

Efficient Zero-Knowledge-Based Cryptographic Mechanisms for Secure Wearable Internet of Things

Chaudhari Minal Yuvaraj¹, Dr. Sanmati Kumar Jain²

1*Research Scholar, School of Computer Science & Engineering, Vikrant University, Gwalior, (M.P.), India
cminal961@gmail.com

2*Ph.D. Guide, School of Computer Science & Engineering, Vikrant University, Gwalior, (M.P.), India
sanmati@vitmindore.com

Abstract

The rapid adoption of wearable Internet of Things (WIoT) devices has enabled continuous monitoring, remote healthcare, fitness tracking, activity recognition, and personalized services. However, wearable devices generate and transmit sensitive information while operating under severe computational, memory, communication, and energy constraints. Conventional authentication and encryption mechanisms may impose significant overhead on such resource-constrained platforms and may expose sensitive identity information during authentication. This paper proposes an efficient zero-knowledge-based cryptographic mechanism for securing wearable Internet of Things environments. The proposed approach uses zero-knowledge proofs (ZKPs) to enable a wearable device to demonstrate possession of a valid secret without directly revealing the secret or sensitive identity attributes. A lightweight authenticated communication layer is incorporated to provide confidentiality and integrity after successful authentication. The proposed architecture consists of a wearable device, a trusted registration authority, a mobile or edge gateway, and a cloud service. The protocol incorporates challenge-response authentication, ephemeral session keys, nonce-based replay protection, and privacy-preserving device authentication. The design is intended to reduce communication and computational overhead while maintaining strong security properties. Security analysis focuses on impersonation, replay, man-in-the-middle, credential disclosure, device tracking, and session-key compromise attacks. Performance evaluation can be conducted using authentication latency, proof-generation time, proof-verification time, communication overhead, memory consumption, and energy consumption as primary metrics. The proposed mechanism provides a research framework for combining zero-knowledge authentication with lightweight cryptography in resource-constrained wearable IoT environments.

Keywords: Wearable Internet of Things, Zero-Knowledge Proof, Lightweight Cryptography, Privacy Preservation, Authentication, IoT Security, Edge Computing, Session Key, Resource-Constrained Devices.

Introduction

The Internet of Things (IoT) has evolved into an ecosystem containing sensors, smartphones, wearable devices, gateways, edge servers, and cloud platforms. Wearable IoT devices such as smartwatches, fitness trackers, smart glasses, medical sensors, and body-area-network devices continuously collect information about users and their surrounding environments. In healthcare applications, these devices may monitor physiological parameters and transmit them to smartphones, healthcare gateways, or cloud services.

Although wearable technology provides significant benefits, its security presents several challenges. Wearable devices generally have limited processing capacity, memory, battery power, and communication bandwidth. Consequently, security mechanisms designed for conventional computers cannot always be deployed directly on wearable platforms. Previous research has specifically identified computational capability, communication overhead, and battery limitations as important considerations in lightweight wearable authentication. ScienceDirect

Security requirements for IoT devices include device identification, secure configuration, data protection, access control, and lifecycle security. NIST guidance similarly emphasizes device cybersecurity capabilities and the need to establish trust before IoT devices are permitted to join a network. NIST Pages+1

Authentication is particularly important because an attacker who successfully impersonates a wearable device may inject false measurements, obtain private information, or gain unauthorized access to associated services. Conventional authentication frequently requires the transmission or verification of identifiers, certificates, passwords, or other credentials. Even when these credentials are cryptographically protected, repeated authentication interactions can potentially contribute to user or device tracking.

Zero-knowledge proofs provide an alternative approach. A zero-knowledge proof enables one party, known as the prover, to demonstrate knowledge of a secret or satisfaction of a statement to another party, known as the verifier, without revealing the underlying secret. Recent research has investigated ZKP mechanisms for IoT security and wearable-based privacy-preserving applications. For example, zk-IoT explores ZKPs for establishing trust in IoT environments, while other research has investigated zero-knowledge mechanisms for privacy-preserving wearable positioning. arXiv+1

This paper therefore investigates a lightweight cryptographic architecture in which ZKP-based authentication is combined with efficient symmetric encryption and ephemeral session-key establishment.

Problem Statement

Wearable IoT security involves a fundamental trade-off between strong protection and limited device resources. A security protocol should provide authentication, confidentiality, integrity, privacy, and replay resistance without imposing excessive computational or energy requirements.

Existing approaches may face one or more of the following challenges:

- High computational cost for resource-constrained wearable devices.
- Excessive communication during authentication.
- Exposure of static device identifiers.
- Vulnerability to replay and impersonation attacks.
- Insufficient protection against device tracking.
- High energy consumption during repeated cryptographic operations.
- Difficulty balancing privacy protection with practical deployment requirements.

Recent work on lightweight cryptographic protocols for wearable health devices illustrates the importance of evaluating computation time, memory footprint, and energy consumption alongside security. IJARCSE

Research Objectives

The primary objectives of this research are:

1. To design a lightweight zero-knowledge-based authentication mechanism for wearable IoT devices.
2. To prevent disclosure of long-term authentication secrets during the authentication process.
3. To provide mutual authentication between wearable devices and gateways.
4. To establish fresh session keys for subsequent secure communication.
5. To provide protection against replay, impersonation, and man-in-the-middle attacks.
6. To reduce authentication communication and computational overhead.
7. To evaluate the proposed mechanism in terms of security, latency, memory usage, communication overhead, and energy consumption.

Proposed System Architecture

The proposed architecture consists of four principal entities:

Wearable Device

The wearable device acts as the resource-constrained IoT endpoint. It collects sensor information and communicates with a trusted gateway. Examples include smartwatches, fitness bands, medical monitoring sensors, and smart wearable accessories.

Registration Authority

The registration authority performs initial device registration and establishes the cryptographic parameters required by the wearable device. It should not need to receive the user's secret during subsequent authentication.

Edge/Mobile Gateway

A smartphone, edge gateway, or local hub acts as an intermediary between the wearable device and cloud services. Computationally expensive verification operations can be shifted toward the gateway when appropriate.

Cloud Service

The cloud platform provides storage, analytics, healthcare services, or other IoT applications. It receives only authenticated and protected information from authorized devices.

The architecture can be represented as:

Wearable Device → Mobile/Edge Gateway → Cloud Service

with the registration authority providing initial trust establishment.

Proposed Cryptographic Mechanism

The proposed mechanism contains five phases:

System Initialization

The system establishes cryptographic parameters and security domains. A cryptographically secure hash function and suitable elliptic-curve or ZKP primitive can be selected according to the target device capabilities.

The system generates public parameters:

$$PP = \{G, q, H, g\}$$

where G represents the selected cryptographic group, q is the relevant group order, H is a cryptographic hash function, and g represents a generator or protocol-specific public parameter.

The precise parameters should be selected after benchmarking the target wearable hardware.

Device Registration

During registration, each wearable device obtains a unique cryptographic identity and associated secret material.

Let the wearable device possess a secret:

$$x \leftarrow \mathbb{Z}_q^*$$

A corresponding public value may be calculated as:

$$X = g^x$$

or through an appropriate elliptic-curve operation:

$$X = xG$$

The registration authority stores only the information required by the selected authentication architecture.

Zero-Knowledge Authentication

During authentication, the wearable device generates a commitment using its secret without transmitting the secret itself.

The device generates a random value:

$$r \leftarrow \mathbb{Z}_q^*$$

and computes a commitment:

$$C = g^r$$

The gateway generates a fresh challenge:

$$c = H(C \parallel N_G \parallel \text{ID}_{\text{session}})$$

where N_G is a gateway-generated nonce.

The wearable computes a response based on its secret and random value:

$$z = r + cx \pmod{q}$$

The gateway verifies the resulting proof using the public information associated with the wearable.

A successful verification establishes that the device possesses the required secret without requiring the secret itself to be transmitted.

The exact construction should be selected according to the intended ZKP security model. For a publication-quality implementation, the researchers should formally specify whether the protocol uses a Schnorr-type proof, a Fiat-Shamir-transformed proof, or another succinct proof system.

Session-Key Establishment

Following successful authentication, the wearable and gateway establish a fresh session key.

For example, using an ephemeral elliptic-curve Diffie-Hellman exchange:

$$K = \text{ECDH}(a, b)$$

The resulting shared value can be processed through a key-derivation function:

$$SK = KDF(K \parallel NW \parallel NG) \quad SK = KDF(K \parallel N_W \parallel N_G)$$

where SK represents the session key and NW, NG, N_W , N_G are fresh nonces.

This prevents the long-term authentication secret from being directly used as the data-encryption key.

Secure Data Transmission

After session establishment, wearable sensor data can be protected using an authenticated encryption mechanism:

$$CT = AEAD_{SK}(M, AD, N) \quad C_T = AEAD_{\{SK\}}(M, AD, N)$$

where:

- MM = sensor message,
- ADAD = authenticated associated data,
- NN = unique nonce,
- CTC_T = ciphertext and authentication tag.

The gateway verifies the authentication tag before forwarding data to the cloud.

Security Requirements

The proposed mechanism should satisfy the following properties.

Confidentiality

Sensor information must remain confidential against unauthorized network participants.

Integrity

An attacker should not be able to modify sensor measurements without detection.

Device Authentication

Only an authorized wearable device should be accepted by the gateway.

Privacy Preservation

The authentication mechanism should avoid unnecessary disclosure of long-term identifiers or authentication secrets.

Replay Resistance

Fresh nonces and challenges should ensure that previously recorded authentication messages cannot simply be reused.

Threat Model

The protocol assumes an active network adversary capable of:

- Intercepting communication.
- Replaying previously recorded messages.

- Modifying messages.
- Injecting fabricated messages.
- Attempting to impersonate legitimate wearable devices.
- Performing man-in-the-middle attacks.
- Observing communication patterns.
- Attempting to obtain long-term authentication secrets.

The adversary is assumed not to possess the internal secret material of an uncompromised wearable device.

Physical compromise of the wearable should be treated as a separate threat model because extraction resistance depends heavily on the hardware platform and secure-storage mechanisms.

Security Analysis

Resistance to Impersonation

An attacker attempting to impersonate a legitimate wearable must generate a valid ZKP response without knowing the device's secret. Assuming the underlying proof system is sound, successful forgery should be computationally infeasible.

Resistance to Replay Attacks

Each authentication session uses fresh challenges and nonces. Consequently, an attacker replaying an old proof should fail verification because the proof is bound to the current challenge.

Resistance to Credential Disclosure

The long-term secret xx is not transmitted during authentication. Instead, the wearable produces a cryptographic proof demonstrating knowledge of the secret.

Man-in-the-Middle Protection

The protocol should bind authentication and session-key establishment to fresh session parameters. Mutual authentication combined with authenticated key exchange can prevent an attacker from transparently substituting an independent session.

Session-Key Protection

Fresh ephemeral key material and a secure KDF can ensure that each communication session obtains an independent session key.

Privacy Protection

Because the wearable proves knowledge of a secret rather than directly disclosing the secret, the protocol can reduce credential exposure. Additional mechanisms, such as pseudonymous identifiers or rotating identifiers, may be required to achieve stronger unlinkability.

Performance Evaluation

The proposed mechanism should be experimentally evaluated using real or representative wearable hardware.

The following metrics are recommended:

Metric	Description
Authentication latency	Time required to complete authentication
Proof generation time	Time required by the wearable to generate a ZKP
Proof verification time	Time required by the gateway to verify the proof
Communication overhead	Total bytes exchanged during authentication
Memory consumption	RAM/flash required by the implementation
Energy consumption	Energy required per authentication session
Session-key generation time	Time required to establish a fresh key
Data encryption throughput	Rate of secure sensor-data processing
Security overhead	Additional computational cost introduced by security mechanisms

A meaningful comparison should include at least one conventional lightweight authentication mechanism and, where technically appropriate, an ECC-based or ZKP-based baseline.

Importantly, performance claims should be reported from actual experiments rather than assumed from theoretical complexity. Recent IoT research demonstrates that ZKP performance can vary considerably depending on the proof system and hardware; for example, one 2026 IoT study reports different proof-generation performance between standard and resource-constrained environments. ScienceDirect

Discussion

The main advantage of the proposed approach is the separation between **proving knowledge of a credential** and **revealing the credential itself**. This characteristic is particularly relevant to wearable environments in which devices frequently communicate through wireless channels and may transmit information associated with an identifiable person.

However, zero-knowledge proofs are not automatically lightweight. Proof generation can introduce additional computation, memory consumption, and energy requirements. Therefore, protocol selection must be based on measurements obtained from the target wearable hardware.

A practical architecture can reduce this burden by assigning verification and other relatively expensive operations to a smartphone or edge gateway while retaining essential secret-handling operations on the wearable. This approach is consistent with broader IoT security research that considers constrained devices alongside gateways and lifecycle security.

Recent research also demonstrates the broader movement toward combining ZKPs with other security mechanisms. For example, PUFZIN combines physical unclonable functions with ZKPs for IoT authentication, while recent IoMT work combines ZKP authentication with ECDH, HKDF, and authenticated encryption. ScienceDirect+1

Limitations

Several limitations should be considered.

The computational cost of the selected ZKP construction may remain significant for extremely constrained wearable devices. Furthermore, privacy at the cryptographic layer does not automatically eliminate traffic analysis or device fingerprinting. Physical attacks, side-channel attacks, compromised gateways, insecure firmware, and malicious cloud services require additional protection mechanisms.

The proposed design should therefore be regarded as one layer within a broader wearable IoT security architecture.

Conclusion

This paper presented an efficient zero-knowledge-based cryptographic framework for securing wearable Internet of Things environments. The proposed mechanism combines privacy-preserving ZKP authentication with fresh session-key establishment and authenticated encryption. The architecture is designed to address the distinctive security and resource constraints of wearable devices while reducing the need to disclose long-term authentication secrets.

The research emphasizes that security and efficiency must be evaluated together. A ZKP mechanism should not be considered suitable for wearable IoT solely because of its theoretical privacy properties; proof-generation cost, verification latency, memory requirements, communication overhead, and energy consumption must also be experimentally measured. Existing research on lightweight wearable cryptography and recent ZKP-based IoT systems provides a foundation for such an evaluation. IJARCSE+2

The proposed framework can therefore serve as a foundation for developing and experimentally validating privacy-preserving authentication protocols for next-generation wearable IoT systems.

References

The research emphasizes that security and efficiency must be evaluated together. A ZKP mechanism should not be considered suitable for wearable IoT solely because of its theoretical privacy properties; proof-generation cost, verification latency, memory requirements, communication overhead, and energy consumption must also be experimentally measured. Existing research on lightweight wearable cryptography and recent ZKP-based IoT systems provides a foundation for such an evaluation.

1. Fagan, M., Megas, K., Marron, J., Brady, K., Cuthill, B., Herold, R., Lemire, D., & Hoehn, N. *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements*. NIST SP 800-213, 2021. NIST Computer Security Resource Center
2. Fagan, M., et al. *IoT Device Cybersecurity Requirement Catalog*. NIST SP 800-213A, 2021. NIST
3. *Lightweight authentication protocols for wearable devices*. Computers & Electrical Engineering, 63, 196–208, 2017. ScienceDirect
4. Ramezan, G., & Meamari, E. *zk-IoT: Securing the Internet of Things with Zero-Knowledge Proofs on Blockchain Platforms*, 2024. arXiv
5. *Maximizing privacy and security of collaborative indoor positioning using zero-knowledge proofs*. Internet of Things, 22, 100801, 2023. ScienceDirect
6. Bindewari, S. *Lightweight Cryptographic Protocols for Wearable Health Devices*, 2025. IJARCSE
7. Commey, D., Hounsinnou, S., & Crosby, G. *PUFZIN: Secure and scalable blockchain-IoT with PUFs and zero-knowledge proofs*. Journal of Information Security and Applications, 100, 104510, 2026. ScienceDirect
8. Anwar et al. *An Energy-Conscious, Regulation-Ready and Formally Verified Security Protocol for Low-Power Medical and Safety Devices*, 2026. IET