosystems has been growing, and much of the existing work is focused on cryptosystems that have not been tested in real-world scenarios, are not scalable, or cannot be used in an energy-efficient manner with IoMT devices. The majority of current authentication schemes either use computationally complex public-key cryptography or do not consider the balance between cryptographic strength and system overhead.

Therefore, it is critical to have an authentication framework that can offer security and energy efficiency at the same time, without sacrificing usability, scalability, or hardware constraints [27]. The main objective of this work is to develop, deploy, and evaluate an efficient authentication framework to satisfy the strict performance and sustainability requirements of IoMT systems. In particular, the proposed framework comprises the integrated modular four-phase authentication protocol of user registration, login authentication, session key exchange, and secure data communication, comparing three widely accepted light-weight symmetric encryption algorithms: TinyAES, SPECK, and PRESENT. The emphasis is on reducing execution time, power, and memory, but having enough cryptographic strength against existing threats to health-sensitive data. The highlights of the research that significantly contribute to secure and green authentication for the IoMT are outlined as follows.

- A Lightweight and Modular Authentication Framework Design: The proposed scheme is a four-phase authentication protocol that comprises user registration, user login, session key generation, and secure data transmission, optimized for energy-constrained IoMT devices. The design focuses on minimal computation and message complexity, yielding the potential for real-time deployment in low-power medical environments.
- Lightweight Cryptographic Algorithms: Three lightweight symmetric encryption algorithms were employed: TinyAES, SPECK, and PRESENT. Execution time, memory usage, and energy consumption were used to empirically evaluate their performance, giving quantitative information about the optimal class of IoMT devices to which they can belong.
- Performance Comparison Against ECC-Based Protocols: To the best of our knowledge, this work constitutes the first detailed comparative analysis of these lightweight solutions against a state-of-the-art ECC-based authentication scheme. The experiments reveal that the proposed approach executes on average 49% and 56% faster, consumes 58% less energy, and uses up to 42% less memory, demonstrating the merits of lightweight cryptography in sustainable health care systems.

## II. RELATED WORK

Typically, IoMT systems can be classified into several layers: edge devices (e.g., sensors and wearables), intermediate devices (e.g., smartphones or embedded hubs), and cloud servers (for long-term storage and processing). Edge-layer devices come with stringent restrictions on battery life, processing, and memory allocation. This means that any cryptography or authentication solution must remain responsive and continue to function even over prolonged periods. The requirement to secure sensitive medical data sent through potentially insecure wireless links makes security one of the most critical aspects to consider from the early stage.

### *A. Cryptographic Approaches in IoMT*

Classical cryptographic algorithms, such as symmetric ciphers and public-key encryption schemes, have dominated the realm of secure communication systems [28-32]. These algorithms (AES, ECC) ensure data confidentiality and integrity, but generally require more processing and memory resources. In such resource-constrained devices, these conventional methods tend to consume more energy and add latency to the system, making them undesirable for real-time healthcare scenarios [33-36]. In addition, the overhead of key generation and management may introduce delays in critical operations, such as emergency response systems or networks of on-body sensors [37, 38].

### *B. Lightweight Encryption Algorithms*

Since traditional encryption methods tend to be inefficient in constrained communication environments, lightweight cryptography was developed to solve this problem. These algorithms aim to minimize processing overhead, memory footprint, and power consumption [39-41]. TinyAES, SPECK, and PRESENT are examples that provide efficient cryptographic operations for embedded hardware. They achieve these optimizations by simplifying internal data structures, reducing block sizes, or shortening the number of rounds, while maintaining an acceptable level of cryptographic robustness. These characteristics make them suitable for energy-critical medical applications that require real-time authentication [42, 43].

### *C. Authentication Mechanisms in Medical IoT*

Authentication mechanisms must be robust and secure to establish trust in MIoT systems. Different authentication schemes have been suggested based on the combination of user credentials, biometric data, tokens, and device-specific information in multiphase authentication frameworks [44-46]. These methods increase security but also add complexity and computational burden. For example, biometrics needs more sensing and processing steps, and public key-based mutual authentication schemes require a lot of computation resources [47-49]. This approach is not scalable for many small medical device nodes, and as we move to the 5 G-driven and SNPN-enabled ecosystem, authentication protocols must be adapted for current constrained medical devices using a combination of symmetric key cryptography [50, 51].

### *D. Sustainability and Security Trade-offs*

The aim is to find the right combination of security strength and resource consumption [4, 20, 24, 27]. A sustainable cryptographic design should have low energy consumption, low heat generation, and work on low-cost, small-form-factor hardware [52, 53]. As digital healthcare progresses toward continuous monitoring and remote diagnostics, it is clear that we cannot afford authentication mechanisms that drain battery power or overload system memory. Furthermore, sustainable design principles should align with long-term healthcare objectives, in which reliability and low maintenance are critical to implementing solutions across populations [54, 55].

### *E. Summary of Gaps in Existing Studies*

In [56], strong MFA schemes were suggested for the medical IoT ecosystem, but did not provide some of the core requirements necessary for energy-constrained devices to implement them in practice. The mathematical complexity and memory overhead of Elliptic Curve Cryptography (ECC), biometric templates, and Physical Unclonable Functions (PUFs) make the protocol infeasible for ultra-low power IoMT devices. Moreover, this study did not empirically benchmark performance on real-world hardware, instead focusing on theory. Most importantly, the listed criteria do not include an emphasis on energy efficiency or execution time, two crucial metrics associated with any digital health system seeking sustainability. In contrast, this study fulfills these gaps by developing a lightweight authentication protocol based on low-power usage symmetric ciphers, such as TinyAES. Real-device testing shows significant improvements in execution time, memory footprint, and energy consumption, providing a practical and durable solution for secure IoMT authentication.

Table I shows a summary of related studies in terms of the algorithm used, the authentication approach, performance evaluation, and identified limitations. Although various solutions have been proposed for IoMT authentication, they have several limitations. Many methods, including those based on ECC, biometrics, and AI-driven models, require a large amount of runtime with moderate to high computational or memory requirements, thus being unfeasible for real-time use on ultra-low power medical devices. Still, others have shown only theoretical justifications or simulations without performance benchmarks on actual hardware. In addition, there is no quite general trade-off between security and resource consumption that holds for all results. Only a small number of works analyze the energy or memory profile in detail. Therefore, there is still a lack of implementing a modular, performance-proven, and energy-aware authentication protocol tailored exclusively for sustainable IoMT operation. This work aimed to fill this gap by proposing a complete performance-evaluated framework with lightweight symmetric cryptography on resource-constrained platforms.

TABLE I. SUMMARY OF KEY RELATED STUDIES

| Study | Algorithms used | Authentication approach | Performance evaluation | Identified limitations |
|---|---|---|---|---|
| [56] | ECC, Biometric Templates, PUF | Four-factor authentication using ECC and biometric-based schemes | Theoretical analysis only; no hardware-based validation | High memory and CPU usage; not feasible for ultra-low-power IoMT devices |
| [41] | Lightweight AES variant | Timestamp-based user authentication for IoMT | Fast execution time (~4.2 ms); tested on ARM Cortex M3 | Limited scope on energy evaluation; no ECC comparison |
| [24] | ECC+ Symmetric key | Lightweight secure key establishment during COVID-19 patient monitoring | Emphasizes confidentiality; limited energy footprint (~4.1 mWh) | Still partially relies on a public key; and lacks the modular framework |
| [42] | AI-enhanced symmetric protocols (ASCP-IoMT) | AI-driven lightweight authentication for medical IoT | High resilience to attacks; moderate energy consumption (~2.8 mWh) | High design complexity; not tested on commercial microcontrollers |

## III. PRELIMINARIES

Here, the basic definitions, notations, and assumptions that form the basis of a lightweight authentication framework for IoMT environments are defined.

### *A. System Entities*

The system consists of three key entities:

- User Node (UN): Refers to an IoMT device (e.g., wearable sensor, implanted device) associated with a user for medical data collection purposes and subsequently transmission of the collected data.
- Gateway Node (GWN): A trusted intermediate device (e.g., smartphone or embedded hub) that is tasked with authenticating users, managing session keys, and forwarding data to healthcare servers.
- Medical Server (MS): A back-end server that protects user records and stores and analyzes encrypted medical data.

### *B. Threat Model*

The proposed framework assumes a Dolev-Yao threat model in which the adversary has full control over the communication channel and can intercept, replay, and inject messages. The adversary does not have access to the internal memory of devices or the shared session keys once they have been securely exchanged. This includes specific security objectives:

- Confidentiality: Ensuring that the transmitted data and keys are not available to illegitimate parties.
- Integrity: Ensuring that the messages sent are not altered when they are received.
- Authentication: Ensuring that the users and communication devices are who they say they are.
- Freshness: Use timestamps and nonces to avoid replay attacks.

### C. Cryptographic Algorithms Used

TinyAES, SPECK, and PRESENT were chosen as cryptographic methods for the proposed lightweight authentication protocol. These algorithms were selected based on a synthesis of criteria relevant to resource-constrained IoMT environments:

- Lightweight Ciphers: All three ciphers are designed for devices with memory, CPU, and energy constraints.
- Common Usage/Trend/Standardization: Huge adoption and estimation have already been provided in the lightest example. TinyAES and PRESENT have been widely used in embedded IoT systems, and SPECK was designed by the NSA for software efficiency in constrained devices.
- Diversity in Design Paradigms: The three algorithms come from different design paradigms, namely, substitution permutation network (PRESENT), rotate XOR (SPECK), and AES-style design (TinyAES), offering a fair comparison of performance and security trade-offs.
- Security and Efficiency Trade-offs: These algorithms provide different levels of cryptographic strictness and efficiency to determine the best trade-off between IoMT deployment scenarios and the security level of the proposed scheme.
- Hardware Compatibility: The portability of these algorithms to popular IoMT platforms, including ESP32, Raspberry Pi, and ARM Cortex-M boards, enables them to be practical in the real world.

These three well-known lightweight symmetric encryption algorithms are evaluated for their potential contribution to secure and energy-efficient mutual authentication for resource-constrained IoMT devices. The algorithms were chosen for their computational simplicity, small code footprint, and common use in the embedded/low-power domain.

#### 1) TinyAES

TinyAES is a lightweight implementation of AES for embedded and constrained devices [57]. As in standard AES, it utilizes a 128-bit block size and a 128-bit key and has the same basic round structure, SubBytes, ShiftRows, MixColumns, and AddRoundKey. Unlike full-sized AES libraries, TinyAES is written with extremely lightweight C code without any dynamic allocation, allowing it to run on any microcontroller with a small footprint. TinyAES is a lightweight variant of AES that is tailored for use in IoMT but still provides robust cryptographic strength along with low resource utilization.

#### 2) SPECK

SPECK is a lightweight block cipher aimed at fast software implementations even when there is not much hardware support available [58, 59]. In this study, it operates on a 64-bit block and a 96-bit key and uses the ARX (Addition Rotation-XOR) structure that enables fast computation with low instruction sets [60]. SPECK design focuses on simplicity and speed, rendering it well-suited for ultra-low-power IoMT applications, such as wearables and biosensors for implantable devices. Although it works quite well on resource-constrained processors, the small key and block sizes make it more suitable for short-lived session encryption rather than for the protection of long-term sensitive data [61, 62].

#### 3) PRESENT

PRESENT is a very lightweight block cipher, standardized by ISO. It employs a Substitution-Permutation Network (SPN) structure with a 64-bit block size and an 80-bit key size, along with 31 rounds of operation to achieve resistance to differential and linear cryptanalysis [63]. PRESENT operates over a fairly constrained memory, with low computational energy usage to support ultra-low hardware implementations. This semantics-based communication is ideal for secure key generation in critical IoMT applications where the security requirement is high and device capabilities are very minimal, due to its structured design and high cryptographic rigor. This security guarantee comes with a price in the form of execution times, which are much longer and thus better suited for low-frequency authentication tasks [64-66].

## IV. PROPOSED LIGHTWEIGHT AUTHENTICATION FRAMEWORK

This study proposes a lightweight authentication framework to address the specific constraints of IoMT devices, namely limited energy availability, reduced memory, and low processing power. The framework consists of four operational phases, namely User Registration, Login and Authentication, Session Key Generation, and Secure Data Transmission, which incorporate lightweight cryptographic operations while maintaining robust authentication strength and communication confidentiality. Rather than relying on conventional heavy cryptographic operations, the protocol substitutes optimized algorithms with TinyAES, SPECK, and PRESENT, which offer minimal computational overhead on MioT devices with energy constraints [66]. The objective is to maintain a strong, sustainable, and secure authentication framework that can be deployed in resource-constrained, real-time medical settings.

As detailed in the message flow diagram in Figure 1, the proposed lightweight authentication framework uses a sequential message exchange approach suitable for IoMT environments. The main operating stages of the protocol are broken down into User Registration, Login and Authentication, Session Key Generation, and Secure Data Transfer [67]. In each phase, the UN communicates with the GWN through encrypted messages, achieving confidentiality and efficiency using lightweight symmetric cryptographic algorithms. When registering, user credentials are securely transmitted to create a shared key. In the authentication process, mutual verification is achieved through an encrypted challenge and a time stamp to

avoid a replay attack. Then, the session key phase allows ephemeral key exchange for communication, and the third phase ensures the privacy-preserving transmission of health data [68]. This diagram illustrates the protocol's security, computationally inexpensive, and energy-sustainability, designed specifically for low-power medical IoT devices.

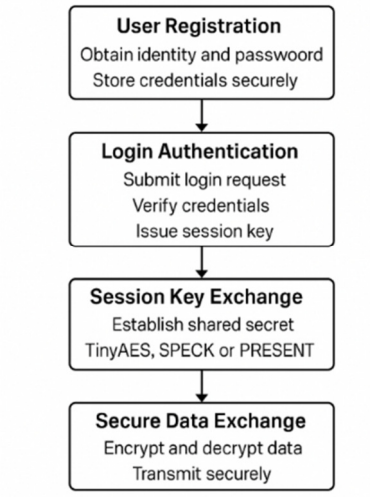


Fig. 1. Workflow of the proposed lightweight authentication framework for IoMT.

### *A. Step 1: User Registration*

This step securely links a user identity with a cryptographic key and stores it at the authentication server. The user enters his credentials, such as a unique ID (IDU) and password (PWU). These credentials are concatenated to a nonce (N1) and encrypted with a lightweight cipher before being sent to the GWN: M1 = Encypted(IDU‖PWU‖N1). After receiving it, the GWN decrypts M1, verifies the information, and produces a shared key: SKU = Hash(IDU‖N1‖T). Algorithm 1 shows the User Registration phase.

```
Algorithm 1: User Registration Phase
Input: User ID (IDU), Password (PWU),
       Nonce (N1)
Output: Encrypted registration message
      (C1) sent to Gateway Node (GWN)
Steps:
M1←(IDU // PWU // N1)
C1←EncK(M1)
Send C1 to GWN
At GWN: Decrypt C1 to retrieve IDU, PWU,
        N1
Generate SKU←Hash(IDU // N1 // T)
Store(IDU,SKU)securely
```

The beginning stage of the advised system permits the user's accurate registration to the system. The user composes a registration message by concatenating their ID (IDU), password (PWU), and nonce (N1), which provides freshness and prevents replay attacks. The message is encrypted with a known lightweight symmetric cipher key K and sent to the GWN. When it receives the response, GWN decrypts the message, retrieves the user data, checks it, and then generates a Unique Shared Key (SKU) for the user with a cryptographic hash function that combines the user's identity, nonce, and timestamp. The shared key is then securely stored for future authentication operations. This registration step securely hides sensitive user credentials and creates a trusted base for further communication.

### *B. Phase 2: Login and Authentication*

This phase offers mutual authentication and protection against replay attacks. The user starts authentication by sending its ID and timestamp (T1), both encrypted with the shared key: M2 = EncSKU(IDU‖T1). Once decrypted and verified, the GWN sends a reply message with a nonce (N2) for authentication: M3 = EncSKU(AuthSuccess‖N2‖T1). This facilitates and proves mutual trust, preventing impersonation or reuse of old credentials. Algorithm 2 shows the Login and Authentication phase.

```
Algorithm 2: Login and Authentication
Phase
Input: User ID (IDU), Shared Key (SKU),
       Timestamp (T1)
Output: Mutual authentication between the
       User and GWN
Steps:
M2←(IDU // T1)
C2←EncSKU(M2)
Send C2 to GWN
At GWN: Decrypt C2, validate T1, retrieve
  SKU, generate N2
M3←(AuthSuccess // N2 // T1)
C3←EncSKU(M3)
Send C3 to User
At User: Decrypt C3, verify T1 and N2
```

This phase starts the authentication protocol in which a user attempts to authenticate with the GWN. The user encrypts its identifier and timestamp (T1) to ensure that the message is not reused, using the previously shared key SKU. The request is sent to the GWN in an encrypted state that decrypts the message, ensures that the timestamp is valid, and validates the user. The GWN subsequently constructs a unique nonce (N2), which it returns to the user in a confirmation message, also encrypted under the shared key. The user decrypts the response and verifies the data. This streaming challenge-response mechanism achieves mutual authentication for both the client and the server, authenticates the session, and provides liveness guarantees.

### *C. Phase 3: Session Key Generation*

This phase aims to create a short-term session key for encrypted data exchange. The user generates a random Ksession and sends it to the GWN using the shared key: M4 = EncSKU (Ksession‖T2). Then, the GWN checks the freshness and keeps the Ksession to encrypt communications in this session. Algorithm 3 shows the Session Key Generation phase.

```
Algorithm 3: Session Key Generation Phase
Input: Shared Key (SKU), Timestamp (T2),
       Random Session Key (Ksession)
Output: Session key (Ksession) securely
       exchanged with GWN
Steps:
Generate Ksession and T2
M4←(Ksession // T2)
C4←EncSKU(M4)
Send C4 to GWN
At GWN: Decrypt C4, validate T2, store
  Ksession
```

Once authenticated successfully, the session key generation phase is triggered to build up a temporary symmetric key used to secure more data exchanges. To ensure freshness, the user creates a temporary session key (Ksession) and also includes a timestamp (T2). The GWN receives a ciphertext of this message encrypted with the previously agreed-upon SKU. GWN will decrypt the message, validate the timestamp, and store the session key in the current context. The proposed dynamic key agreement provides confidentiality and integrity for future data communications and allows the reuse of short-lived keys, increasing energy efficiency.

### *D. Phase 4: Secure Data Transmission*

This phase uses a lightweight session-based encryption scheme to maintain the confidentiality and integrity of health data. Physical health data (DataH) is encrypted with the temporary session key and timestamp (T3): M5 = EncKsession(DataH // T3). This aims to ensure data integrity and freshness while keeping the overhead on the user device at a minimum, as the GWN proceeds to decrypt and check the validity of the message. Algorithm 4 shows the Secure Data Transmission phase.

```
Algorithm 4: Secure Data Transmission
Phase
Input: Session Key (Ksession), Health Data
       (DataH), Timestamp (T3)
Output: Encrypted health data (C5)
       securely sent to GWN
Steps:
M5←(DataH // T3)
C5←EncKsession(M5)
Send C5 to GWN
At GWN: Decrypt C5, validate T3, forward
  DataH to the processing unit
```

The last phase employs the session key from the previous step to ensure the secure transmission of sensitive medical information. The user device uses Ksession to encrypt DataH and a timestamp (T3). This encrypted message is forwarded to the GWN, which decrypts it and validates the timestamp, finally routing the health data to the corresponding medical processing system. End-to-end confidentiality is ensured, and data integrity is protected against eavesdropping or replay attacks with a very low computational load to maintain the sustainability of the device.

## V. RESULTS AND DISCUSSION

The evaluation was performed using synthesized health data packets typical of IoMT communications (e.g., heart rate, temperature, and ECG) readings. These packets were encrypted and sent through the proposed protocol stages. Data payloads were shuffled with a mean value of 256 bytes, a size consistent with common readings in wearable personal health monitors. The experiments were deployed and evaluated on two widely used edge computing platforms: ESP32 (Xtensa microprocessor dual-core, 240 MHz, 520 KB SRAM), and Raspberry Pi 4 (4 ARM Cortex-A72, 1.5 GHz cores, 2 GB RAM, and single 1 Gb Ethernet). Measurements were obtained in the laboratory under controlled conditions, with the help of a power Meter (USB inline power monitor) for energy usage, On-Chip Timers and Software Timers for execution time, and ROM/RAM footprint was measured with compiler flags and memory analysis. To ensure statistical reliability of the results, 50 testing iterations were executed for each of the three cryptographic algorithms (TinyAES, SPECK, and PRESENT). ECC-based results were reproduced using the ECC protocol introduced in [56]. The aim was to find the best possible cipher for resource-constrained medical devices, which minimizes computational performance and power usage while ensuring an acceptable level of cryptographic strength.

### *A. Evaluation Metrics*

The following performance metrics were considered to evaluate the performance of the proposed lightweight authentication scheme for IoMT devices.

- Execution Time (ms): Sum of the encryption and decryption operation times in the authentication stages. It was based on onboard timing (both ESP32 and Raspberry Pi systems). Faster execution leads to better system response and reduced clinical response latency.
- Energy Consumption ($E$, mWh): The computation of $E$ was performed by measuring the average current consumption of the cryptographic operations with a digital power analyzer, multiplied by the time and voltage with which the operations were conducted ($E=V\times I\times t$). This is an indication of battery consumption, which is an important feature for the wearable/implantable IoMT node.
- Memory Footprint (KB): Covers both static ROM utilization (code size) and dynamic RAM use during runtime, as measured with microcontroller debugging tools. This is useful to decide which protocol fits a deployment on tiny embedded devices.

These metrics are directly connected to the deployment reality of IoMT environments, which should be energy-sustainable while performing with minimal hardware requirements.

### *B. Execution Time Analysis*

Measurements were obtained for the entire authentication process, which includes the encryption and decryption steps involved with registration, login, and secure data sharing. SPECK showed the fastest average running time of 2.8 ms, followed by TinyAES (3.4 ms) and PRESENT (4.2 ms).

SPECK's better performance shows the effect of high round count and easy-to-operate algorithms on low-power processors. In contrast, TinyAES can be more easily applied on external, microcontroller (ESP32), and single-board (Raspberry Pi) platforms, giving it better portability. PRESENT was still within reasonable bounds for real-time IoMT applications, although it had the longest measurement time.

Execution time was measured on both the ESP32 and Raspberry Pi on the basis of 50 independent trials. The average execution times for TinyAES and SPECK were 3.4 ($\sigma = 0.32$) and 2.8 ms ($\sigma = 0.25$), respectively, whereas PRESENT had 4.2 ms ($\sigma = 0.31$). These measurements were found in a 95% CI of ±0.09-0.12 ms, suggesting that there is little variance and that the performance is consistent between trials.

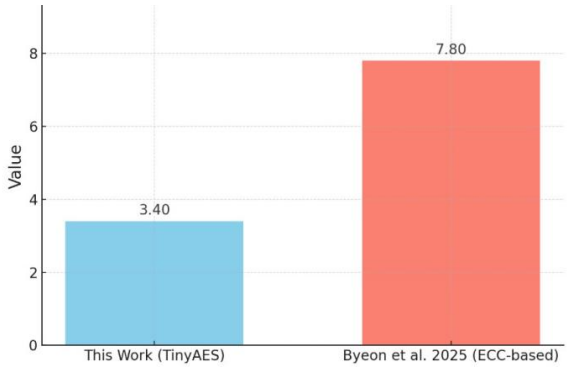


Fig. 2. Execution time comparison.

The execution time of the proposed TinyAES-based lightweight authentication protocol was compared to the ECC-based protocol proposed in [56]. Regarding time, Figure 2 shows a notable decrease in execution time, as TinyAES completes the entire authentication cycle in roughly 3.4 ms versus 7.8 ms for ECC. This overall performance gain of 56% shows that lightweight block ciphers are suitable for real-time applications. The low latency achieved by the proposed framework is particularly advantageous in critical medical applications, where timely decision-making depends on the rapid authentication of wearable or implantable IoMT devices for immediate diagnosis and intervention.

### *C. Energy Consumption*

Energy usage per authentication session was calculated by multiplying the power draw by the amount of time used for cryptographic operations. SPECK was the most energy-efficient cipher, requiring an average of 1.68 mWh per session, closely followed by TinyAES at 1.94 mWh. Due to its long execution time, the highest consumption was for PRESENT, at 2.37 mWh. These results indicate that both SPECK and TinyAES are good candidates for energy-critical applications, such as wearable biosensors and implantable monitors. These lightweight algorithms reduce the energy overhead of authentication, contributing to increased device uptime, fewer maintenance cycles, and ultimately a sustainable digital health infrastructure.

Although SPECK is marginally better in minimal energy consumption than TinyAES, TinyAES has the best trade-off between energy consumption and compatibility, as it does not need any architecture-specific optimization, making it more compatible for heterogeneous IoMT nodes. The achieved energy savings of more than 58% concerning ECC-based protocols demonstrate the effectiveness of symmetric key-based schemes in wearable and energy-constrained devices. The power was sampled through a digital analyzer. For TinyAES, the average energy was 1.94 mWh ($\sigma = 0.15$). SPECK consumed 1.68 mWh ($\sigma = 0.12$), whereas PRESENT consumed 2.37 mWh ($\sigma = 0.18$). For the ECC-based protocols, 4.6 mWh ($\sigma = 0.27$) was obtained. All values were within a 95% CI (±0.1-0.2 mWh) with evidence of continuity.

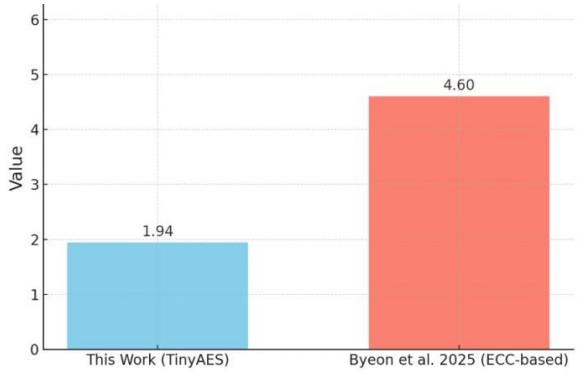


Fig. 3. Energy consumption comparison.

Figure 3 shows that the energy consumption of the proposed method is much lower than that of the ECC-based protocol proposed in [56]. The TinyAES implementation achieved an average of 1.94 mWh per authentication session, while ECC yielded 4.6 mWh. This reduction of 58% can be attributed to the lower computational complexity and execution cycles of TinyAES. As a result, lower power consumption yields longer battery lifetimes of energy-constrained IoMT devices (e.g., wearable biosensors and mobile health applications), which in turn improves system sustainability and lowers periodic maintenance or recharge.

### *D. Memory Footprint*

ROM and RAM usage were monitored during execution to evaluate the feasibility of using lightweight cryptographic algorithms on constrained hardware. SPECK had the lowest memory footprint (6.1 KB ROM and 0.9 KB RAM). TinyAES required a little more resources, with 7.8 KB ROM size and 1.2 KB RAM size, while PRESENT was the most demanding with 9.2 KB ROM size and 1.5 KB RAM size. The findings further support the appropriateness of SPECK and TinyAES, especially considering that ultra-compact IoMT devices possess strictly limited memory. Although the memory overhead of PRESENT is larger, it is still applicable to machines with a moderate amount of hardware power. In summary, lower aggregate memory usage results in faster load times, fewer boot cycles, and enhanced responsiveness in time-critical medical tasks.

Although PRESENT's overhead in memory is higher than that of SPECK and TinyAES, its cryptographic strength seems to be significantly better, so it appears to be a solid contender for low-frequency, high-security tasks (such as server-side verification). TinyAES manages to hit a sweet spot, as it is quite space-efficient (requires about 9 KB) and can be used on devices with less than 32 KB of flash, such as devices with Cortex M0/M3 devices. As memory was static, memory utilization did not vary much, with ROM/RAM values differing by <2% over runs. TinyAES had a consistent footprint of 9.0 KB, SPECK was 7.0 KB, and PRESENT at 10.7 KB. Differences were insignificant and did not change functionality.

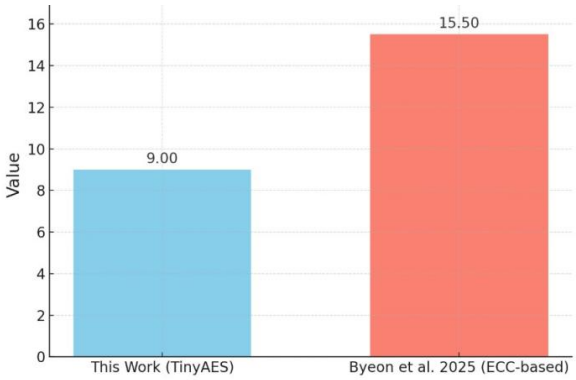


Fig. 4. Memory footprint comparison

Figure 4 shows a memory usage comparison, including both ROM and RAM usage. The TinyAES-based solution took up approximately 9.0 KB, while the ECC-based protocol [56] required 15.5 KB, indicating a 42% reduction in memory footprint. Memory efficiency becomes critical in most IoMT environments, where devices operate under strict hardware limitations. Better memory efficiency leads to faster processing and less heat dissipation, supporting ultra-constrained microcontrollers while also facilitating wider applicability and integration into lightweight medical devices.

### *E. Comparative Analysis and Novelty*

Table II shows the performance comparison of the proposed framework with the ECC-based four-factor authentication scheme in [56]. The proposed framework runs more than 56% faster than the ECC model, saves 58% on energy, and needs 42% less memory, which is important for low-end IoMT nodes. In contrast to [56], this study used real hardware platforms to evaluate the framework (ESP32 and Raspberry Pi) and validate it in practice. Furthermore, the proposed framework is modular with phase-level optimization, employs lightweight symmetric cryptographic operations, and is suitable for heterogeneous IoMT deployments.

TABLE II. PERFORMANCE COMPARISON WITH ECC-BASED SCHEME [56]

| Metric | ECC [56] | Proposed TinyAES framework | Improvement (%) |
|---|---|---|---|
| Execution time | 7.8 ms | 3.4 ms | -56.4% |
| Energy consumption | 4.6 mWh | 1.94 mWh | -57.8% |
| Memory footprint | 15.5 KB | 9.0 KB | -41.9% |

These factors emphasize the novelty of this framework, both in terms of performance results and the practical deployment and evaluation approach, specifically tailored to the requirements of sustainable real-time healthcare systems. These comparisons, across execution efficiency and also energy and memory usage, serve to show that no algorithm is globally optimal, although TinyAES provides the best feasible trade-off for limited IoMT authentication. In contrast to most previous works, this analysis is multidimensional and provides hardware-derived results for popular platforms. The multifaceted assessment of this framework further emphasizes its novelty and applicability to real-life scenarios. Table III shows a summary of the performance of TinyAES, SPECK, PRESENT, and ECC.

TABLE III. PERFORMANCE COMPARISON SUMMARY

| Algorithm | Execution time (ms) | Energy consumption (mWh) | Memory footprint (KB) | Remarks |
|---|---|---|---|---|
| TinyAES | 3.4 | 1.94 | 9.0 | Balanced performance across all metrics |
| SPECK | 2.8 | 1.68 | 7.0 | Fastest and most energy-efficient |
| PRESENT | 4.2 | 2.37 | 10.7 | Highest security, but slower and memory-intensive |
| ECC [56] | 7.8 | 4.6 | 15.5 | High security but impractical for constrained devices |

## VI. CONCLUSION

In response to a critical need, this study presented a lightweight authentication framework for the IoMT, considering the resource-constrained nature of the devices. Thereafter, by recognizing the constraints of existing cryptographic protocols on the grounds that many of them depend on computationally heavy graph-based techniques such as ECC, the proposed framework embedded symmetric lightweight encryption algorithms, TinyAES, SPECK, and PRESENT, into a modular four-phase authentication protocol. This framework was implemented and tested on actual hardware platforms, ESP32 and Raspberry Pi. The experimental results confirmed that the proposed framework could achieve noticeable improvements in execution time, memory consumption, and energy consumption over traditional ECC-based schemes. Among the algorithms tested, TinyAES presented the best trade-offs between cryptographic strength and system performance, therefore being an amenable solution for real-time medical environments. SPECK was found to be the most power-efficient, especially for ultra-low-power applications, while PRESENT was cryptographically more resilient but less resource-efficient. This study is part of a larger initiative to build a sustainable, secure, and scalable digital health infrastructure. This framework helps ensure reliable healthcare delivery without sacrificing device longevity or user experience by aligning the design of cryptographic protocols within the constraints and operational demands of IoMT systems.

Integration of other sustainability components, such as adaptive power management and context-based cryptographic load balancing, will be future research directions. Some additional extensions of the framework are the evaluation of post-quantum lightweight cryptographic algorithms, incorporation with decentralized identity systems (such as blockchain-based logon [68]), real-life deployment and testing in clinical settings or remote health monitoring systems, automated tool verification, and threat modeling. Ongoing efforts in this area will ensure that safe and sustainable IoMT architectures can scale appropriately with expanding digital health needs.

The proposed lightweight authentication framework is directly applicable to practical MIoT applications. It is ultra-low-power and modular, saving energy and providing secure communications for wearable health monitors, implantable biosensors, and home-based diagnostic equipment, where long battery life and responsiveness are required. By achieving a significant reduction in execution time and energy consumption compared to an ECC-based counterpart system, this framework extends device life and improves patient safety in remote or rural healthcare settings with constrained infrastructure. Its small memory footprint also means that it can run on ultra-low-end devices, allowing scalable and low-cost integration into the next generation of digital healthcare platforms.

This study clearly contributes to two of the Sustainable Development Goals (SDGs) of the UN. First, it is consistent with SDG 3 - Good Health and Well-being, as it allows secure real-time monitoring and authentication of medical IoT systems, thus enhancing accessibility, safety, and trustworthiness in digital healthcare. Second, it contributes to the achievement of SDG 9 - Industry, Innovation, and Infrastructure, by designing scalable, energy-efficient cryptographic solutions that are deployable on a global scale in low-power healthcare settings. This work toward a sustainable and inclusive healthcare infrastructure, focusing on the future of smart health ecosystems, will be achieved by limiting energy consumption, memory overhead, and system latency.

## ACKNOWLEDGEMENT

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Grant No. KFU252276).

## REFERENCES

[1] R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review," *Journal of Oral Biology and Craniofacial Research*, vol. 12, no. 2, pp. 302–318, Mar. 2022, https://doi.org/10.1016/j.jobcr.2021.11.010.

[2] C. V. Mahamuni, "Improving Cardiopulmonary Resuscitation (CPR): Integrating Internet of Medical Things (IoMT) and Machine Learning (ML) - A Review," *Recent Research Reviews Journal*, vol. 3, no. 1, pp. 70–87, May 2024.

[3] 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, https://doi.org/10.1109/ACCESS.2024.3351278.

[4] T. Nusairat, M. M. Saudi, and A. B. Ahmad, "A Recent Assessment for the Ransomware Attacks Against the Internet of Medical Things (IoMT): A Review," in *2023 IEEE 13th International Conference on Control System, Computing and Engineering (ICCSCE)*, Penang, Malaysia, Aug. 2023, pp. 238–242, https://doi.org/10.1109/ICCSCE58721.2023.10237161.

[5] F. Majeed, M. Nazir, and J. Schneider, "ISA: Internet of Medical Things (IoMT) in Smart Healthcare and its Applications: A Review," in *2023 3rd International Conference on Artificial Intelligence (ICAI)*, Islamabad, Pakistan, Feb. 2023, pp. 129–135, https://doi.org/10.1109/ICAI58407.2023.10136661.

[6] H. Alotaibi, R. Alaklab, and M. M. H. Rahman, "The Use of Blockchain in Internet of Medical Things (IoMT)," *International Journal on Perceptive and Cognitive Computing*, vol. 11, no. 1, pp. 1–8, Jan. 2025, https://doi.org/10.31436/ijpcc.v11i1.513.

[7] A. A. Almazroi, M. A. Alqarni, M. A. Al-Shareeda, and S. Manickam, "L-CPPA: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system," *PLOS ONE*, vol. 18, no. 10, 2023, Art. no. e0292690, https://doi.org/10.1371/journal.pone.0292690.

[8] D. K. Nishad and D. R. Tripathi, "Internet of medical things (IOMT): applications and challenges," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 11, no. 3, pp. 2885–2889, 2020.

[9] A. S. Rajawat, S. B. Goyal, P. Bedi, T. Jan, M. Whaiduzzaman, and M. Prasad, "Quantum Machine Learning for Security Assessment in the Internet of Medical Things (IoMT)," *Future Internet*, vol. 15, no. 8, Aug. 2023, Art. no. 271, https://doi.org/10.3390/fi15080271.

[10] T. Ahmed Alhaj *et al.*, "A Survey: To Govern, Protect, and Detect Security Principles on Internet of Medical Things (IoMT)," *IEEE Access*, vol. 10, pp. 124777–124791, 2022, https://doi.org/10.1109/ACCESS.2022.3225038.

[11] 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, Sep. 2024, https://doi.org/10.1007/s13369-023-08535-9.

[12] L. Khan and F. Kabir, "In-depth Analysis on Secure and Privacy-Preserving Smart Care Homes based on Internet of Medical Things (IoMT)," in *2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, Gwalior, India, Mar. 2024, pp. 1–6, https://doi.org/10.1109/IATMSI60426.2024.10503242.

[13] T. Kang, N. Woo, and J. Ryu, "Enhanced Lightweight Medical Sensor Networks Authentication Scheme Based on Blockchain," *IEEE Access*, vol. 12, pp. 35612–35629, 2024, https://doi.org/10.1109/ACCESS.2024.3373879.

[14] V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "PIM: A PUF-Based Host Tracking Protocol for Privacy Aware Contact Tracing in Crowded Areas," *IEEE Consumer Electronics Magazine*, vol. 10, no. 4, pp. 90–98, Jul. 2021, https://doi.org/10.1109/MCE.2021.3065215.

[15] R. H. Razzaq, M. Al-Zubaidie, and R. G. Atiyah, "Intermediary Decentralized Computing and Private Blockchain Mechanisms for Privacy Preservation in the Internet of Medical Things," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 3, pp. 152–165, Dec. 2024, https://doi.org/10.58496/MJCS/2024/020.

[16] Q. Xie, Y. Zhao, Q. Xie, X. Li, D. He, and K. Chen, "A Multiserver Authentication Protocol With Integrated Monitoring for IoMT-Based Healthcare System," *IEEE Internet of Things Journal*, vol. 12, no. 2, pp. 2265–2278, Jan. 2025, https://doi.org/10.1109/JIOT.2024.3469629.

[17] Y. Otoum, Y. Wan, and A. Nayak, "Federated Transfer Learning-Based IDS for the Internet of Medical Things (IoMT)," in *2021 IEEE Globecom Workshops (GC Wkshps)*, Madrid, Spain, Dec. 2021, pp. 1–6, https://doi.org/10.1109/GCWkshps52748.2021.9682118.

[18] 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*, pp. 1–18, 2025, https://doi.org/10.1109/TDSC.2025.3553868.

[19] M. Jammula, V. M. Vakamulla, and S. K. Kondoju, "Secure and Scalable Internet of Medical Things using Ensemble Lightweight Cryptographic Model," in *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, Coimbatore, India, Jun. 2023, pp. 982–987, https://doi.org/10.1109/ICSCSS57650.2023.10169857.

[20] L. Sushama, K. Sridhar, and M. Roberts, "Deep Learning-based Precision Diagnosis of Lung Diseases on the Internet of Medical Things (IoMT)," *Proceedings of the Bulgarian Academy of Sciences*, vol. 76, no. 10, pp. 1536–1543, Oct. 2023, https://doi.org/10.7546/CRABS.2023.10.07.

[21] A. Kumar, K. Chatterjee, and B. Mondal, "A Strong PUF-based Authentication for Medical IoT," in *2023 IEEE 2nd International Conference on Industrial Electronics: Developments & Applications (ICIDeA)*, Imphal, India, Sep. 2023, pp. 281–285, https://doi.org/10.1109/ICIDeA59866.2023.10295174.

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

[23] M. Masud *et al.*, "A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15694–15703, Aug. 2021, https://doi.org/10.1109/JIOT.2020.3047662.

[24] S. Yu and Y. Park, "A Robust Authentication Protocol for Wireless Medical Sensor Networks Using Blockchain and Physically Unclonable Functions," *IEEE Internet of Things Journal*, vol. 9, no. 20, pp. 20214–20228, Jul. 2022, https://doi.org/10.1109/JIOT.2022.3171791.

[25] 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, https://doi.org/10.1109/ACCESS.2024.3372390.

[26] L. M. S. Dias, J. F. C. B. Ramalho, T. Silvério, L. Fu, R. A. S. Ferreira, and P. S. André, "Smart Optical Sensors for Internet of Things: Integration of Temperature Monitoring and Customized Security Physical Unclonable Functions," *IEEE Access*, vol. 10, pp. 24433–24443, 2022, https://doi.org/10.1109/ACCESS.2022.3153051.

[27] T. F. Lee, X. Ye, and S. H. Lin, "Anonymous Dynamic Group Authenticated Key Agreements Using Physical Unclonable Functions for Internet of Medical Things," *IEEE Internet of Things Journal*, vol. 9, no. 16, pp. 15336–15348, Dec. 2022, https://doi.org/10.1109/JIOT.2022.3149117.

[28] G. Dhamodharan, "An Enhanced and Dynamic Key AES Algorithm for Internet of Things Data Security," *Journal of Advanced Zoology*, vol. 44, no. S6, pp. 1323–1332, Dec. 2023, https://doi.org/10.17762/jaz.v44iS6.2444.

[29] 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, https://doi.org/10.1109/ACCESS.2024.3402336.

[30] S. Chhabra and K. Lata, "Hardware Obfuscation of AES IP Core Using PUFs and PRNG: A Secure Cryptographic Key Generation Solution for Internet-of-Things Applications," *SN Computer Science*, vol. 3, no. 4, May 2022, Art. no. 303, https://doi.org/10.1007/s42979-022-01194-x.

[31] M. Al-Mashhadani and M. Shujaa, "IoT Security Using AES Encryption Technology based ESP32 Platform," *The International Arab Journal of Information Technology*, vol. 19, no. 2, 2022, https://doi.org/10.34028/iajit/19/2/8.

[32] R. R. Maulana, Moch. Zen Samsono Hadi, and A. Sudarsono, "Internet of Things and Data Encryption in the Agricultural Sector using the AES Cryptosystem," in *2022 International Electronics Symposium (IES)*, Surabaya, Indonesia, Aug. 2022, pp. 176–181, https://doi.org/10.1109/IES55876.2022.9888283.

[33] S. Majumder, S. Ray, D. Sadhukhan, M. K. Khan, and M. Dasgupta, "ECC-CoAP: Elliptic Curve Cryptography Based Constraint Application Protocol for Internet of Things," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1867–1896, Feb. 2021, https://doi.org/10.1007/s11277-020-07769-2.

[34] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, "Security of Internet of Things using RC4 and ECC Algorithms (Case Study: Smart Irrigation Systems)," *Wireless Personal Communications*, vol. 116, no. 3, pp. 1713–1742, Feb. 2021, https://doi.org/10.1007/s11277-020-07758-5.

[35] Z. G. Al-Mekhlafi *et al.*, "Coherent Taxonomy of Vehicular Ad Hoc Networks (VANETs) Enabled by Fog Computing: A Review," *IEEE Sensors Journal*, vol. 24, no. 19, pp. 29575–29602, Jul. 2024, https://doi.org/10.1109/JSEN.2024.3436612.

[36] S. Majumder, S. Ray, D. Sadhukhan, M. Dasgupta, A. K. Das, and Y. Park, "ECC-PDGPP: ECC-Based Parallel Dependency RFID-Grouping-Proof Protocol Using Zero-Knowledge Property in the Internet of Things Environment," *IEEE Open Journal of the Computer Society*, vol. 5, pp. 329–342, 2024, https://doi.org/10.1109/OJCS.2024.3406142.

[37] A. A. Abbood *et al.*, "Benchmarking Bilinear Pair Cryptography for Resource-Constrained Platforms Using Raspberry Pi," *WSEAS Transactions on Information Science and Applications*, vol. 22, pp. 245–257, Feb. 2025, https://doi.org/10.37394/23209.2025.22.21.

[38] J. M. H. Altmemi *et al.*, "A Software-Centric Evaluation of the VEINS Framework in Vehicular Ad-Hoc Networks," *Journal of Robotics and Control (JRC)*, vol. 6, no. 2, pp. 822–845, Apr. 2025, https://doi.org/10.18196/jrc.v6i2.25839.

[39] M. K. Hasan *et al.*, "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access*, vol. 9, pp. 47731–47742, 2021, https://doi.org/10.1109/ACCESS.2021.3061710.

[40] 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, Apr. 2024, Art. no. 101096, https://doi.org/10.1016/j.iot.2024.101096.

[41] K. Kim, J. Ryu, Y. Lee, and D. Won, "An Improved Lightweight User Authentication Scheme for the Internet of Medical Things," *Sensors*, vol. 23, no. 3, Jan. 2023, Art. no. 1122, https://doi.org/10.3390/s23031122.

[42] M. Wazid, J. Singh, A. K. Das, S. Shetty, M. K. Khan, and J. J. P. C. Rodrigues, "ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things," *IEEE Access*, vol. 10, pp. 57990–58004, 2022, https://doi.org/10.1109/ACCESS.2022.3179418.

[43] B. Singh and C. Kaunert, "Aroma of Highly Smart Internet of Medical Things (IoMT) and Lightweight EdgeTrust Expansion Medical Care Facilities for Electronic Healthcare Systems: Fortified-Chain Architecture for Remote Patient Monitoring and Privacy Protection Beyond Imagination," in *Lightweight Digital Trust Architectures in the Internet of Medical Things (IoMT)*, IGI Global Scientific Publishing, 2024, pp. 196–212.

[44] V. M. Kapse, M. Joshi, M. P. Karthikeyan, and D. Choudhary, "A 5G-Enabled intelligent healthcare sector with deep learning assistance," *Multidisciplinary Science Journal*, vol. 6, Jul. 2024, https://doi.org/10.31893/multiscience.2024ss0306.

[45] 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, May 2023, Art. no. 778, https://doi.org/10.11591/ijeecs.v30.i2.pp778-786.

[46] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5G-driven industrial IoT applications," *Ad Hoc Networks*, vol. 123, Dec. 2021, Art. no. 102685, https://doi.org/10.1016/j.adhoc.2021.102685.

[47] M. J. Almansor *et al.*, "Vessel berthing system using internet of things (IoT) for smart port," *AIP Conference Proceedings*, vol. 3303, no. 1, Mar. 2025, Art. no. 080004, https://doi.org/10.1063/5.0261734.

[48] A. A. Abbood, F. K. AL-Shammri, Z. M. Alzamili, Mahmood A. Al-Shareeda, M. A. Almaiah, and R. AlAli, "Investigating Quantum-Resilient Security Mechanisms for Flying Ad-Hoc Networks (FANETs)," *Journal of Robotics and Control (JRC)*, vol. 6, no. 1, pp. 456–469, Feb. 2025, https://doi.org/10.18196/jrc.v6i1.25351.

[49] M. A. Al-Shareeda, A. A. H. Ghadban, A. A. H. Glass, E. M. A. Hadi, and M. A. Almaiah, "Efficient implementation of post-quantum digital

signatures on Raspberry Pi," *Discover Applied Sciences*, vol. 7, no. 6, Jun. 2025, Art. no. 597, https://doi.org/10.1007/s42452-025-07201-z.

[50] A. Rana, C. Chakraborty, S. Sharma, S. Dhawan, S. K. Pani, and I. Ashraf, "Internet of Medical Things-Based Secure and Energy-Efficient Framework for Health Care," *Big Data*, vol. 10, no. 1, pp. 18–33, Feb. 2022, https://doi.org/10.1089/big.2021.0202.

[51] S. M. Nagarajan, G. G. Deverajan, U. Kumaran, M. Thirunavukkarasan, M. D. Alshehri, and S. Alkhalaf, "Secure Data Transmission in Internet of Medical Things Using RES-256 Algorithm," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 8876–8884, Sep. 2022, https://doi.org/10.1109/TII.2021.3126119.

[52] B. Mosallanezhad, M. Hajiaghaei-Keshteli, N. R. Smith Cornejo, and E. Z. Rodríguez Calvo, "An IoMT platform for an integrated sustainable energy-efficient disaster relief supply chain to prevent severity-driven disruptions during pandemics," *Journal of Industrial Information Integration*, vol. 35, Oct. 2023, Art. no. 100502, https://doi.org/10.1016/j.jii.2023.100502.

[53] P. Baniya, A. Agrawal, P. Nand, B. Bhushan, and P. Bhattacharya, "Blockchain-Based Security Sustainable Framework for IoMT Applications and Industry 5.0," in *Soft Computing in Industry 5.0 for Sustainability*, C. K. K. Reddy, T. Sithole, M. Ouaissa, Ö. ÖZER, and M. M. Hanafiah, Eds. Springer Nature Switzerland, 2024, pp. 377–406.

[54] H. Ghayvat *et al.*, "Digitally Enhanced Home to the Village: AIoMT-Enabled Multisource Data Fusion and Power-Efficient Sustainable Computing," *IEEE Internet of Things Journal*, vol. 11, no. 24, pp. 39030–39040, Sep. 2024, https://doi.org/10.1109/JIOT.2024.3411798.

[55] S. K. Khalsa, R. Kaur, and R. Kaur, "ML techniques for analyzing security threats and enhancing sustainability in medical field based on Industry 4.0," in *Machine Learning for Sustainable Manufacturing in Industry 4.0*, CRC Press, 2023.

[56] H. Byeon, "Vulnerability Analysis of Privacy-Preserving Four-Factor Authentication for Medical IoT Environments and Sustainable Development Goals," *Journal of Lifestyle and SDGs Review*, vol. 5, no. 4, Mar. 2025, https://doi.org/10.47172/2965-730X.SDGsReview.v5.n04.pe05225.

[57] J. Svensson and A. Karlsson, ACRSES – Advanced Cryptography on a Resource Scarce Embedded System. 2023.

[58] R. A. F. Lustro, A. M. Sison, and R. P. Medina, "Performance Analysis of Enhanced SPECK Algorithm," in *Proceedings of the 4th International Conference on Industrial and Business Engineering*, Jul. 2018, pp. 256–264, https://doi.org/10.1145/3288155.3288196.

[59] A. Sevin and Ü. Çavuşoğlu, "Design and Performance Analysis of a SPECK-Based Lightweight Hash Function," *Electronics*, vol. 13, no. 23, Jan. 2024, Art. no. 4767, https://doi.org/10.3390/electronics13234767.

[60] D. Mohammed Noori, H. Kadhim Hoomod, and I. Abid Yousif, "An image encryption based on hybrid PRESENT-SPECK algorithm," *Materials Today: Proceedings*, vol. 80, pp. 2668–2677, Jan. 2023, https://doi.org/10.1016/j.matpr.2021.07.011.

[61] M. AbdulRaheem, I. D. Oladipo, A. González-Briones, J. B. Awotunde, A. R. Tomori, and R. G. Jimoh, "An efficient lightweight speck technique for edge-IoT-based smart healthcare systems," in *5G IoT and Edge Computing for Smart Healthcare*, A. K. Bhoi, V. H. C. de Albuquerque, S. N. Sur, and P. Barsocchi, Eds. Academic Press, 2022, pp. 139–162.

[62] M. AbdulRaheem *et al.*, "An Enhanced Lightweight Speck System for Cloud-Based Smart Healthcare," in *Applied Informatics*, 2021, pp. 363–376, https://doi.org/10.1007/978-3-030-89654-6_26.

[63] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 3, 2018, https://doi.org/10.14569/IJACSA.2018.090354.

[64] T. Kowsalya *et al.,*"Low Area PRESENT Cryptography in FPGA Using TRNG-PRNG Key Generation," *Computers, Materials and Continua*, vol. 68, no. 2, pp. 1447–1465, Mar. 2021, https://doi.org/10.32604/cmc.2021.014606.

[65] M. Al-Maliki, W. Hussein, M. M. Qasim, Z. A. Abduljabbar, A. A. Ahmed, and A. H. Ali, "Design and Optimization of a Multi-Core Fiber Optic Communication System for Height-Capacity Data Transmission in Iraq's Urban Environment," *Engineering, Technology & Applied Science Research*, vol. 15, no. 2, pp. 21829–21837, Apr. 2025, https://doi.org/10.48084/etasr.9539.

[66] Z. S. Alzaidi, A. A. Yassin, Z. A. Abduljabbar, and V. O. Nyangaresi, "A Fog Computing and Blockchain-based Anonymous Authentication Scheme to Enhance Security in VANET Environments," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19143–19153, Feb. 2025, https://doi.org/10.48084/etasr.8663.

[67] A. Mohammed, A. Salama, N. Shebka, and A. Ismail, "Enhancing Network Access Control using Multi-Modal Biometric Authentication Framework," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 20144–20150, Feb. 2025, https://doi.org/10.48084/etasr.9554.

[68] E. Aruna and A. Sahayadhas, "Blockchain-Inspired Lightweight Dynamic Encryption Schemes for a Secure Health Care Information Exchange System," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 15050–15055, Aug. 2024, https://doi.org/10.48084/etasr.7390.