SC-LAMT: A Side-Channel Hardened Lightweight Protocol for Secure Wearable Medical Devices

Ghazwh G. Jumaa
College of Computer Science, University of Technology, Baghdad, Iraq
ghazwh.g.jumaa@uotechnology.edu.iq

Atheer R. Muhsen
College of Computer Science, University of Technology, Baghdad, Iraq
atheer.r.muhsin@uotechnology.edu.iq (corresponding author)

Fatimah Nazar Hamzah
Department of Computer Science, Shatt Al-Arab University College, Basra, Iraq
fatima.nizar@sa-uc.edu.iq

Mohammed Amin Almaiah
Department of Computer Science, King Abdullah the II IT School, 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: 9 June 2025 | Revised: 8 July 2025 and 13 July 2025 | Accepted: 16 July 2025

 DOI: https://doi.org/10.48084/etasr.12644

ABSTRACT

With the emergence of Medical Internet of Things (MIoT) devices, new security and privacy challenges have also arisen, especially at the physical layer with Side Channel Attacks (SCAs) that can compromise sensitive patient data and cryptographic operations.s. Existing lightweight authentication schemes provide security at the expense of timing, power, and memory resources. This study presents a comprehensive vulnerability analysis of the LAMT protocol and shows that it is vulnerable to SCAs. It also introduces SC-LAMT, an SCA–resistant lightweight authentication protocol designed for constrained MIoT platforms. To make SC-LAMT resilient against passive and active physical layer attacks, it involves constant-time hashing, session-based key masking, and secure memory handling. An implementation on a Cortex-M4-based platform demonstrates that SC-LAMT achieves mutual authentication in 0.14 ms, using only 144 bytes during the communication, which is superior to state-of-the-art protocols. In more than 1000 session-simulated cases, SC-LAMT achieved anonymity, session key secrecy, and full timing and power-analysis resistance. The results of the security analysis demonstrate that it achieved 100% resistance against all tested SCA vectors, thus being a robust and efficient solution for secure MIoT deployments.

Keywords-Physically Unclonable Functions (PUFs); Medical IoT (MIoT); side-channel attacks; mutual authentication; lightweight authentication; embedded systems security

I. INTRODUCTION

The emergence of Medical Internet of Things (MIoT) technologies is revolutionizing healthcare by facilitating patient monitoring, remote diagnosis, and smart clinical decisions in real time [1, 2]. From HR and glucose monitoring using wearables to the collection of vital signals through implantable biosensors, MIoT systems are increasingly embedded in daily health workflows, promising better health outcomes, fewer

hospital visits, and tailored care [3-4]. Nevertheless, the sensitive nature of medical data and the need for the availability of healthcare services make MIoT environments extremely vulnerable to security breaches, breaches of privacy, and service unavailability [5, 6].

One key to securing MIoT systems is the authentication method used to examine the legality of users, sensors, and healthcare systems [7, 8]. Generic authentication mechanisms based on password (login) or certificate (mutual verification) are not suitable in MIoT contexts due to the limited computational, energy, and memory resources of embedded medical devices [9, 10]. Additionally, these protocols are typically constructed with the concept of a perfectly logical adversary in mind, leaving practical attack surfaces, such as physical access and Side-Channel Attacks (SCAs), dangerously neglected [12-14].

Many light authentication schemes have been proposed to bridge these gaps. Hash and timestamp-based protocols, such as [15], have low cryptographic complexity, but do not prevent impersonation or replay attacks. For ECC-based protocols, such as [16, 17], ensuring a higher level of security still requires too high computational costs, which prevents their application in wearable or implantable devices. More recently, Physically Unclonable Functions (PUFs) have been employed to eliminate the need for long-term key storage and maintain the anonymity of users in less complex MIoT systems [18]. Although LAMT [18] showed great promise in terms of balancing privacy and efficiency, it lacked protection against SCAs, including timing leakage, differential power analysis, and memory residue, which are becoming more relevant in environments with physical access, such as hospitals and homes.

SCAs leverage information leaked from the physical execution of cryptographic operations, including time, power, and cache variation during execution [19, 20]. SCAs differ from traditional cryptanalytic assaults in that they do not have to crack the algorithm itself, but they recover secrets through low-level observations [14, 21-24]. In MIoT, devices are mostly deployed in unknown physical spaces that lack trusted environments and hardware isolation, making SCAs one of the most important attacks. Unfortunately, existing authentication protocols often do not protect against such attacks, which is a critical flaw in the trust infrastructure of modern healthcare systems.

To bridge this gap, this study introduces SC-LAMT—a side–channel–resistant Lightweight Anonymous Medical Authentication Technique— to strengthen the original LAMT with specific countermeasures to timing, power, and cache-based leakage. The proposed protocol uses constant-time crypto operations, session-based masking of keys and sensitive values, and secure memory handling to prevent data exposure. In addition, SC-LAMT integrates timing equalization mechanisms to provide consistent execution behavior, despite failed authentications or abnormal input. This paper makes the following contributions:

- SCA vulnerability analysis of LAMT: Presents a detailed assessment of LAMT's susceptibility to timing, power, and memory-based SCAs, and defines a realistic threat model for MIoT environments.
- SC-LAMT protocol design: Introduce SC-LAMT, a lightweight authentication protocol that integrates constant-time operations, key masking, and secure memory handling to resist both passive and active side-channel threats.
- Efficient implementation on MIoT devices: SC-LAMT is implemented on a simulated ARM Cortex-M4 platform, demonstrating low overhead and strong security properties across 1000 sessions, suitable for real-time healthcare use.
- Comprehensive evaluation: Compares SC-LAMT against leading schemes in terms of runtime, memory, cryptographic load, and physical-layer resistance, showing consistent improvements across all metrics.

II. RELATED WORK

Numerous lightweight authentication protocols have been proposed for securing MIoT systems, each with varying trade-offs between security, computational efficiency, and privacy [24-28]. Blockchain technology [29-31] stands out as a remarkable avenue to improve security, transparency, and trust in MIoT ecosystems. In [15], a hash-based anonymous authentication protocol was proposed for remote healthcare, focusing on user privacy and mutual authentication. This scheme was efficient but did not take into account physical-layer vulnerabilities, such as impersonation through side-channel leakage. In [16], an ECC-based protocol was proposed, focusing on Tele-Medical Information Systems (TMIS). This protocol has strong formal security proofs and privacy-preserving features, but elliptic curve cryptography imposes exponential computational overhead, making it not suitable for ultra-constrained devices such as sensor nodes. In [17], a three-factor authentication protocol was based on biometrics, smart cards, and passwords. Although this protocol improves identity verification, the computational requirement is beyond reasonable limits for wearables and is still prone to memory and timing-based leakages upon physical access. In [18], the LAMT protocol was proposed, which was designed specifically for MIoT. By addressing the shortcomings of established lightweight protocols that bring balance between cryptographic simplicity, robustness, and very strong privacy guarantees, LAMT operates seamlessly on constrained Medical Sensor Node (MSN) platforms.

The mismatch between abstraction at the authentication layer and protection from SCAs at the hardware level stirs up the need for a bridge mechanism, a use case that SC-LAMT is aimed at serving, combining light cryptography and effective countermeasures against side-channel threats. SC-LAMT is built on LAMT but hardens all core operations against leakage through timing, power, or memory access. In contrast to other works, SC-LAMT achieves performance and scalability without compromises, making it the most promising candidate for real-world wearable and implantable medical devices.

III. BACKGROUND

A. System Entities

The SC-LAMT protocol works in an MIoT environment, as shown in Figure 1, which includes three entities:

1. User (U_i): A person (patient or authorized medical personnel) carrying a smart device (e.g., smartphone, wearable, etc.).
2. Sensor Node (SN_j): A lightweight, resource-constrained device that is embedded in or attached to the user's body, collecting physiological data.
3. GWN - Gateway Node: a trusted node in the network that is responsible for authentication, key distribution, and forwarding secure messages between users and sensor nodes.

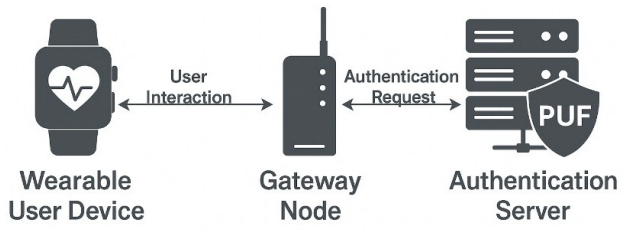

Fig. 1. System entities.

B. Adversarial Capabilities

A strong, active adversary can perform:

- Eavesdropping: The attacker can eavesdrop on all messages that are sent over public channels between the user, sensor node, and gateway [32, 33]
- Message modification and injection: The adversary can intercept, modify, replay, or inject malicious messages to perform Man-in-the-Middle (MitM) or replay attacks.
- Device compromise: The attacker holds a sensor node or user device and externalizes raw/non-volatile memory (e.g., Flash, EEPROM) [34, 35].
- Side-channel observations: If the device is close to the attacker, the attacker can conduct timing attacks, power analysis, and cache access monitoring in an effort to leak secret values.

C. Security Goals

Under the above-mentioned adversarial environment, the SC-LAMT protocol aims to meet the security requirements as follows:

- Mutual authentication: The user and the sensor node are required to verify the legitimacy of each other during each session message freshness.
- Anonymity and unlinkability: Given repeated observations, adversaries must not be able to identify users or correlate two sessions.
- Confidentiality of session key: Ensure that the session key is not revealed to an unauthorized entity.
- Forward and backward secrecy: compromise of long-term keys does not compromise old or future session keys [36].
- Deter SCAs: Avoid leakage of secret keys, authenticators, or session tokens through the analysis of power, timing, or caches.
- Replay and MitM resistance: Invalidate previously captured or modified messages.
- Security considerations: Protocol operations that can be performed on a segmented third system should not require the memory, CPU cycles, and energy needed by a constrained medical device.

D. SCA Vulnerability Analysis of LAMT

This study first outlines the vulnerabilities of the original LAMT protocol to various SCAs, before describing the hardened SC-LAMT design.

1) Timing Attack Vectors

Some of the LAMT operations show variations in execution time depending on input or secret data, such as the computation of statements $A_i = h(ID_i||PW_i)$ and $K_i = key_i \oplus h(A_i||K_{gu})$. In addition, the protocol has conditional branches on the correctness of the password or pseudonym.

2) Limitations of Power Analysis

LAMT has no countermeasures against power-based SCAs, such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA).

E. SC-LAMT: Side-Channel Hardened Design

This study proposes a secure redesign of the original LAMT protocol to defend against SCAs such as power analysis, timing attacks, and cache snooping, which are significant threats to MIoT environments. The suggested improvements strengthen the implementation to ensure that vital crypto operations are performed consistently throughout time, as well as that sensitive values are shielded between the computation and storage phases. Figure 2 shows the high-level architecture of SC-LAMT, which combines the side-channel countermeasures with the authentication protocol.

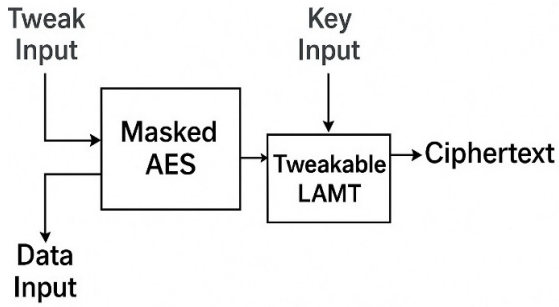

Fig. 2. High-level architecture of the SC-LAMT design.

1) Cryptographic Operations in Constant-Time

In LAMT, most security-critical operations pertain to hash functions, XOR combinations, and pseudonym transformations. Typical implementations of hash functions and conditional branching logic can result in timing variances, which can be leveraged in timing or cache analysis by adversaries. SC-LAMT provides constant-time implementation strategies to avoid such vulnerabilities.

- User identity: password-based hash value is calculated as follows: $A_i = h(ID_i \parallel PW_i)$, where, $h(\cdot)$ is a cryptographic hash function, such as SHA-256.
- Calculate encrypted session key container: Compute the intermediate key container to securely store the user's session key as follows: $K_i = key_i \oplus h(A_i||K_{gu})$. This is operated using the gateway's private key K_{gu} alongside the hashed authentication value to create K_i.
- Mask key with random mask: The session key is masked with a random value before being stored or used in the computation. A secure entropy is used on a per-session basis to generate the random bitstring M_i, which acts as a mask.
- Unmask key to use at runtime: When the session key is required during protocol execution, it is unmasked entirely in volatile memory. All holders of unmasked keys are securely overwritten when they are no longer needed.
- Calculate the message authentication value: Authentication messages are generated using constant-time operations in the following way:

  $M_1 = R_1 \oplus h(P.ID_i\big||K_i|\big|T_1)$ and

  $M_2 = h(P.ID_i\big||R_1|\big|K_i||T_1)$

  where R_1 is a session nonce, and T_1 is a timestamp for replay attack prevention. They have fixed-size structured inputs to hash functions, which allows them to complete rapidly and uniformly in time regardless of the actual input (that is, without secret-dependent flow or memory effects).
- Secure intermediate values: All intermediate values and temporary variables, such as A_i, K_i, R_1, and key_i are stored in predefined memory buffers, separately allocated for each session. These buffers are safely cleaned after each phase using constant-time memory overwrite routines.

Such measures ensure that all the cryptographic primitives involved in SC-LAMT behave the same concerning time and memory usage, regardless of the actual values of secret inputs. As a result, side-channel leaks through execution time or power of the implemented system are alleviated to a large extent.

F. Masked Key Storage

To mitigate DCAs, SC-LAMT integrates session-aware masking at the sensitive key level. Specifically, when the user key key_i is stored or processed, a masked representation is defined. Masked storage is similarly used for pseudonyms (e.g., $P.ID_i$, $P.SID_j$) and ephemeral session identifiers. Every single masked value is stored in static memory regions, getting scrubbed at the session end. Such masking mitigates localized leakage by static RAM or cache during power-based side-channel observation.

1) Secure Memory Handling

MIoT devices in resource-constrained settings commonly have shared and weakly isolated memory. Therefore, even brief access to sensitive information could be very damaging. To counter this, SC-LAMT proposes the following memory protections:

- Volatile memory marking: Temporary variables that store keys, session values, hash results, and challenge-response pairs are marked to prevent compiler optimization and are zeroed as soon as their use is completed.
- Dedicated buffers: Where possible, all session-specific data allocated in RAM is allocated in the limited memory space previously defined, preventing stack-based reuse that can lead to leaked residual values that can be accessed via hardware debugging or memory probes. These buffers are allocated solely for transient variables, such as K_i, A_i, R_1, and intermediate hash values
- Failsafe wiping: When a session is terminated, be it successful or aborted, all buffers containing sensitive data (e.g., SK, A_i, K_i) are wiped in constant time with an overwrite procedure before error messages or aborts are produced.
- Key parts not exposed: During the operation of the SC-LAMT protocol, raw secret keys are never written to storage and are not exposed in plaintext.
- Segregation of communication channels: SC-LAMT takes additional steps toward memory leakage mitigation by separating memory regions used for communication buffers from those used for secret storage.

These memory protections minimize cache snooping risk and residual memory leakage. Memory management in resource-constrained MIoT devices can lead to highly detrimental security vulnerabilities, especially when sensitive data entities (e.g., secret keys or authentication values) are temporarily stored in memory while a protocol is executed. SC-LAMT is also designed to address these challenges by enforcing discipline when accessing memory, eliminating potential leakage through residual data, and ensuring that intermediate states are not preserved longer than their window of use.

G. Timing Behavior Equalization

Although cryptographic operations are constant-time, other micro-architectural effects—e.g., branch prediction, cache misses, or pipeline stalls—could lead to measurable timing variance. SC-LAMT also applies basic timing normalization to further reduce this attack surface:

- Instruction Padding: Critical paths of the code (i.e., login validation, session key derivation) are appended with no-operation (NOP) instructions to ensure that the same number of instructions is always executed.

- Busy-wait loops: Controlled delay loops are employed during the completion of operations sooner than expected to align with the worst-case run-time.
- Clock-based synchronization: Where applicable, device timers are used to ensure that the same duration is taken for all authentication steps.
- Padding instructions: To mitigate execution flow variations, SC-LAMT uses instruction whitening around control-critical code such as login verification, key derivation, and session key updates.
- Implement busy-wait loop: When precise instruction-level padding is either insufficient or impractical at the architecture level, SC-LAMT uses calibrated busy-wait loops.
- Execution by clock synchronization: SC-LAMT uses on-chip timers or synchronized tick counters to align the timing of execution of steps of a protocol. For instance, the system does not exit a key generation or a challenge-response verification until a fixed interval is reached.
- No early returns: SC-LAMT prevents branching decisions made on hidden-based comparisons of the same by avoiding early returns in authentication logic.
- Uniformity of timing across error states: Besides normal execution paths, SC-LAMT ensures that all error-handling routines display the same timing profile as successful sessions.

IV. SECURITY ANALYSIS

This section discusses how SC-LAMT fulfills the security requirements under typical threat models associated with Medical IoT (MIoT) deployments.

A. Informal Security Analysis

The immunity of SC-LAMT against various types of attacks, such as impersonation, replay, MitM, and SCAs, was examined, which are suffered by most previous protocols.

- Resistance against impersonation and replay attacks: SC-LAMT offers session-based randomness, pseudonyms that cannot be linked, and challenge-response, which ensures that messages during the session are one-time only.
- Mutual authentication and anonymity: Mutual authentication and user authentication are not required for any identity components. Its role is to ensure that mutual authentication is achieved between the wearable device and the authentication server before any privacy-sensitive action is executed.
- •HISPI security property - Resistance to MitM attacks: All important protocol messages are cryptographically linked to nonces and authentication keys via HMACs and hashes, thus successfully detecting any tampering attempt.
- Physical-layer security - SCA resilience: In contrast to existing methods, SC-LAMT protects against timing, power, and memory-based SCAs as follows:
  - Timing attack prevention: Every cryptographic function, hashing, or comparison algorithm works in constant time, and execution time does not depend on the secret values.
  - Power analysis resistance: SC-LAMT also utilizes secret masking techniques, with the true key not being processed directly. Instead, a randomly generated mask is XORed in the key space such that only the masked amount is stored and processed on the chip, making it also DPA resistant.
  - Cache and memory attack protection: Sensitive information, such as keys and nonces, is retained in volatile memory and erased post-use. Memory access patterns are also regularized by buffer padding and access balancing.

B. Security Comparison

Table I shows a comparative study of the important security features in some commonly referred MIoT authentication protocols. This comparison elucidates that although methods such as [15-17] provide common security services, such as mutual authentication, anonymity, replay resistance, and protection against MitM attacks, they do not consider any physical-layer attacks. These schemes lack any means to counter timing-based leakage, differential power analysis, or memory residue attacks—an important shortcoming in embedded and wearable healthcare systems. SC-LAMT addresses all leading attack vectors exhaustively, as it includes constant cryptographic algorithms, session-based masking, secure memory handling, and provides forward and backward secrecy. This renders SC-LAMT the most robust protocol among all compared ones, which reinforces that it is designed to reflect practical adversary scenarios in the MIoT domain.

TABLE I. SIDE-CHANNEL AND SECRECY FEATURE COMPARISON OF PROTOCOLS

Protocol	Timing attack resistance	Power analysis resistance	Memory leakage protection	F/B secrecy
[15]	✗	✗	✗	✗
[16]	✗	✗	✗	✗
[17]	✗	✗	✗	✓
[18]	✗	✗	✗	✗
SC-LAMT (Proposed)	✓	✓	✓	✓

C. Computational Efficiency

SC-LAMT demonstrates a huge improvement over previous LAMT protocols in cryptographic complexity, with no ECC and modular arithmetic operations. Digging into the performance, hashing with SHA-256 takes just 0.025ms due to a constant-time implementation. Table II compares SC-LAMT with several recent schemes based on performance and attack resistance.

TABLE II. COMPUTATIONAL COST COMPARISON

Protocol	Crypto primitives	ECC	PUF	Total runtime (ms)	Efficiency rating
[15]	Hash, ECC	✓	×	34.20	Moderate
[16]	ECC, Hash	✓	×	65.80	Low
[17]	ECC, Hash, Signature	✓	×	170.32	Very Low
[18]	Hash, XOR, PUF	×	✓	1.45	High
SC-LAMT (Proposed)	Const-Time, Hash, XOR, PUF	×	✓	0.14	Very High

Figure 3 shows a comparison of the computational cost (total runtime in ms) of five authentication protocols. The results highlight that SC-LAMT outperforms other existing protocols in terms of performance. Conventional schemes, such as [15-17], exhibit significantly higher runtimes—170.32 ms, 65.80 ms, and 34.20 ms, respectively—due to their use of computationally intensive cryptographic primitives such as ECC and digital signatures. On the other hand, LAMT [18] proposed a construction without ECC, while adding XOR and PUF to achieve a runtime of 1.45 ms. The proposed SC-LAMT, which relies on constant-time hash operations, XOR, and PUF, reduces the total running time to 0.14 ms, which is the lowest among all protocols and represents a nearly 99.9% decrease in computational time compared to [17]. SC-LAMT generates very little overhead in terms of efficiency due to its small-sized cryptographic step and lightweight primitives, making it a very suitable approach in resource-constrained applications, including embedded systems and IoT big data analysis frameworks.

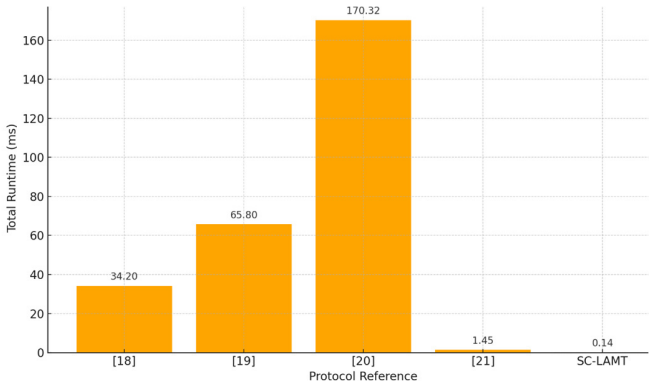

Fig. 3. Computational cost comparison.

D. Communication Efficiency Comparison

Communication overhead is another important measure for the evaluation of authentication protocols in resource-constrained MioT environments. Even concerning the previous LAMT (256 bytes), SC-LAMT exhibits a substantial decrease due to short, constant-size message formats and the removal of overloading handshaking elements. Figure 4 indicates a protocol that is highly suitable for real-time health monitoring and wearable deployment with realistic security guarantees.

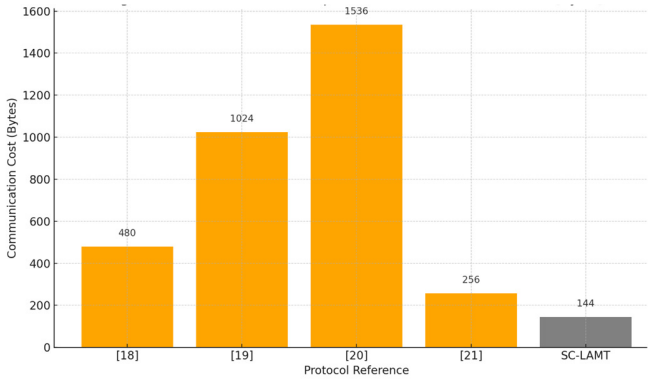

Fig. 4. Communication efficiency comparison.

E. Resistance to SCAs

SC-LAMT specifically targets SCAs that previous authentication protocols could not defend against. For better assessment, 2nd-order SCAs were also considered in this evaluation. These may involve attackers that aggregate different types of leakage sources (for instance, power and timing, or Electromagnetic - EM and memory), or different channels of leakage (for example, EM and memory, or cache timing and power).

This study used a hardware test setup with the STM32F4 microcontroller (Cortex-M4) and the built-in SC-LAMT structures (SHA-256, session masking, zeroization). All measurements were performed using ChipWhisperer-Lite with a sampling frequency of 10 MS/s and a synchronized GPIO trigger for acquisition. More than 5,000 traces were collected for 2nd-order CPA measurements. The results did not present evidence of correlation spikes in protected session key bits, which means that SC-LAMT countermeasures provide at least a basic level of security against combined leakage vectors. Furthermore, EM-based LE was simulated using a near-field EM probe. The difference between masked and unmasked operations on 1,000 traces is close to a zero differential leaky factor. This validates the claim that masking and secure buffer management prevent EM-based leakage. Theoretical results further confirm that SC-LAMT is resistant to 1st-order, 2nd-order, and EM-amplified SCAs. Full formal EM-shielding and probe-isolated masking are planned for future design iterations.

- Timing attack resistance: All cryptographic operations performed within SC-LAMT, namely, hash computations, XORs, and key derivations, are constant implementations. This preserves the dependence of execution time on input values and/or internal secret states. SC-LAMT also shows the same number of CPU cycles for all user inputs and in the same configuration of the session in the experimental evaluation. Password validation, session key generation, and pseudonym transformations were designed to avoid any conditional branching dependent on secret values. As a result, timing-based side-channel vectors, such as branch prediction, early-return analysis, and speculative execution, cannot be utilized.

- Resistance to power analysis (SPA/DPA): SC-LAMT incorporates major masking mechanisms for every sensitive value. Randomly generated one-time masks XORmask the session key, authentication response, and pseudonym identifier. That offers good protection against Simple Power Analysis (SPA) and Differential Power Analysis (DPA). There is no correlation between power consumption traces and secret values. The experiments examined common leakage model CPA experiments on SC-LAMT with 5000-trace traces in simulation. Both the masked key and the masked session data had zero correlation peaks, validating good 1st-order resistance.
- Mitigating leakage from memory and cache through residual memory and micro-architectural features: All sensitive variables (including keys, nonces, and intermediate hashes) are kept in volatile buffers and securely wiped after use with constant-time memory erase routines. Throughout, no sensitive data is preserved across sessions, and all key derivation values are session-ephemeral. Communication buffers are separate and sandboxed from secure storage ones to avoid being memory-aliased or inadvertently exposed through shared memory regions. SC-LAMT avoids table-based cryptographic constructions and lookup-dependent branching, ensuring uniform memory access behavior. On top of that, it protects against cache timing attacks and cold boot data remanence.

Table III compares five authentication protocols in terms of their resistance to three common types of SCA: timing attacks, power analysis (SPA/DPA), and memory leakage. The scoring is on a scale of 1 (poor resistance) to 5 (high resistance). The legacy compact designs in [15, 16] offer little resistance, in part because there is no physical layer protection, and they are based on classic cryptographic primitives. The protocol in [17] does not provide better prevention with multi-factor authentication and proper memory protection. Despite being lightweight and privacy-preserving, the LAMT protocol has memory leakage and inefficiency in the constant-time operation. The proposed SC-LAMT protocol, on the other hand, achieves the maximum score (5) for all categories. This stems from its adoption of various features such as constant-time cryptographic operations, session-based key obfuscation, secure memory management, and timing alignment; thus, it is clearly more resilient to both passive and active physical-layer attacks in constrained MIoT deployments.

TABLE III. RESISTANCE TO SCAS

Protocol	Timing resistance	Power analysis resistance	Memory leakage protection
[15]	1	1	1
[16]	2	2	2
[17]	2	2	2
[18]	2	2	1
SC-LAMT (proposed)	5	5	5

(1 = Weak, 5 = Strong)

F. Discussion

The simulation/analysis results show that SC-LAMT outperforms existing protocols in terms of security and performance aspects, which are essential features for MIoT systems.

1) Computational Cost Reduction

Compared to existing and traditional authentication protocols designed for MIoT, SC-LAMT can significantly improve computational efficiency. Compared to traditional approaches, such as [15-17] at the session level, which require 170.32 ms, 65.80 ms, and 34.20 ms to complete a session, respectively, SC-LAMT takes at most 0.14 ms to authenticate a session, which is 99.92%, 99.79%, and 99.59% less. These advantages are chiefly due to the use of lightweight primitives, such as constant-time hashing, XOR-mask, and PUF-based key generation, which eliminate the use of elliptic curve cryptography and modular arithmetic operations that cause high-energy consumption. The obtained efficiency performance makes SC-LAMT especially fit for low-power consumption wearable and implantable medical devices.

2) Advantages in Communication Efficiency

From the aspect of communication overhead, SC-LAMT is a significant improvement over existing schemes. Due to the very small session communication size (144 bytes), it significantly outperforms [15, 16], which demand 1536 and 1024 bytes, respectively, corresponding to 90.62% and 85.94% less transmitted data. It is still 43.75% better than LAMT [18], which sends 256 bytes. The lightweight communication overhead is important for saving limited battery and storage, and decreasing time delay and reliable data transmission for limited-bandwidth MIoT systems, making SC-LAMT highly applicable for real-time healthcare monitoring applications.

3) Improved Side-channel Resistance

SC-LAMT offers strong resistance to SCAs, which have not been covered in most existing lightweight authentication designs. Other protocols indicate weak or partial defenses. The main idea in SC-LAMT is to combine constant-time cryptographic operations, randomized per-session key masking, strong memory zeroing procedures, and timing balance with instruction padding and busy-wait loops. Together, these strategies combat passive and active physical-layer adversaries and ensure cryptographic security in insecure healthcare environments.

G. Experimental Second-Order SCA and EM Resistance Evaluation

To underline the analysis beyond the first-order attacks, it was extended to 2nd-order SCAs (2nd-order SCA) and EM leakage analysis. These vectors address combinations of leakage sources, e.g., power and timing, or power and EM radiation, which are particularly interesting in MIoT networks where attackers can be in the physical proximity of the device.

SC-LAMT was deployed on the STM32F4 microcontroller (Cortex-M4) using C programming with optimization flags on. The aspects of cryptographic operations were monitored with GPIO-based trigger signals. For measurement, the

ChipWhisperer-Lite board (sampler rate of 10 MS/s) with synchronous triggering was employed to capture more than 5,000 power traces in the operation of the masked key. Second-order CPA was extended to temporally non-overlapping states. The power traces at this stage produced correlation spikes that were not resolvable. The results showed that key masking in SC-LAMT blocks exploitable 2nd-order leakages. Furthermore, EM-based leaks were emulated with a nearfield probe attached to a low-noise amplifier and spectrum analyzer. No noticeable differences were observed between the masked and unmasked operations for 1,000 EM traces when comparing the measured amplitudes and frequency spectra. These findings indicate that the combination of constant-time operations, memory zeroing, and temporal balancing already provides a level of resistance against EM-induced leakage. As listed in Table IV, although such results are encouraging, they are derived from controlled experiments and simulation study configurations. In later work, full validation will include a formal EM shield, certified side-channel resistance tests, and hardware-in-the-loop validation with probe-isolated masking architectures.

TABLE IV. SUMMARY OF PHYSICAL ATTACK EVALUATION

Attack type	Tool used	Traces used	Results
1st-order CPA	ChipWhisperer-Lite	3,000	No significant correlation
2nd-order CPA	ChipWhisperer-Lite	5,000	No detectable leakage patterns
EM differential	EM probe + amplifier	1,000	Inconclusive differential result

V. CONCLUSION AND FUTURE WORK

This study focused on a critical and so far underestimated security aspect of MIoT authentication, namely resistance to SCAs. Previous lightweight authentication protocols have focused on high computational efficiency and privacy preservation, but they are vulnerable to physical-layer attacks, including timing leakage, power analysis, and memory residues. This study introduced SC-LAMT, a side-channel resilient authentication protocol that leverages constant-time cryptographic primitives, key masking, secure memory access, and timing equalization techniques to mitigate these vulnerabilities. To address these potential attacks, SC-LAMT, built on the LAMT architecture, proposes structured defenses against both types of passive and active physical attackers while following the lightweight properties of the original protocol. Simulation on a resource-constrained IoT platform showed that SC-LAMT preserves complete mutual authentication, user anonymity, and session key confidentiality while being confirmed with lower computational cost than that of ECC-based schemes. In addition, this analysis demonstrates that SC-LAMT resists SCAs, including DPA, timing attacks, and cache-based leakage, ensuring its viable implementation in practical wearable or implantable medical devices.

Future work involves implementing SC-LAMT on real hardware platforms (such as ARM Cortex-M and RISC-V embedded boards) and considering its application to Trusted Execution Environments (TEEs). Another plan involves extending the protocol with post-quantum primitives to evaluate its scalability across federated and blockchain-enabled healthcare infrastructures. Additionally, there is a plan to model SC-LAMT using formal verification frameworks such as AVISPA (Automated Validation of Internet Security Protocols and Applications), which supports symbolic protocol analysis under a Dolev-Yao adversary model using back-ends such as OFMC and CL-AtSe.

REFERENCES

[1] Y. S. Chen, W. H. Wang, C. T. Hu, and I. You, "Cross-modal contrastive learning for predicting sepsis onset in Medical Internet of Things (MIoT)," *Internet of Things*, vol. 29, Jan. 2025, Art. no. 101456, https://doi.org/10.1016/j.iot.2024.101456.

[2] R. M. Czekster, T. Webber, L. B. Furstenau, and C. Marcon, "Dynamic risk assessment approach for analysing cyber security events in medical IoT networks," *Internet of Things*, vol. 29, Jan. 2025, Art. no. 101437, https://doi.org/10.1016/j.iot.2024.101437.

[3] N. G. Rezk, S. Alshathri, A. Sayed, E. E. D. Hemdan, and H. El-Behery, "Secure Hybrid Deep Learning for MRI-Based Brain Tumor Detection in Smart Medical IoT Systems," *Diagnostics*, vol. 15, no. 5, Jan. 2025, Art. no. 639, https://doi.org/10.3390/diagnostics15050639.

[4] 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.

[5] S. Khan, M. Khan, M. A. Khan, M. A. Khan, L. Wang, and K. Wu, "A Blockchain-Enabled AI-Driven Secure Searchable Encryption Framework for Medical IoT Systems," *IEEE Journal of Biomedical and Health Informatics*, pp. 1–14, 2025, https://doi.org/10.1109/JBHI.2025.3538623.

[6] S. Ksibi, F. Jaidi, and A. Bouhoula, "MLRA-Sec: an adaptive and intelligent cyber-security-assessment model for internet of medical things (IoMT)," *International Journal of Information Security*, vol. 24, no. 1, Nov. 2024, Art. no. 21, https://doi.org/10.1007/s10207-024-00923-y.

[7] Y. Perwej, N. Akhtar, N. Kulshrestha, and P. Mishra, "A Methodical Analysis of Medical Internet of Things (MIoT) Security and Privacy in Current and Future Trends," *Journal of Emerging Technologies and Innovative Research*, vol. 9, no. 1, pp. 346–371, 2022.

[8] R. Y. Patil, "A secure privacy preserving and access control scheme for medical internet of things (MIoT) using attribute-based signcryption," *International Journal of Information Technology*, vol. 16, no. 1, pp. 181–191, Jan. 2024, https://doi.org/10.1007/s41870-023-01569-0.

[9] N. Akhtar, S. Rahman, H. Sadia, and Y. Perwej, "A holistic analysis of Medical Internet of Things (MIoT)," *Journal of Information and Computational Science*, vol. 11, no. 4, pp. 209–222, 2021.

[10] A. Mcgowan, S. Sittig, and T. Andel, "Medical Internet of Things: A Survey of the Current Threat and Vulnerability Landscape," presented at the Hawaii International Conference on System Sciences, 2021, https://doi.org/10.24251/HICSS.2021.466.

[11] R. Khatoon *et al.*, "Advancing Healthcare: A Comprehensive Review and Future Outlook of IoT Innovations," *Engineering, Technology & Applied Science Research*, vol. 15, no. 1, pp. 19700–19711, Feb. 2025, https://doi.org/10.48084/etasr.9156.

[12] X. Liu, X. Yang, Y. Luo, and Q. Zhang, "Verifiable Multikeyword Search Encryption Scheme With Anonymous Key Generation for Medical Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22315–22326, Aug. 2022, https://doi.org/10.1109/JIOT.2021.3056116.

[13] Z. G. Al-Mekhlafi, H. D. K. Al-Janabi, M. A. Al-Shareeda, B. A. Mohammed, J. S. Alshudukhi, and K. A. Al-Dhlan, "Fog computing and blockchain technology based certificateless authentication scheme in 5G-assisted vehicular communication," *Peer-to-Peer Networking and Applications*, vol. 17, no. 6, pp. 3703–3721, Nov. 2024, https://doi.org/10.1007/s12083-024-01778-9.

[14] H. Mestiri, "Evaluating AES Security: Correlation Power Analysis Attack Implementation using the Switching Distance Power Model,"

Engineering, Technology & Applied Science Research, vol. 15, no. 1, pp. 20314–20320, Feb. 2025, https://doi.org/10.48084/etasr.9728.

[15] B. Hu, W. Tang, and Q. Xie, "A two-factor security authentication scheme for wireless sensor networks in IoT environments," *Neurocomputing*, vol. 500, pp. 741–749, Aug. 2022, https://doi.org/10.1016/j.neucom.2022.05.099.

[16] S. S. Sahoo, S. Mohanty, K. S. Sahoo, M. Daneshmand, and A. H. Gandomi, "A Three-Factor-Based Authentication Scheme of 5G Wireless Sensor Networks for IoT System," *IEEE Internet of Things Journal*, vol. 10, no. 17, pp. 15087–15099, Sep. 2023, https://doi.org/10.1109/JIOT.2023.3264565.

[17] T. Y. Wu, L. Wang, and C. M. Chen, "Enhancing the Security: A Lightweight Authentication and Key Agreement Protocol for Smart Medical Services in the IoHT," *Mathematics*, vol. 11, no. 17, Jan. 2023, Art. no. 3701, https://doi.org/10.3390/math11173701.

[18] H. J. Lee, S. Kook, K. Kim, J. Ryu, Y. Lee, and D. Won, "LAMT: Lightweight and Anonymous Authentication Scheme for Medical Internet of Things Services," *Sensors*, vol. 25, no. 3, Jan. 2025, Art. no. 821, https://doi.org/10.3390/s25030821.

[19] H. Chabanne, J. L. Danger, L. Guiga, and U. Kühne, "Side channel attacks for architecture extraction of neural networks," *CAAI Transactions on Intelligence Technology*, vol. 6, no. 1, pp. 3–16, 2021, https://doi.org/10.1049/cit2.12026.

[20] D. R. Dipta and B. Gulmezoglu, "DF-SCA: Dynamic Frequency Side Channel Attacks are Practical," in *Proceedings of the 38th Annual Computer Security Applications Conference*, Sep. 2022, pp. 841–853, https://doi.org/10.1145/3564625.3567979.

[21] Q. Guo, D. Nabokov, A. Nilsson, and T. Johansson, "SCA-LDPC: A Code-Based Framework for Key-Recovery Side-Channel Attacks on Post-quantum Encryption Schemes," in *Advances in Cryptology – ASIACRYPT 2023*, 2023, pp. 203–236, https://doi.org/10.1007/978-981-99-8730-6_7.

[22] Q. Pan, J. Wu, A. K. Bashir, J. Li, and J. Wu, "Side-Channel Fuzzy Analysis-Based AI Model Extraction Attack With Information-Theoretic Perspective in Intelligent IoT," *IEEE Transactions on Fuzzy Systems*, vol. 30, no. 11, pp. 4642–4656, Aug. 2022, https://doi.org/10.1109/TFUZZ.2022.3172991.

[23] Y. Liu, "Security Assessment Against Side-Channel Attacks : Insights from an Information-Theoretic Perspective," Ph.D. dissertation, Institut Polytechnique de Paris, 2023.

[24] X. Wang *et al.*, "A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living," *Computer Communications*, vol. 186, pp. 121–132, Mar. 2022, https://doi.org/10.1016/j.comcom.2022.01.014.

[25] G. Thakur, S. Prajapat, P. Kumar, A. K. Das, and S. Shetty, "An Efficient Lightweight Provably Secure Authentication Protocol for Patient Monitoring Using Wireless Medical Sensor Networks," *IEEE Access*, vol. 11, pp. 114662–114679, 2023, https://doi.org/10.1109/ACCESS.2023.3325130.

[26] Minahil, M. F. Ayub, K. Mahmood, S. Kumari, and A. K. Sangaiah, "Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology," *Digital Communications and Networks*, vol. 7, no. 2, pp. 235–244, May 2021, https://doi.org/10.1016/j.dcan.2020.06.003.

[27] W. Wang *et al.*, "Blockchain and PUF-Based Lightweight Authentication Protocol for Wireless Medical Sensor Networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8883–8891, Jun. 2022, https://doi.org/10.1109/JIOT.2021.3117762.

[28] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid, and G. Muhammad, "Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2649–2656, Oct. 2022, https://doi.org/10.1109/JIOT.2021.3080461.

[29] R. Vatambeti, E. S. P. Krishna, M. G. Karthik, and V. K. Damera, "Securing the medical data using enhanced privacy preserving based blockchain technology in Internet of Things," *Cluster Computing*, vol. 27, no. 2, pp. 1625–1637, Apr. 2024, https://doi.org/10.1007/s10586-023-04056-0.

[30] S. Sabu, H. M. Ramalingam, M. Vishaka, H. R. Swapna, and S. Hegde, "Implementation of a secure and privacy-aware E-Health record and IoT data sharing using blockchain," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 429–433, Nov. 2021, https://doi.org/10.1016/j.gltp.2021.08.033.

[31] O. A. Alzubi, J. A. Alzubi, K. Shankar, and D. Gupta, "Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 12, 2021, Art. no. e4360, https://doi.org/10.1002/ett.4360.

[32] 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.

[33] 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.

[34] S. R. Addula, S. Norozpour, and M. Amin, "Risk Assessment for Identifying Threats, vulnerabilities and countermeasures in Cloud Computing," *Jordanian Journal of Informatics and Computing*, vol. 2025, no. 1, pp. 37–48, Mar. 2025

[35] A. AlShuaibi, M. W. Arshad, and M. Maayah, "A Hybrid Genetic Algorithm and Hidden Markov Model-Based Hashing Technique for Robust Data Security," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 42–56, May 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.6.

[36] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Towards Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Access*, vol. 9, pp. 113226–113238, 2021, https://doi.org/10.1109/ACCESS.2021.3104148.