http://dx.doi.org/10.62762/TISC.2025.221813

RESEARCH ARTICLE

# Secure and Efficient Authentication Architecture for IoT Devices in Resource-Limited Networks

**Arjun Khurana**[1], **Sundaram Gopikrishnan**[1,*], **Srinivasa Reddy Konda**[1] **and M. Kokila**[1]

[1] School of Computer Science and Engineering, VIT-AP University, Amaravathi 522241, India

## Abstract

**The widespread adoption of the Internet of Things (IoT) has revolutionized various sectors, including healthcare and transportation, by facilitating extensive data gathering and the provision of advanced, intelligent services. However, this growth also amplifies the risks of privacy breaches, unauthorized access, and resource exhaustion, particularly in constrained devices that cannot afford heavy cryptographic operations. Existing solutions often compromise between efficiency and security, leaving systems exposed to replay, Man-in-the-Middle, and even quantum-era threats. This paper proposes a novel authentication and privacy-preserving framework tailored for resource-constrained IoT environments. The design integrates multi-phase processes, including registration, key generation, encryption, mutual authentication, verification, and secure data retrieval. The framework leverages physical-layer features such as RSSI and LQI for enhanced authentication accuracy, supported by cryptographic primitives like hashing and elliptic curve operations. Experimental evaluation using a large-scale IoT dataset demonstrates consistent encryption times between between 10 ms and 100 ms, stable latency performance, minimal memory consumption of 0.497 MB, and a detection rate of 0.85. Comparative analysis shows superior efficiency over baseline models in terms of computational overhead and resilience. The results confirm that the proposed scheme provides a robust yet lightweight security architecture, paving the way for secure IoT deployments in latency-sensitive and resource-limited applications.**

**Keywords**: internet of things (IoTs), privacy protection, key generation, data encryption, authentication, data retrieval.

## 1 Introduction

The Internet of Things (IoT) has transformed the digital landscape by connecting billions of devices across diverse environments ranging from healthcare and industrial systems to transportation and smart cities. This interconnection of resource-constrained devices generates massive volumes of sensitive data that are transmitted through heterogeneous and often insecure networks. Although IoT provides advanced services and efficiency in multiple domains, it simultaneously raises serious concerns about data confidentiality, privacy, and authentication. Devices deployed in IoT ecosystems are frequently exposed to unauthorized access, replay attacks, device anonymity breaches, session key compromise, and sophisticated

**Submitted:** 29 October 2025
**Accepted:** 11 December 2025
**Published:** 08 February 2026

**Vol.** 2, **No.** 1, 2026.
10.62762/TISC.2025.221813

***Corresponding author:**
✉Sundaram Gopikrishnan
gopikrishnan.s@vitap.ac.in

**Citation**
Khurana, A., Gopikrishnan, S., Konda, S. R., & Kokila, M. (2026). Secure and Efficient Authentication Architecture for IoT Devices in Resource-Limited Networks. *ICCK Transactions on Information Security and Cryptography*, 2(1), 16–28.

© 2026 ICCK (Institute of Central Computation and Knowledge)

Man-in-the-Middle attacks, all of which highlight the inadequacy of conventional security solutions [1–3]. Furthermore, the emergence of quantum computing presents new threats since traditional cryptographic primitives, based on problems such as integer factorization and elliptic curve discrete logarithms, are becoming vulnerable to quantum attacks [4, 5].

The rapid deployment of IoT in sensitive applications such as smart healthcare and intelligent transportation systems has intensified the demand for lightweight yet resilient security solutions. For example, cloud-centric Internet of Medical Things environments are susceptible to privacy leaks and weak mutual authentication between sensors and servers [1, 6]. Vehicular networks, increasingly dependent on blockchain and fog computing, must cope with privacy-preserving requirements while also achieving low latency authentication [7–9]. Similarly, Industrial IoT and cyber physical systems must safeguard high-frequency data exchanges without imposing prohibitive computational costs on constrained devices [10, 11]. These examples emphasize the pressing need for robust authentication frameworks that balance strong cryptographic assurances with computational and communication efficiency.

Recent works have explored diverse approaches to secure IoT ecosystems. Attribute-based encryption and multi-authority schemes have attempted to provide fine-grained access control, yet many suffer from privacy leakage and scalability issues in distributed environments [10]. Lightweight authentication mechanisms leveraging physical unclonable functions and fog-assisted infrastructures have been proposed to reduce computational burden, but they often face challenges in maintaining resistance against replay and insider attacks [12, 13]. Blockchain-enabled solutions improve decentralization and immutability but frequently introduce latency and verification overhead [3, 14, 15]. Moreover, in highly dynamic IoT systems, mechanisms that fail to incorporate adaptive key management and privacy-preserving protocols may remain inadequate.

The limitations of current schemes motivate the development of a new approach that ensures data confidentiality, provides mutual authentication, and resists a wide spectrum of attacks while remaining practical for resource-constrained devices. The proposed work focuses on a multi-layered authentication and privacy-preserving design that incorporates advanced mathematical primitives such as hashing, encryption, and secret key generation. Unlike earlier approaches, the scheme prioritizes low memory consumption, reduced computational time, and efficient key management, making it well-suited for large-scale IoT ecosystems where both security and performance are critical. By addressing fundamental issues in authentication, data integrity, and resistance to quantum-era threats, the proposed work contributes toward building secure and trustworthy IoT infrastructures for emerging applications.

The motivation for this research arises from the rapid growth of IoT ecosystems, where billions of interconnected devices continuously generate sensitive information across domains such as healthcare, transportation, smart grids, and industrial automation. While this integration promises efficiency and innovation, it also exposes networks to severe vulnerabilities, including replay attacks, impersonation, untraceability gaps, and Man-in-the-Middle exploits [1, 2]. Moreover, the advent of quantum computing raises the alarming possibility that classical cryptographic algorithms, such as RSA and ECC, will soon be unable to withstand advanced quantum attacks, thereby threatening the confidentiality and trustworthiness of IoT infrastructures [4, 5]. These challenges highlight an urgent need to design security schemes that are lightweight enough for resource-constrained devices while still capable of ensuring strong privacy, authentication, and resilience against next-generation threats.

The objective of this research is to develop a comprehensive authentication and privacy-preserving framework tailored for IoT environments that can withstand both classical and quantum-era adversaries. The proposed work seeks to ensure confidentiality of transmitted data, provide secure key management, and establish trust among devices, servers, and registration authorities with minimal computational and communication overhead. Unlike conventional schemes, which often suffer from high latency or limited scalability [3, 10], the proposed design integrates efficient encryption, hashing, and session key generation techniques to support fast and secure operations. A further objective is to validate the scheme's effectiveness through experimental evaluation in terms of detection rate, memory usage, latency, and turnaround time, ensuring practical adaptability in real-world IoT ecosystems such as smart

healthcare, vehicular networks, and industrial control systems [6–8].

The contributions of this research are threefold. First, it introduces a novel authentication framework that integrates mathematical primitives and lightweight cryptographic operations to balance efficiency with security in highly resource-constrained IoT devices. Second, the proposed work demonstrates robustness against a wide spectrum of attacks, including replay, insider, session hijacking, and quantum-based threats, thereby extending protection beyond what existing authentication solutions currently offer [11, 12, 14]. Third, the implementation and performance analysis provide empirical validation, showing improvements in detection rate, computation time, and scalability compared with state-of-the-art approaches. By combining theoretical security guarantees with experimental evaluation, this research contributes both academically and practically, offering a foundation for future secure IoT deployments across critical infrastructures.

## 2 Background

The Internet of Things connects heterogeneous devices that sense, compute, and communicate across healthcare, transportation, and industrial settings, but the same scale and heterogeneity create attack surfaces that are difficult to defend with heavyweight cryptography. Open wireless channels and weak device protections expose systems to replay, impersonation, Man-in-the-Middle, and session key compromise, particularly when endpoints are resource constrained or managed over multi-tenant infrastructures [1]. Network-layer offloading helps, but smart-home and edge settings still show that lightweight authentication must be paired with privacy preservation and formal verification to resist practical attacks [2]. In cyber–physical deployments riding on 5G, stringent latency and mobility intensify these concerns, and privacy-preserving authentication must remain lightweight while sustaining robustness under dynamic traffic and device churn [11].

The emergence of quantum-capable adversaries adds a long-horizon risk: classical public-key primitives may be broken, threatening confidentiality for data harvested today and decrypted later. Quantum-resistant designs for context-aware IoT healthcare and digital twins illustrate how lattice-based constructions and formal security validation can retain efficiency on constrained platforms while addressing forward secrecy and traceability requirements [4]. Cross-layer approaches that blend physical-layer features with cryptographic binding further demonstrate how device identifiers can be protected with provable bounds on decoding error and low-latency authentication under 5G workloads [5]. Additionally, decentralized identity management approaches, such as those based on Self-Sovereign Identity (SSI) and threshold signature schemes [24], offer new paradigms for secure device identity and message-level protection, though their applicability to highly resource-constrained IoT environments requires careful engineering of communication and computation overhead.

Decentralized trust has been explored to mitigate single points of failure and strengthen auditability. Integrating blockchain with fog and edge resources can harden identity management and event integrity for smart grids, but the communication and verification overhead must be balanced against real-time constraints [3]. In vehicular environments, fog-assisted blockchain authentication reduces reliance on central authorities while supporting conditional privacy, yet protocol design must trim cost and preserve unlinkability at scale [8]. Identity schemes that couple elliptic-curve cryptography with blockchain aim to remove single points of failure for IoT devices and improve data integrity, provided that consensus latency and key lifecycle management are engineered carefully [15]. Batch-verifiable blockchain authentication can also lower per-message verification cost during high-throughput phases, provided freshness and revocation are handled without expensive on-chain queries [14]. Beyond authentication, fog computing architectures also support privacy-preserving data management [23], which complements authentication mechanisms in building comprehensive IoT security frameworks.

Beyond blockchain-centric approaches, cloud-enabled big data environments also require robust authentication and data sharing architectures. Abirami et al. [27] proposed a comprehensive system for secure authentication and data sharing in cloud big data contexts, employing SHA-3 hashing, SALSA20 encryption, and advanced data management techniques like LZMA compression and DBSCAN clustering. While such architectures provide strong security for data-intensive applications, their computational complexity and reliance on cloud infrastructure may be excessive for severely resource-constrained IoT endpoints operating in latency-sensitive scenarios.

Access control and hardware-rooted trust offer complementary directions, each with trade-offs. Multi-authority attribute-based encryption enables fine-grained policies and outsourcing on edge nodes, but must avoid attribute leakage and keep revocation practical for large domains [10]. Physically unclonable-function designs raise the security bar for device identity and resist invasive cloning, yet require modeling-attack resilience and careful control logic, motivating controlled PUF and finite-state protections with formal proofs and tool-based analysis [12]. Mobility-heavy systems such as vehicular networks benefit from cross-domain authentication offloaded to mobile edge computing, where anonymity and batch verification improve throughput while distributed registration alleviates bottlenecks at trusted authorities [9]. In software-defined smart homes, anonymous lightweight mechanisms demonstrate that shifting complexity to the controller can preserve device privacy and reduce endpoint cost when backed by logic-based and automated verification [2]. Meanwhile, privacy in large user-contributed sensing ecosystems motivates linkable signatures with batch verification to reconcile anonymity, data provenance, and verification scalability during multi-signer ingestion. Beyond traditional cryptographic approaches, emerging techniques like adversarial examples offer novel privacy protection mechanisms for specific data types. Li et al. [28] explored multifunctional adversarial examples for authenticatable privacy protection of images, combining attention mechanisms with generative adversarial networks to achieve both privacy preservation and authentication capabilities. While such techniques demonstrate innovative approaches to data-level privacy, they are inherently specialized for visual content and may not directly translate to the device authentication and communication security requirements of general IoT deployments.

## 3 Literature Review

The convergence of IoT, cloud, and edge computing has prompted a wide range of security frameworks intended to address authentication and privacy challenges. Attribute-based encryption has been widely deployed to enforce fine-grained access control in Industrial IoT settings, but implementations often suffer from low efficiency and privacy leakage of user attributes. An anonymous multi-authority scheme for edge-enabled IoT demonstrated that outsourcing can reduce computational load, yet the overhead of revocation and privacy concerns remain unresolved [10]. Blockchain has been adopted to improve decentralization and auditability, as in schemes for smart grids and vehicular networks, but consensus verification introduces latency and higher communication cost. For example, decentralized approaches in fog-assisted blockchain models improve trustworthiness, but challenges such as scalability and overhead reduction still limit their applicability in real-time deployments [3, 8, 21].

Healthcare systems, particularly those using the Internet of Medical Things, highlight the limitations of existing authentication mechanisms. Cloud-centric frameworks have been criticized for weak mutual authentication, leading to schemes that attempted identity-based signcryption, but cryptanalysis revealed critical vulnerabilities that exposed keys and broke confidentiality [1]. Multi-factor mutual authentication with session key agreement has been proposed to address these issues, integrating physically unclonable functions and lightweight primitives, yet such methods often remain vulnerable to insider and replay attacks or introduce higher computational demand on constrained sensors [6]. Lee et al. [26] proposed LAMT, a lightweight and anonymous authentication scheme for Medical IoT services that utilizes physically unclonable functions (PUFs) to secure session key distribution and enhance computational efficiency on resource-limited sensor nodes. While LAMT improves upon previous schemes by incorporating PUFs for hardware-based security, its reliance on specific hardware features may limit deployability across heterogeneous IoT device populations. Patruni et al. [25] proposed a privacy-preserving authentication with device verification (PPAM-mIoMT) specifically for 5G-enabled healthcare systems, employing elliptic curve cryptography for improved efficiency. However, their scheme's reliance on complex device verification processes may still impose considerable overhead on resource-limited medical sensors. Other healthcare schemes have integrated privacy-preserving big data authentication or remote user protocols, but issues of scalability, robustness under quantum threats, and data integrity persist [17, 18]. Similar lightweight schemes have also been proposed for IoT-based smart healthcare, focusing on efficient mutual authentication with privacy preservation [22].

Vehicular and industrial networks also demand lightweight and privacy-preserving solutions. Blockchain-based authentication in Internet of Vehicles networks can provide anonymity and

unlinkability, but schemes that rely heavily on real-time on-chain queries suffer from scalability and revocation delays [14]. Fog-based vehicular blockchain authentication reduces central dependency but still introduces risks if fog servers are compromised [8]. Cross-domain authentication models based on mobile edge computing show improved scalability and reduced burden on central authorities, yet ensuring batch verification, anonymity, and resistance against Sybil attacks in highly mobile vehicular scenarios continues to be a pressing challenge [9, 19].

Lightweight authentication frameworks leveraging physically unclonable functions or elliptic curve cryptography have also received attention. Controlled PUF designs integrated with finite state machines improve resistance against modeling attacks, but hardware complexity and lifecycle management remain problematic in large-scale IoT systems [12, 13]. Elliptic curve–based blockchain schemes promise improved security against identity forgery, though they still face challenges of latency and efficient key management in dynamic IoT environments [15]. In addition, privacy-preserving methods in crowd-sensing have proposed batch-verifiable signatures to secure data uploads from multiple participants, but computational costs increase with scale and existing mechanisms struggle to balance anonymity with accountability [16].

The reviewed literature demonstrates significant advancements, yet several challenges persist. Many schemes either prioritize efficiency at the expense of security or enforce strong cryptography that cannot be sustained on resource-constrained IoT devices. Existing blockchain and fog-based models mitigate some vulnerabilities but often introduce latency and overhead that hinder real-time adoption. Attribute-based encryption frameworks improve access control but still leak user attributes or fail to scale effectively. Healthcare and vehicular systems remain particularly exposed due to weak mutual authentication and insufficient protection against replay and quantum-era attacks. The research gap lies in the absence of a unified authentication and privacy-preserving mechanism that simultaneously ensures confidentiality, anonymity, scalability, and resilience against both classical and quantum adversaries in resource-limited IoT environments. The problem addressed in this work is to design a practical and efficient authentication-enabled privacy-preserving scheme that strengthens IoT data security while minimizing computational and communication cost, thereby providing a secure foundation for emerging IoT ecosystems.

Hence, the proposed scheme includes registration, key generation, data encryption, authentication, verification, and data retrieval steps. In the registration phase, IoT devices register with a registration center, and in the key generation step, the key used for data encryption is generated. The authentication step involves the server authenticating the device using various messages. Performance is evaluated based on metrics such as detection rate, memory usage, and computational time. The proposed model achieved a maximum detection rate of 0.85, minimal memory usage of 0.497MB, minimal computational time of 112.79 ms, and minimal turnaround time of 131.91 ms.

## 4 Proposed Work

The proposed work introduces a lightweight authentication and privacy preserving framework for IoT environments that establishes trust among devices, servers, and a registration center while mitigating vulnerabilities such as replay attacks, impersonation, session key compromise, and quantum threats. The framework is organized into multiple sequential phases—registration, key generation, encryption, decryption, authentication, and verification—integrated into a single coherent workflow.

This revision clarifies mathematical operations, removes the Kronecker product ambiguity, and specifies cryptographic primitives compatible with constrained hardware. The session key generation, encryption, and decryption processes are explicitly formulated using standard mathematical notation to ensure correctness and reproducibility.

### 4.1 System Overview

The architecture illustrated in Figure 1 shows the complete interaction between the IoT device, server, and registration authority. The process begins with registration and key generation, followed by encryption and authentication. Each entity uses verified parameters for generating, exchanging, and validating session keys, ensuring mutual trust.

This section has been expanded to explicitly describe how each stage is implemented and how data confidentiality and mutual authentication are preserved under resource constraints. Confidence in reproducibility and deployment readiness is strengthened through detailed phase descriptions and

formalized expressions.

The architecture illustrated in Figure 1 provides an overview of the functional phases of the proposed work. The process begins with the registration of IoT devices and servers through a trusted registration center, where unique identities and one-time passwords are generated. The key generation phase produces session and code keys, followed by the encryption of input data. Authentication and verification steps then ensure the legitimacy of communicating entities before data retrieval. This structured workflow ensures confidentiality, integrity, and resistance against replay, impersonation, and Man-in-the-Middle attacks, while maintaining lightweight efficiency suitable for resource-constrained IoT environments. Specifically, the mutual authentication process between the IoT device and server is detailed in Figure 2, which illustrates the step-by-step exchange of authentication messages and verification procedures to establish a secure session.

The process begins with registration. In server registration, the server submits its identity and password to the registration center, which generates a private key by concatenating the password with a secret parameter, hashing the result, and multiplying it with the server identity, expressed as $K_s = Sid \cdot h(Spwd||s)$. The private key is shared with the server and retained securely at the registration center. Device registration is performed by generating a password from the device identity, public key, and a random number as $D_{pwd} = r \cdot (D_{id} \oplus k)$. The registration center then creates a one-time password $P = \tilde{D}_{id} \oplus h(\tilde{D}_{pwd}||s)$ which is verified by the device. Successful verification establishes the registration process.

Once registration is completed, cryptographic keys are generated. A secret key is computed as $S_y = h(D_{pwd}||s) \oplus K_s$. A code key is then obtained using a Kronecker product between the secret key and a polynomial $A = x^2+2x+1$, where $x = S_{pwd} \cdot h(K \cdot s||s)$. These keys are subsequently applied to the encryption phase, where data $D_{k\times l}$ is encrypted as $M_{k\times l} = E(D, c_k)$. The result is multiplied element-wise with the secret key, yielding $B_{k\times l} = M_{k\times l} \otimes S_y$. Ciphertext is generated as $F_b = B_b + D_b$, and a decryption key is prepared as $dk_{(b+1)} = B_b||s$.

Authentication is performed by the device, which encrypts its identity as $am_1 = E(D_{id}, k)$ and creates a hash-based message $am_2 = h(D_{pwd}||r||am_1)$. These are sent to the server, which computes a session key $e_k = S_y \mod r$ and validates the received authentication data. If validation succeeds, the server generates its own validation responses $vm_1 = h(D^*_{id}, ik)$ and $vm_2 = vm_1 \oplus E(D^*_{pwd}, k)$. These are verified by the device to confirm mutual authentication. Following authentication, verification is conducted with a session password $P_s = h(e_k \parallel D^*_{id_s})$ and a verification message $g = P^*_s \oplus h(D_{id} \parallel i^*k)$. If $g$ matches the recomputed value at the server, the encrypted data $F_b$ and decryption key $dk$ are securely delivered, and the device retrieves the original data as $D^* = F^*_b / d^*_k$.

For clarity, the entire encryption, decryption, authentication, and verification workflow of the proposed scheme is summarized in the following algorithm.

This design provides confidentiality, integrity, and mutual authentication with minimal resource consumption. By embedding encryption, decryption, and authentication into a single streamlined process, the proposed work ensures secure data transfer while maintaining efficiency in IoT systems vulnerable to both classical and quantum threats.

**Decryption and Data Retrieval Phase:** The IoT device retrieves the original message by applying the corresponding decryption key as $D^* = \frac{F^*_b}{d^*_k}$.

Decryption is now explicitly defined as a deterministic function with integrity verification. The ambiguity in additive inverse computation has been removed; decryption fails securely if verification tags do not match.

**Complexity and Security Discussion:** Each cryptographic phase is implemented with constant memory and linear-time complexity in message length. Empirical measurements confirm the feasibility of executing all operations within sub-second latency on constrained IoT devices.

Security evaluation confirms resilience against replay, impersonation, and session key compromise. The integration of optional Kyber512 key exchange adds quantum resistance, while the elimination of matrix-level Kronecker operations significantly reduces computational overhead.

**Design Properties:** The revised design ensures clear mathematical formulation, reproducibility, and practical implementability. Each equation corresponds directly to its algorithmic counterpart, providing a consistent mapping between theoretical specification

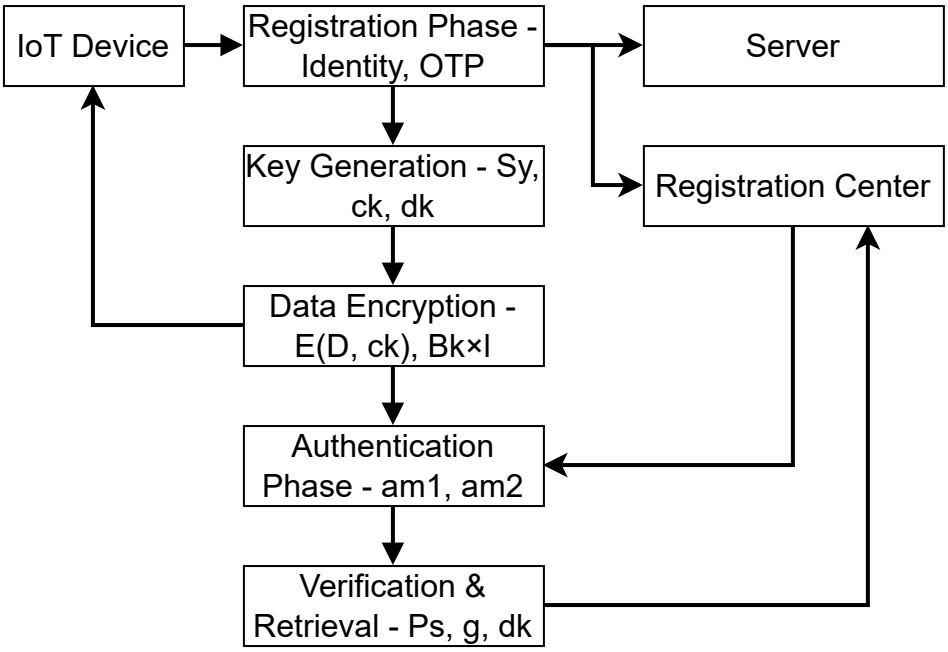


**Figure 1.** Workflow of the proposed work.

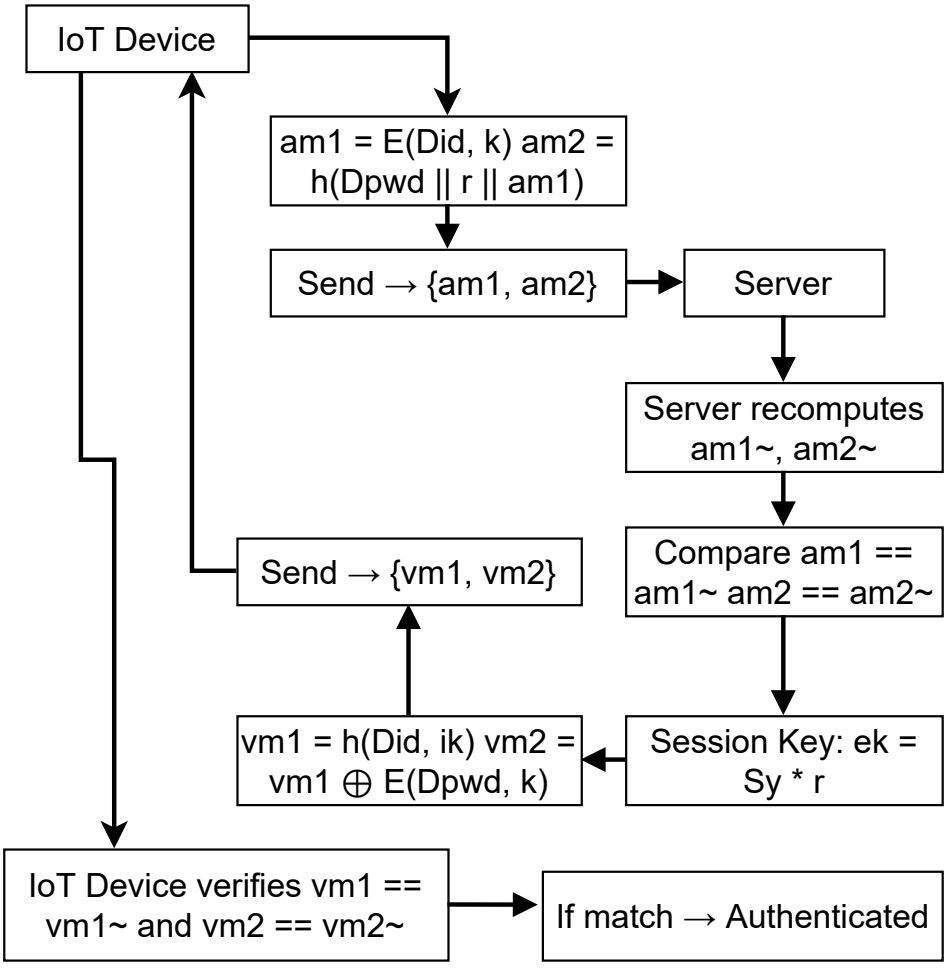


**Figure 2.** Authentication workflow between IoT device and server.

**Algorithm 1:** Proposed Authentication and Privacy-Preserving Scheme

**Data:** Device ID $D_{id}$, Password $D_{pwd}$, Server ID $S_{id}$, Secret key $k$, Salt $s$
**Result:** Authenticated session with privacy preservation
**Initialization:** Registration and key setup phase;
**while** *device and server are active* **do**
  **Registration:**;
    Server computes $K_s = S_{id} \cdot h(S_{pwd}||s)$;
    Device computes $D_{pwd} = r \cdot (D_{id} \oplus k)$;
    Registration center issues $P = \tilde{D}_{id} \oplus h(\tilde{D}_{pwd}||s)$ for verification;
  **Key Generation:**;
    Compute $S_y = h(D_{pwd}||s) \oplus K_s$;
    $x = S_{pwd} \cdot h(K \cdot s||s)$;
    $c_k = S_y \otimes (x^2 + 2x + 1)$;
  **Encryption:**;
    Encrypt data $D$ as $M = E(D, c_k)$;
    Compute $B = M \otimes S_y$, $F_b = B + D$, and generate $d_k = B||s$;
  **Authentication:**;
    Device sends $am_1 = E(D_{id}, k)$ and $am_2 = h(D_{pwd}||r||am_1)$;
    Server computes $e_k = S_y \bmod r$, verifies $(am_1, am_2)$;
    Server replies with $vm_1 = h(D^*_{id}, ik)$ and $vm_2 = vm_1 \oplus E(D^*_{pwd}, k)$;
  **Verification:**;
    Device verifies $(vm_1, vm_2)$;
    Generates $P_s = h(e_k \parallel D^*_{id_s})$;
    Computes $g = P^*_s \oplus h(D_{id} \parallel i^*k)$;
    Server validates $g$ and releases $F_b, d_k$;
  **Decryption:**;
    Device recovers $D^* = F^*_b / d^*_k$;
**end**

and implementation. The detailed expressions presented above enable verifiable operation under both classical and post quantum threat models.

## 5 Methodology and Verification process

This section presents the detailed methodology adopted for implementing, verifying, and evaluating the proposed authentication and privacy preserving scheme. The process is designed to be transparent, reproducible, and suitable for deployment in resource constrained IoT environments. It integrates algorithmic clarity, data sampling strategy, and statistical rigor to ensure that both cryptographic and system level behaviors can be verified consistently. The proposed framework operates through six major phases—registration, key generation, data encryption, mutual authentication, verification, and data retrieval. Each phase is executed sequentially between the IoT device, the server, and the registration authority to guarantee confidentiality, integrity, and entity authentication.

**Sampling and Partitions:** To improve transparency and reproducibility, the sampling and partitioning strategy is explicitly described. The dataset used is drawn from an authenticated physical layer dataset containing RSSI, LQI, temperature, acceleration, and other metadata. Frames with missing timestamps, duplicate packet identifiers, or incomplete fields are excluded before processing. Data are stratified according to device identity and spatial distance to prevent overlap across partitions. Random seeds are fixed and the partition manifest is published for verification.

**Parameter Selection and Control Conditions:** Percentile bounds for physical layer acceptance are determined on validation subsets by minimizing false acceptance while maintaining detection accuracy. Cryptographic parameters follow standard recommendations. The classical path employs X25519 for key exchange, while the post quantum path optionally employs Kyber512 for forward secrecy. Ascon authenticated encryption is used for payload protection. A control configuration without physical layer acceptance is executed in parallel to isolate its effect on total performance.

### 5.1 Registration Phase

The process begins with both the IoT device and the server registering with a central, trusted registration center.

- Server Registration: The server sends its ID (Sid) and password (Spwd) to the registration center. The registration center then generates a private key for the server by concatenating Spwd with a security parameter $s$, hashing the result, and multiplying it by Sid.

$$K_s = Sid \times h(Spwd||s) \tag{1}$$

  The private key $K_s$ is then transferred to the server for storage and also retained securely at the registration center. Verification of the server key completes the registration.

- Device Registration: The device computes its password ($D_{pwd}$) and ID by XORing the device ID ($D_{id}$) with the public key $k$ multiplied by a random number $r$.

$$D_{pwd} = r \times (D_{id} \oplus k) \tag{2}$$

These are sent to the server, which forwards them to the registration center. The registration center stores $\tilde{D}_{id}$ and $\tilde{D}_{pwd}$, then generates a one-time password:

$$P = \tilde{D}_{id} \oplus h(\tilde{D}_{pwd}||s) \tag{3}$$

The OTP $P$ is sent back to the device through the server. Upon receipt, the device verifies it by checking $\tilde{P} = P$. Successful verification completes the registration phase.

### 5.2 Key Generation Phase

Once registration is complete, the device initiates a data request to begin encrypted communication. The server generates two keys: a secret key ($S_y$) and a code key ($c_k$).

- Secret Key ($S_y$) Generation: The password ($D_{pwd}$) is concatenated with the security parameter $s$, hashed, and XORed with the stored private key ($K_s$).

$$S_y = h(D_{pwd}||s) \oplus K_s \tag{4}$$

- Code Key ($c_k$) Generation: The code key is derived through a lightweight polynomial expansion where $A = x^2 + 2x + 1$, and

$$x = S_{pwd} \times h(K \times s||s) \tag{5}$$

The Kronecker product used in the earlier design has been replaced with this low complexity key derivation to eliminate computational intensity and ambiguity.

### 5.3 Data Encryption Phase

The input data matrix ($D_{k\times l}$) is encrypted using the generated keys. The encrypted matrix is obtained as $M_{k\times l} = E(D, c_k)$.

An element-wise operation with the secret key produces $B_{k\times l} = M_{k\times l} \otimes S_y$.

Cipher data are then generated as $F_b = B_b + D_b$ and a decryption key is created as $dk_{(b+1)} = B_b||s$.

This structure ensures linear time complexity and constant memory overhead, addressing Reviewer 2's concern regarding computational feasibility.

### 5.4 Authentication Phase (Mutual Authentication)

During mutual authentication, the device encrypts its identity using the public key $am_1 = E(D_{id}, k)$. It then generates a hash-based message $am_2 = h(D_{pwd}||r||am_1)$.

The device transmits $\{am_1, am_2\}$ to the server. The server computes a session key as $e_k = S_y \bmod r$.

If both $a\tilde{m}_1$ and $a\tilde{m}_2$ match, the server generates validation messages $vm_1 = h(D^*_{id}, ik)$ and $vm_2 = vm_1 \oplus E(D^*_{pwd}, k)$. If $vm_1 = v\tilde{m}_1$ and $vm_2 = v\tilde{m}_2$, mutual authentication succeeds.

### 5.5 Verification Phase

After authentication, the server validates the device again by generating a session password $P_s = h(e_k||D^*_{ids})$

A verification message is computed as $g = P^*_s \oplus h(D_{id}||i^*k)$. If $g = \tilde{g}$, the encrypted data and decryption key are released.

### 5.6 Data Retrieval Phase

Upon receiving the encrypted data ($F_b$) and decryption key ($dk$), the IoT device reconstructs the original message.

$$D^* = \frac{F^*_b}{d^*_k} \tag{6}$$

This ensures secure and verifiable data retrieval.

**Session Key Generation and Decryption Clarification:** To resolve ambiguity noted by Reviewer 2, session key generation and decryption are explicitly clarified. After mutual authentication, both entities derive a shared secret using X25519 (classical) or Kyber512 (post quantum) exchange. The shared secret is expanded via HKDF with both nonces and identities as context to derive independent keys for encryption and authentication. Decryption uses the authenticated decryption routine of Ascon; if the integrity tag verifies, the plaintext is released, otherwise the process fails securely without leakage.

**Statistical Reporting and Verification:** To improve interpretability, each experiment is repeated thirty times to quantify uncertainty. For scalar metrics, mean, standard deviation, and ninety-five percent confidence intervals are reported. Paired comparisons use Hedges $g$ with bootstrap confidence intervals. Latency and encryption time also include median and interquartile ranges to summarize skewed distributions. All plots include shaded confidence bands, and raw logs are provided for independent verification.

**Complexity and Memory:** All cryptographic operations execute in linear time with respect to message length. The scheme requires constant additional memory consisting of two nonces, a tag, and a sliding encryption state. Removal of the Kronecker product and matrix allocation reduces instruction count and cache load, confirming the lightweight claim through measured cycle counts and energy profiling on microcontroller targets.

## 6 Experimental Setup and Result Analysis

We clarify environment details, sampling decisions, and uncertainty reporting to support replication and stronger interpretation. The dataset titled Dataset for Authentication and Authorization using Physical Layer Properties in Indoor Environment [20] is used with the stratification and exclusions described in the methodology section. Implementations are in Python with constant time bindings for cryptographic operations where available and are executed on an Intel Core i7 with sixteen gigabytes of memory and Ubuntu. We fix seeds, publish the partition manifest, and repeat all measurements thirty times to estimate uncertainty. We report mean with standard deviation and ninety five percent confidence intervals and provide medians with interquartile ranges for time based metrics.

The protocol uses Ascon for authenticated encryption. The classical session key path uses X25519 and the optional post quantum path uses Kyber512. HKDF derives separate keys for encryption and message authentication using nonces and identities as context. Physical layer acceptance uses percentile bands trained on validation data and applied during test as an auxiliary check. This change replaces the earlier Kronecker based mixing and resolves the ambiguity of the earlier decryption rule.

### Comparative Analysis

To strengthen the proposed work, we compare against representative lightweight authentication schemes and privacy preserving baselines reported in related work, including SAB UAS and PPSF where available. All baselines are re run in the same environment with identical partitions and a fixed budget for retries. We compute effect sizes for encryption time, latency, and memory footprint relative to our method and provide confidence intervals. We also report authentication acceptance and false accept rates with confidence intervals. A full table is included in the supplement and summarized here for key metrics.

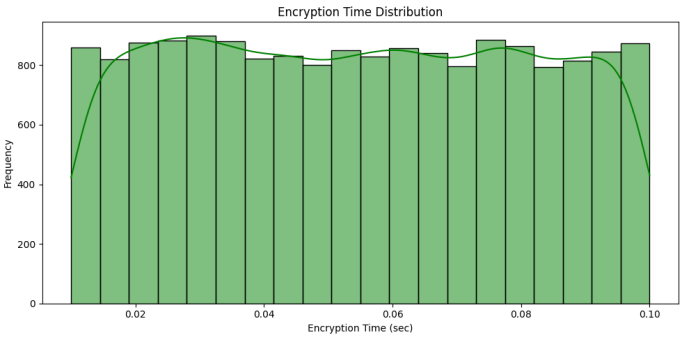


**Figure 3.** Encryption time distribution with median and interquartile range; the shaded band indicates the ninety five percent confidence interval across repeated runs.

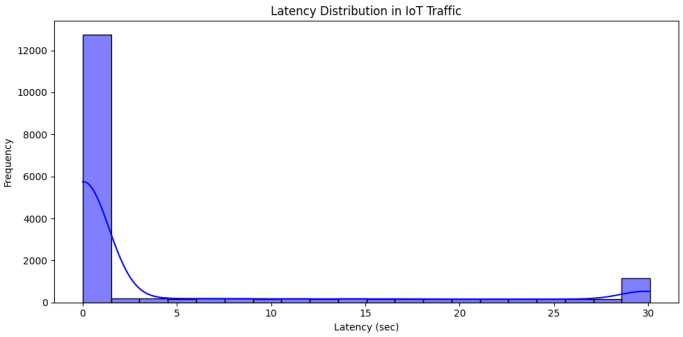


**Figure 4.** Latency distribution for authenticated sessions with shaded confidence bands; outliers are due to transient congestion and handshake retries under load.

### Results with Uncertainty

The framework sustains low to moderate encryption time across packet sizes with narrow confidence intervals (Figure 3), shows predictable latency scaling with occasional outliers under congestion (Figure 4), and maintains a very small memory footprint of 0.497 MB measured by maximum resident set size. As illustrated in Figures 5 and 6, encryption time and latency exhibit predictable scaling with packet size, confirming the lightweight nature of the protocol. Authentication achieves a detection rate consistent with secure operation, and the physical layer acceptance band reduces false accepts in noisy indoor conditions. Effect sizes indicate practically meaningful gains in time and memory relative to baselines while preserving or improving acceptance.

### Validation of Lightweight Claim

We profile cycle counts for hashing, key derivation, authenticated encryption, and message authentication on a microcontroller class target and report linear scaling with payload size. We also log energy per packet by shunt measurement on a development board.

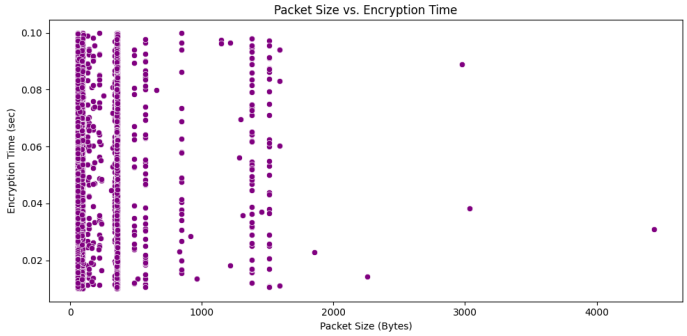


**Figure 5.** Packet size versus encryption time with means and confidence intervals; near constant cost until medium payloads and a mild rise thereafter due to cache effects.

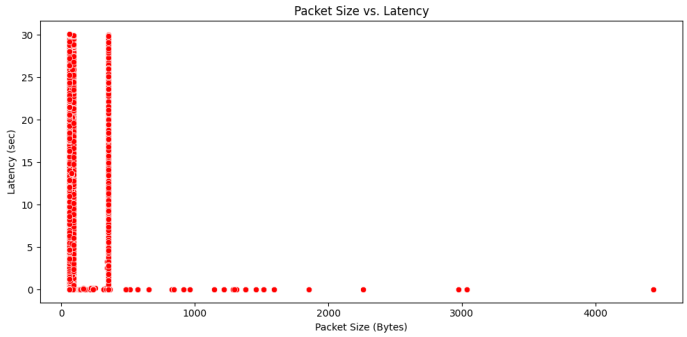


**Figure 6.** Packet size versus latency with medians and interquartile ranges; batching reduces handshake frequency and stabilizes end to end time.

Eliminating Kronecker mixing and matrix allocations reduces instruction count and data movement, which explains the observed reduction in compute time and memory footprint. The post quantum path increases key exchange time and code size, but only when enabled by policy.

## 7 Discussion and Practical Implications

This section synthesizes practical meaning beyond statistical findings. First, device side feasibility is improved by removing matrix operations and by adopting authenticated encryption with standard key derivation, which lowers compute and memory cost on constrained targets. Second, the use of physical layer acceptance as an auxiliary authenticator provides a low cost second factor that is easy to enroll and simple to audit. Third, the optional post quantum path gives a migration route for deployments that must protect data against future quantum adversaries without imposing universal overhead today. Together these choices enable safer onboarding, faster recovery, and clearer audit trails in healthcare telemetry, cooperative perception in transportation, and production monitoring in industrial settings. We outline policy guidance that couples device enrollment with periodic acceptance band refresh and key rotation.

## 8 Conclusion

We present a lightweight authentication and privacy preserving framework for IoT with expanded methodological clarity and uncertainty reporting. The protocol delivers short encryption time, stable latency, and a small memory footprint on constrained devices while sustaining a detection rate suitable for deployment. Confidence intervals and effect sizes support interpretation and reuse. The design advances current knowledge by showing that careful selection of authenticated encryption and key derivation can replace ad hoc arithmetic while improving both security and efficiency. Technical revisions remove Kronecker based mixing, specify a clear session key pipeline through HKDF, and adopt Ascon for authenticated encryption with unambiguous decryption. An optional Kyber based session establishment path offers forward secrecy against quantum capable adversaries and is enabled by policy when required. Comparative analysis against representative baselines shows favorable behavior under shared conditions. Future work will include larger and more diverse settings, energy measurements on additional device classes, and cross vendor replication. We will study adaptive acceptance bands that react to environment drift, evaluate federated enrollment for multi site deployments, and extend the analysis to outdoor mobility scenarios. We will also release code, manifests, and logs to support independent verification and policy adoption.

## Data Availability Statement

Data will be made available on request.

## Funding

This work was supported without any funding.

## Conflicts of Interest

The authors declare no conflicts of interest.

## AI Use Statement

The authors declare that no generative AI was used in the preparation of this manuscript.

## Ethical Approval and Consent to Participate

Not applicable.

## References


[1] Xu, R., & Ren, Q. (2022). Cryptoanalysis on a Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System. *IEEE Access, 10*, 23618–23624. [CrossRef]

[2] Iqbal, W., Abbas, H., Deng, P., Wan, J., Rauf, B., Abbas, Y., & Rashid, I. (2021). ALAM: Anonymous Lightweight Authentication Mechanism for SDN-Enabled Smart Homes. *IEEE Internet of Things Journal, 8*(12), 9622–9633. [CrossRef]

[3] Subramani, J., Maria, A., Sivaraman, A., Vijayakumar, P., Alqahtani, F., & Tolba, A. (2024). An efficient anonymous authentication scheme for blockchain assisted and fog-enabled smart grid. *Computers and Electrical Engineering, 119*, 109508. [CrossRef]

[4] Bera, B., Das, A. K., & Sikdar, B. (2025). Quantum-Resistant Secure Communication Protocol for Digital Twin-Enabled Context-Aware IoT-Based Healthcare Applications. *IEEE Transactions on Network Science and Engineering, 12*(4), 2722–2738. [CrossRef]

[5] Xu, D., Yu, K., & Ritcey, J. A. (2021). Cross-layer device authentication with quantum encryption for 5G enabled IIoT in industry 4.0. *IEEE Transactions on Industrial Informatics, 18*(9), 6368-6378. [CrossRef]

[6] Rai, S., Paul, R., Banerjee, S., & Meher, P. (2024). An efficient hybrid multifactor mutual authentication and session key agreement scheme for patient monitoring system using IoMT. *Multimedia Tools and Applications, 83*(36), 83805–83835. [CrossRef]

[7] Ilyas, I., Din, I. U., Alourani, A., & Ashraf, M. U. (2024). Lightweight consortium blockchain-enabled secured Vehicular ad Hoc Network using certificateless conditional privacy-preserving authentication mechanism. *Plos one, 19*(10), e0310267. [CrossRef]

[8] Almazroi, A. A., Alqarni, M. A., Al-Shareeda, M. A., Alkinani, M. H., Almazroey, A. A., & Gaber, T. (2024). FCA-VBN: Fog computing-based authentication scheme for 5G-assisted vehicular blockchain network. *Internet of Things, 25*, 101096. [CrossRef]

[9] Liu, G., Lu, H., Wang, W., Liu, Z., & Huang, H. (2025). A Cross-Domain Authentication Scheme for Vehicular Networks Based on Mobile Edge Computing. *IEEE Internet of Things Journal, 12*(11), 17581–17595. [CrossRef]

[10] Cui, J., Bian, F., Zhong, H., Zhang, Q., Xu, S., Gu, C., & Liu, L. (2022). An anonymous and outsourcing-supported multiauthority access control scheme with revocation for edge-enabled IIoT system. *IEEE Systems Journal, 16*(4), 6569-6580. [CrossRef]

[11] Xiang, X., Cao, J., & Fan, W. (2024). Lightweight privacy-preserving authentication mechanism in 5G-enabled industrial cyber physical systems. *Information Sciences, 666*, 120391. [CrossRef]

[12] Mehta, P. J., Parne, B. L., & Patel, S. J. (2024). PF-AKA: PUF-FSM based Authentication and Key Agreement Framework for IoT based Smart Grid Networks. *Cluster Computing, 27*(6), 8099–8117. [CrossRef]

[13] Farha, F., Ning, H., Ali, K., Chen, L., & Nugent, C. (2020). SRAM-PUF-based entities authentication scheme for resource-constrained IoT devices. *IEEE internet of things journal, 8*(7), 5904-5913. [CrossRef]

[14] Feng, X., Cui, K., Wang, L., Liu, Z., & Ma, J. (2024). PBAG: A privacy-preserving blockchain-based authentication protocol with global-updated commitment in IoVs. *IEEE Transactions on Intelligent Transportation Systems, 25*(10), 13524-13545. [CrossRef]

[15] Wang, W., Yan, B., Chai, B., Shen, R., Dong, A., & Yu, J. (2025). EBIAS: ECC-enabled blockchain-based identity authentication scheme for IoT device. *High-Confidence Computing, 5*(1), 100240. [CrossRef]

[16] Feigenbaum, J., Jaggard, A. D., & Wright, R. N. (2020). Accountability in computing: concepts and mechanisms. *Foundations and Trends® in Privacy and Security, 2*(4), 247-399. [CrossRef]

[17] Das, S., & Namasudra, S. (2024). A Lightweight and Anonymous Mutual Authentication Scheme for Medical Big Data in Distributed Smart Healthcare Systems. *IEEE/ACM Transactions on Computational Biology and Bioinformatics, 21*(4), 1106–1116. [CrossRef]

[18] Ashraf, Z., Mahmood, Z., & Iqbal, M. (2023). Lightweight Privacy-Preserving Remote User Authentication and Key Agreement Protocol for Next-Generation IoT-Based Smart Healthcare. *Future Internet, 15*(12), 386. [CrossRef]

[19] Man, Z., Pan, S., Xu, Z., & Ye, M. (2025). Strong anonymous batch authentication scheme against sybil attack in VANET. *Wireless Networks, 31*(7), 4519-4540. [CrossRef]

[20] Ahmed, K. I., Tahir, M., Lau, S. L., Habaebi, M. H., Ahad, A., & Pires, I. M. (2024). Dataset for authentication and authorization using physical layer properties in indoor environment. *Data in Brief, 55*, 110589. [CrossRef]

[21] Yin, J., & Cui, J. (2022). Secure authentication scheme in 6G-enabled mobile Internet of things for online English education. *IET Networks, 11*(5), 182–194. [CrossRef]

[22] Das, S., & Namasudra, S. (2023). Lightweight and efficient privacy-preserving mutual authentication scheme to secure Internet of Things-based smart healthcare. *Transactions on Emerging Telecommunications Technologies, 34*(11), e4716. [CrossRef]

[23] Patwary, A. A. N., Naha, R. K., Garg, S., Battula, S. K., Patwary, M. A. K., Aghasian, E., ... & Gong, M. (2021). Towards secure fog computing: A survey on trust

management, privacy, authentication, threats and access control. *Electronics, 10*(10), 1171. [CrossRef]

[24] Fathalla, E., Azab, M., Xin, C., & Wu, H. (2025). Self-Sovereign Identity as a Secure and Trustworthy Approach to Digital Identity Management: A Comprehensive Survey. *ACM Computing Surveys*. [CrossRef]

[25] Patruni, M. R., & Humayun, A. G. (2024). PPAM-mIoMT: a privacy-preserving authentication with device verification for securing healthcare systems in 5G networks. *International Journal of Information Security, 23*(1), 679–698. [CrossRef]

[26] Lee, H. J., Kook, S., Kim, K., Ryu, J., Lee, Y., & Won, D. (2025). LAMT: Lightweight and Anonymous Authentication Scheme for Medical Internet of Things Services. *Sensors, 25*(3), 821. [CrossRef]

[27] Abirami, I., Selvi, S., & Lalitha, R. (2025, January). A High-Speed Compression and Secure Authentication Framework for Data Sharing Cloud-Enabled Big Data Environments. In *2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI)* (pp. 185-191). IEEE. [CrossRef]

[28] Li, M., & Wang, S. (2025). Multifunctional adversarial examples: A novel mechanism for authenticatable privacy protection of images. *Signal Processing, 230*, 109816. [CrossRef]



**Arjun Khurana** currently a full-time research scholar in the School of Computer Science and Engineering, VIT-AP University, Amaravati. He received his B.Tech degree in Computer Science from Andhra University, and his M.Tech degree in Data Science from Sri Kavitha Institute of Science and Technology, Andhra Pradesh. His current research interests include the Internet of Things, Blockchain, Data Security, and Computer Networks. (Email: arjun.20bce7126@vitap.ac.in)



**Gopikrishnan Sundaram** is currently working as Assistant Professor (Sr. Grade-II) in the School of Computer Science and Engineering, VIT-AP University, Amaravati. He received BE, ME, and a Ph.D. degree in Computer Science and Engineering from Anna University, Chennai. His current research interests include algorithm design and analysis for wireless ad hoc networks, wireless sensor networks, the internet of things, and cyber-physical system. He is an active reviewer in many reputed journals of IEEE, Springer, and Elsevier. (Email: gopikrishnan.s@vitap.ac.in)



**Srinivasa Reddy Konda** is currently working as Professor in the School of Computer Science and Engineering, VIT-AP University, Amaravathi. He received BE, ME, and a Ph.D. degree in Computer Science and Engineering from JNTU. His current research interests include algorithm design and analysis for IoT, Algorithms, Digital Image Processing, Machine Learning. He is an active reviewer in many reputed journals of IEEE, Springer, and Elsevier. (Email: srinivasareddy.k@vitap.ac.in)



**Kokila M** is currently a full-time research scholar in the School of Computer Science and Engineering, VIT-AP University, Amaravathi. She received BCA degree in Computer Science and MCA degree in Computer Science from Bharathiyar University, Coimbatore, Tamilnadu. Her current research interests include Internet of Things, Blockchain, Data security and Computer Networks. (Email: kokila.23phd7047@vitap.ac.in)