# A Novel Energy-efficient and Secure Identity Authentication Scheme for IoT Networks

Annu Malik
Department of Computer Science & Engineering and Information Technology, Jaypee Institute of Information Technology

Rashmi Kushwah
Department of Computer Science & Engineering and Information Technology, Jaypee Institute of Information Technology

https://doi.org/10.5109/7342466

出版情報：Evergreen. 12 (1), pp.460-475, 2025-03. Interdisciplinary Graduate School of Engineering Sciences, Kyushu University, Japan
バージョン：

# A Novel Energy-efficient and Secure Identity Authentication Scheme for IoT Networks

Annu Malik[1,*], Rashmi Kushwah[1]

[1]Department of Computer Science & Engineering and Information Technology, Jaypee Institute of Information Technology, A 10, A Block, Block A, Industrial Area, Sector 62, Noida, Uttar Pradesh, 201304, India

*Author to whom correspondence should be addressed:
E-mail: annu.knit@gmail.com, rashmi.31130@gmail.com

(Received June 7, 2024; Revised February 6, 2025; Accepted February 16, 2025).

**Abstract**: The Internet of Things (IoT) is a network of various interconnected devices that communicate and exchange data through the Internet. The IoT devices rely on the unreliable web for data transfer; therefore, it is vital to develop secure communication to safeguard end-to-end communication among these devices. IoT devices must transmit data that is resistant to a variety of hostile attacks to reduce energy consumption while maintaining data privacy and integrity. The existing Public Key Infrastructure (PKI)-based secure authentication technique is challenging in many IoT devices due to associated costs with key distribution and management. Therefore, we provided a novel identity authentication system for energy-efficient IoT devices. This paper proposes an Energy-efficient and Secure Identity Authentication (ESIA) scheme for the delay constraint, low power and secure communication in IoT networks. The proposed method achieves mutual identity authentication between IoT servers and devices using three steps: initialization, pairing, and authentication. These steps establish secure sessions among the interacting devices. The proposed scheme enhances the security of IoT devices by removing the need for third-party authentication. The ESIA scheme is robust, energy efficient and resistant to a variety of possible attacks. The simulation results show that the proposed method transmits data with less computation and transmission overhead than existing methods.

Keywords: IoT; Authentication; ESIA; Identity; Attacks

## 1. Introduction

The Internet of Things (IoT) is a rapidly growing network of interconnected wireless devices that are deployed in diverse applications. Over the past decade, IoT has attracted significant attention due to the increasing number of wireless endpoints and the potential for enabling smart environments. However, a major challenge hindering the widespread adoption of IoT is the security requirements associated with these devices[1,2]. Many IoT terminals are low-cost, resource-constrained devices that operate in remote or unattended environments, often without human intervention. These devices are typically deployed in a wide range of settings, from smart homes and healthcare to industrial automation, where real-time control and monitoring of environmental conditions are required.

Energy efficiency is another critical factor for IoT devices, as most are designed to operate for extended periods on limited power resources[3]. As a result, energy consumption plays a pivotal role in the overall performance and longevity of IoT networks. Securing communication between these devices, while also ensuring low energy consumption, is therefore a complex task[4]. These devices generate real-time data that needs to be transmitted to remote servers or gateways for processing and visualization. It is crucial that the transmitted data is resistant to potential attacks, as any compromise in security can have significant consequences. Thus, improving network security, energy efficiency, and transmission rate simultaneously is essential for maintaining the integrity of IoT communications.

Despite advancements in IoT security mechanisms, securing these resource-constrained devices remains a challenge. Traditional security approaches often require significant computational resources, which may not be feasible for lightweight IoT devices. The need for security mechanisms that can ensure safe and efficient communication between these devices while minimizing power consumption is more pressing than ever[5,6]. Moreover, as IoT devices become integral to critical infrastructures, the need for robust, scalable, and energy-efficient security solutions becomes even more evident. This paper addresses these challenges by proposing an Energy-efficient and Secure Identity Authentication

(ESIA) scheme that balances security and energy efficiency in IoT networks.

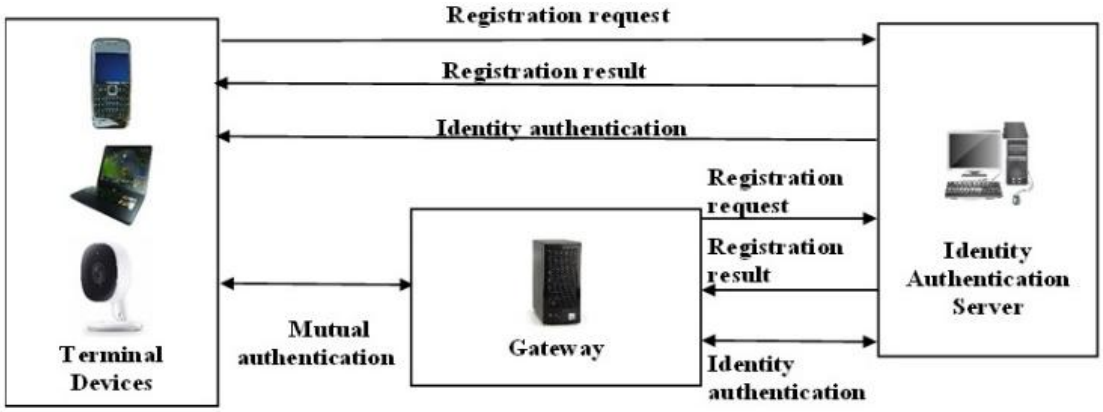


**Fig. 1:** Identity authentication model of IoT devices.

The design and implementation of security mechanisms for the Internet of Things (IoT) must be carried out with care, as vulnerabilities in critical infrastructures cannot be tested continuously through patch updates. In an IoT network, identification typically involves sending a private key and performing a cross-validation test. A device is considered legitimate if it matches the credentials of a previously registered device[1,7]. Ensuring secure identity verification at higher layers is crucial for IoT terminal devices to establish safe communication with the network. Endpoint device identification and authentication methods generally fall into two categories: cryptographic and non-cryptographic-based approaches. The Public Key Infrastructure (PKI) method is widely used in cybersecurity for identity authentication; however, implementing PKI in lightweight smart devices can be problematic due to the high cost of key management and the resource-intensive nature of the system[2,8]. This challenge has hindered the widespread application of PKI in IoT networks, where every device requires a digital identity tied to a PKI system.

In this context, we propose an Energy-efficient and Secure Identity Authentication (ESIA) scheme that addresses both the need for secure identity verification and the energy constraints of IoT devices. The ESIA scheme strengthens the security of IoT devices by eliminating the need for third-party authentication and supporting secure, efficient data transfer between devices. This approach is particularly beneficial for IoT applications with privacy concerns, such as smart cities, smart hospitals, automation in industries, and smart buildings. The proposed ESIA scheme is designed for resource-constrained devices that gather and send data via gateways to remote servers for processing and analysis.

The primary objectives of the proposed work are to reduce energy consumption and enhance security within the IoT network model. To ensure continuous data transmission between devices, the strategy minimizes battery usage while safeguarding transmitted messages from potential eavesdroppers. Figure 1 illustrates the identity authentication model for IoT devices, where authentication begins with IoT terminal devices. Each device is assigned a unique identifier, and the authentication process is managed by an Authentication Server (IAS). The IAS verifies the device's identity, registers the terminal devices within the network, and assigns identity keys based on the specific identifiers of the devices. The IAS securely transmits these identity keys to the devices and gateways. In response to registration requests from terminal devices, the IAS sends the registration results and authentication messages back to the devices. A mutual authentication process takes place when an IoT device wishes to send data to an IoT gateway, ensuring secure communication between devices and the gateway, with both parties authenticated by the IAS.

The main contributions of the proposed work are as follows

• A registration phase is proposed for resource-constrained IoT devices. These devices are registered with a remote server directly to save undue processing time and delay. Additionally, the registration phase ensures green communication by preserving the resources of smart devices.

• We propose an authentication phase that is substantially lighter than the existing methods and uses fewer hash codes and Exclusive OR (XOR) operations. This phase ensures that reliable sessions are set up between the communication devices, such as IoT devices, gateways, and a distant server.

• The proposed identity authentication process is lightweight yet incredibly strong. The security of transmitted data is preserved using pseudo-random numbers. Also, the ESIA scheme enhances the security of IoT devices by removing the need for third-party authentication.

• The proposed scheme increases the network's lifespan while conserving the device's energy. Additionally, the network latency between communicating entities is decreased using lightweight cryptographic primitives.

The remainder of the paper is organized as follows. Related work is discussed in section 2. Section 3 presents the proposed Energy-efficient and Secure Identity

Authentication Scheme for IoT Networks. Section 4 provides the performance analysis of the proposed work against various attacks. The implementation and results are covered in Section 5. Finally, the conclusion is presented in Section 6.

## 2. Related Work

To minimize energy consumption while ensuring data privacy and integrity, various schemes have been proposed in the literature. For example, in[1], the Advanced Encryption Standard (AES) is employed within a protean authentication technique to encrypt data and establish a secure connection between IoT gateways and end devices. The AES is a block cypher and symmetric encryption technique. The data is encrypted and decrypted using the same key. The secret encryption key must be used and known by both the sender and the recipient. This distinguishes AES from asymmetric algorithms, which encrypt and decrypt data using separate keys. With a block cypher, AES divides a message into fragments and encrypts each unit to transform the plaintext message into ciphertext, which is an incomprehensible format. This mechanism allows for secure key generation and sharing between devices in resource-constrained IoT networks, preventing device cloning and message replay attacks. Although effective, this method does not address the challenge of scalability in highly dynamic IoT environments. Further advancements in IoT security have been explored by integrating physical unclonable functions with cryptographic techniques. In[2], a unique device identifier combining a Combined Public Key (CPK) and a physical unclonable function (PUF) is used to enhance IoT device verification. This dual verification process between power-constrained IoT end devices and servers improves security. However, the CPK-based identification method does not offer anti-collusion attack protection, which can be a significant vulnerability in IoT networks.

Energy efficiency in IoT systems is another critical area of research. In[3], a heterogeneous IoT system supported by Unmanned Aerial Vehicles (UAVs) is introduced, where macro-cells and energy-harvesting IoT transmitters (IoT-Ts) are used to optimize energy efficiency. The approach considers one-slot and two-slot charging based on device position in three-dimensional space. By optimizing the density of IoT-Ts, the system enhances overall energy efficiency, although this solution may be limited by the practical challenges of UAV deployment in real-world environments. Another method to enhance energy efficiency is proposed in[4], where a joint optimization problem is formulated to allocate power in IoT systems. This joint energy-efficient iterative approach ensures guaranteed convergence and low computational costs. However, the use of successive convex approximation and Lagrangian dual decomposition methods makes this scheme complex and costly to implement, limiting its practicality in resource-constrained environments.

In[5], a cognitive energy management strategy is introduced, which integrates offloading and computational states to optimize energy usage. By utilizing state learning, the technique adjusts processing times based on the current load and available energy, aiming to prevent energy saturation. Despite its potential, this strategy suffers from poor cognitive management due to missing characteristics and non-linear switching, which could lead to inefficiencies in real-time operation. Security and energy efficiency are also closely linked, as evidenced by the approach presented in[6], which uses node weight to determine attack paths in IoT networks. This method allows for early detection of threats and security status evaluation through hierarchical analysis. However, this technique relies on stream sensing, which can be prone to delays and may not provide real-time protection against sophisticated attacks. The integration of blockchain technology has also been explored to enhance security in IoT systems. In[7], an energy-efficient data aggregation mechanism is proposed that incorporates blockchain and edge computing. This combination ensures secure, on-demand services for IoT networks with minimal delay. While this approach provides strong security, it is vulnerable to attacks that target the data sent by cluster heads, which could include sensitive or unencrypted information.

In[8], LightIoT, a secure and fast communication method, is introduced for exchanging data in healthcare infrastructures. LightIoT operates in three stages: initiation, pairing, and authentication. Its use of lightweight hash values and XOR operations enables the quick transfer of time-sensitive data. However, the method's one-step certification process, performed offline, limits its ability to validate mobile wearable devices in real-time environments, which poses a challenge for dynamic IoT applications. Further advancements in IoT security and energy efficiency are explored in[9], where the author optimizes the allocation of computational and communication resources to improve both secrecy and energy efficiency in computation offloading. This optimization ensures that latency requirements for Machine Type Communication Devices (MTCDs) are met. The approach uses successive convex approximation and convex programming to derive a closed-form expression for power allocation. Although this method improves secrecy and energy efficiency, it relies on the Knapsack method to allocate computational resources, which may introduce complexity in resource allocation. In[10], the IoT Hardware Platform Security Advisor (IoT-HarPSecA) is proposed to address security requirements for IoT devices. It provides three main functionalities: security requirement elicitation, security best practice guidelines, and lightweight cryptographic algorithms (LWCAs). However, a key limitation of this framework is the lack of sufficient LWCAs for both software and hardware implementations, which could hinder its widespread adoption in resource-constrained IoT devices.

Another contribution in[11] addresses the challenge of user scheduling in IoT communications by combining various scheduling schemes, including optimal, threshold-based, and random scheduling. This technique aims to support energy-efficient and secure transmissions by calculating the secrecy outage probability and secure energy efficiency for each scheduling scheme. However, the proposed approach lacks a balanced trade-off between computational requirements and secrecy performance, which may limit its practical applicability in IoT systems. Energy efficiency and security are also critical in Wireless Body Area Networks (WBANs), as discussed in[12], where the author highlights the challenges of managing energy consumption in energy-constrained sensors while protecting sensitive patient health data. In[13], a certificateless algorithm based on a bilinear cryptosystem is used to enhance security in WBANs, offering improved computation security and sensor status evaluation through encryption techniques. Although effective in terms of security, this approach does not directly address the energy efficiency issues inherent in WBANs. The Energy-Efficient Multilevel Secure Routing (EEMSR) scheme, presented in[17], combines energy management, privacy, and the diversity of IoT devices. By using an analytic hierarchy process, EEMSR balances energy, node level, and algorithmic priorities to optimize routing efficiency. It also employs cipher feedback and cipher block chaining modes of operation to detect and prevent selective ciphertext attacks. While this approach offers strong security, its implementation of AES encryption for preventing attacks may be computationally intensive for resource-constrained devices.

In the context of WBANs, a simple key agreement and authentication method is proposed in[20] that utilizes lightweight hash functions and XOR operations during the authentication phase. This approach is efficient and ensures privacy, but it is vulnerable to sensor node acquisition attacks, which may compromise the system's overall security. The use of 6LoWPAN with routing protocols to address security concerns in low-power, lossy networks is discussed in[21], but it faces challenges in maintaining network performance while meeting memory requirements. Similarly, the approach outlined in[22] implements an Intrusion Detection System (IDS) on a 6LoWPAN network to detect attacks, but it struggles with scalability and real-time detection of security breaches. In[18], an encryption-based three-factor authentication system for wireless medical sensor networks is proposed, incorporating fuzzy techniques to manage biometric data. Although it improves security by addressing device loss attacks and ensuring forwarding privacy, it introduces additional complexity in terms of time and communication resource requirements.

Further, the Lightweight Anonymous Authentication Protocol (LAAP) described in[19] enhances security by using AES encryption for data transmission and observing routing attacks through an IDS. However, it faces challenges in terms of scalability and real-time response. A lightweight cryptography scheme, Edge-aided Searchable Public-key Encryption (ESPE), is introduced in[23], which allows IIoT devices to outsource some encryption tasks to external parties to conserve energy and storage. While this method improves power efficiency, it may expose the system to potential security risks from third-party involvement. In[24], AES encryption is used for end-to-end session protection in IoT networks, ensuring protection against attacks such as snooping and message manipulation. Similarly, a blockchain-based technique for ensuring data protection is discussed in[25], which guarantees data integrity by preventing attackers from altering or supplying fake data. While blockchain offers strong security, its efficiency depends on the hashing algorithm's performance, which can impact overall system throughput. Proposed Energy-efficient and Secure Identity Authentication Scheme for IoT Networks.

A hybrid cryptographic approach presented in[26] aims to enhance security in IoT and AI applications by addressing key distribution challenges and improving encryption efficiency. The study reviews hybrid techniques in WSNs, cloud computing, and intelligent banking. However, it lacks discussions on computational overhead, scalability, and real-world implementation challenges, highlighting a research gap in optimizing the security-performance trade-off. A lightweight authentication protocol introduced in[27] is designed for cloud-based IoT devices, utilizing ECDLP, hash functions, and XOR operations to enhance security. The protocol effectively reduces computational costs and resists various attacks, with validation performed using BAN logic and AVISPA. However, the study does not analyze scalability, real-time performance, or adaptability to dynamic IoT environments. A secure data transmission scheme proposed in[28] addresses black hole attacks in MANETs. It is based on the AOMDV protocol, K-Nearest Neighbor (KNN) node selection, and a False Key-Build AES (FAES) encryption scheme. This approach reduces energy consumption and EE-delay while increasing throughput, ensuring reliable communication despite the presence of malicious nodes. However, the research does not include testing on large-scale networks or real-time IoT applications.

A Hybrid Energy-Efficient (HEE) paradigm introduced in[29] for Mobile Cloud Computing (MCC) integrates Pheromone Termite (PT) and Cuckoo Search (CS) algorithms to improve energy efficiency, security, and throughput. It incorporates blockchain-enabled authentication and data-mining detection to prevent malicious attacks and is validated using CloudSim. However, the study lacks an analysis of time complexity and blockchain vulnerabilities in real-world scenarios. A multifactor authentication scheme proposed in[30] for IoT-enabled WSNs employs physically unclonable functions (PUFs) for efficient node authentication and adaptive session key updates for secure communication. This

scheme reduces computational and communication overhead while ensuring robust security. However, its evaluation in real-time applications, such as military or smart city environments, remains unaddressed. The

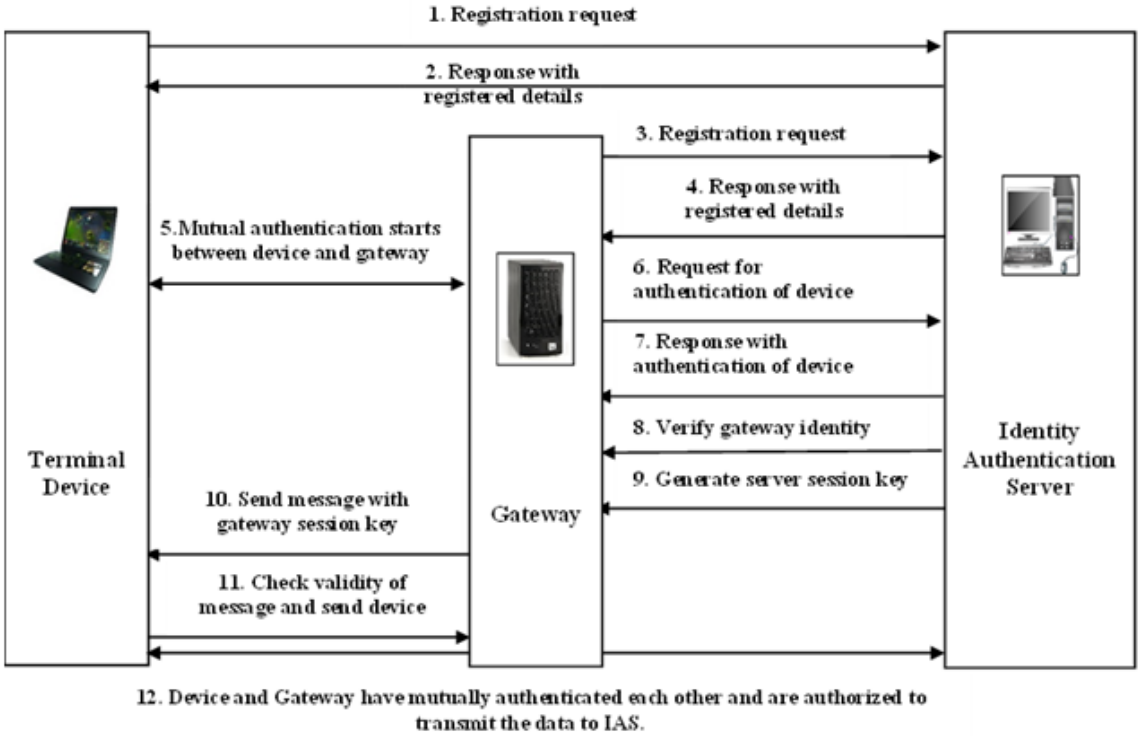


**Fig. 2:** Proposed IoT identity authentication scheme.

CLIENT model, introduced in[31] for energy-efficient and secure communication in IoT environments, incorporates five key mechanisms: Chaotic Map-based Elgamal authentication, credit score-based clustering, Capuchin search optimization routing, signature-based en-route filtering, and deep learning-based anomaly packet detection. Despite its potential, the study does not explore scalability and energy optimization in blockchain components in depth.

These studies collectively highlight the ongoing challenges in balancing energy efficiency with robust security mechanisms in IoT networks[14]. While various methods have been proposed to address energy and security concerns, many of them face limitations related to scalability, real-time application, or computational requirements[15,16]. The proposed Energy-efficient and Secure Identity Authentication (ESIA) scheme aims to overcome these limitations by offering a lightweight and robust solution that improves both energy efficiency and security in IoT networks.

### 3.1 Network Model

The network model of the proposed scheme is shown in Fig. 2 which consists of N IoT terminal devices represented by $D_1$, $D_2$, $D_2$..$D_N$, one server IAS represented by S and one IoT gateway represented by G. Each terminal device and gateway are first assigned a primary key by the IAS to maintain the security of the proposed network. Each terminal device and gateway are authenticated by using a number of hash codes and Exclusive OR (XOR) operations to make the network free from the attack. Three phase procedure is used to ensures that reliable sessions are set up between the communication devices, such as terminal devices, gateway, and IAS. Figure 2 shows the sequence of the proposed IoT identity authentication scheme which consists of twelve steps as given below:

**Step 1:** In the first step, each terminal device sends registration request to IAS.

**Step 2:** In the second step, the IAS sends reply to device with device registered details.

**Step 3:** In this step, the gateway sends registration request to IAS.

**Step 4:** In the fourth step, the IAS sends reply to gateway with gateway registered details.

**Step 5:** After getting registered details or keys, mutual authentication between device and gateway starts.

**Step 6:** During mutual authentication, gateway sends an identity authentication request for device to IAS.

**Step 7:** In response of step 6, the IAS verifies the device identity.

**Step 8:** The IAS also verifies the gateway's identity.

**Step 9:** The IAS generates the server's session key and send the key to verified gateway.

**Step 10:** The gateway sends the message with gateway's session key to the corresponding IoT device.

**Step 11:** In response of step 8, the device checks the validity of message and send device's session key to the corresponding gateway.

**Step 12:** Finally, device and gateway are mutually authenticated and authorized to transmit data to IAS.

By imitating the identities of users and gateways, an attacker can access the network's infrastructure to introduce a variety of challenges. It might also replicate itself in order to have a significant hostile impact on the system as a whole. We propose a strong, lightweight, reliable, and privacy-preserved method for important data in order to stop such attacks. The ESIA is able to prevent a variety of potential attacks

### 3.1.1 Replay attack

An attacker has the ability to replay a sequence of data that have already been sent to users.

### 3.1.2 Forgery attack

One or more of the network objects could be the target of a forgery attempt by an opponent. It might take control of the messages that are transmitted, alter them, and pretend to be these trustworthy organizations.

### 3.1.3 De-synchronization attack

This attack can be initiated by a hostile party who stops messages between the communicating parties in order to modify the order of messages.

### 3.1.4 Key compromise during mutual authentication and key agreement

An attacker can start this attack by stealing or faking the shared session keys.

### 3.2 Working procedure of proposed ESIA scheme

The proposed ESIA scheme utilizes the given algorithm.

### 3.2.1 ESIA Algorithm

1) Device $D_i$ send registration details to IAS
2) IAS store and send ($ID_i$, KDi , $PID_i$) to device $D_i$
3) Gateway G send registration details to IAS
4) IAS store and send ($ID_S$, $K_S$, $PID_S$) to gateway
5) Device $D_i$ chose random number $r_D$ , time stamp $t_{d1}$
6) Device $D_i$ Compute $H_1$ = hash ($PID_i$ ||$r_D$|| $KD_i$) and $Message_1$= ($ID_i$,$r_D$, $t_{d1}$, $H_1$)
7) Device $D_i$ Send ($Message_1 \oplus PID_i$ ) to IAS
8) IAS Check if ($|t_S - t_{d1}| < \blacktriangle T$ )
9) Compute $H_1$'= hash ($PID_i$ ||$r_D$|| $KD_i$)
10) Check if ($H_1$= =$H_1$')
11) Compute D_new_$ID_i$ = hash (IDi || $r_D$ || $t_{d1}$ || $t_S$ ) and $H_2$ ← hash (D_new IDi ⊕ $ID_G$)
12) IAS send ($Message_2$ = $H_2$ , ts) to device
13) Device $D_i$ check if ($| t_{d2} - ts | < \blacktriangle T$ )
14) Compute PID_i ← D_new ID_i ← hash ($ID_i$ ||$r_D$ ||$t_{d1}$ ||ts) and $ID_G$ ← H2 ⊕ hash (D_new $ID_i$ || ts)
15) Device $D_i$ chose random number $R_D$, time stamp $T_{d1}$
16) Compute A1 = hash ($ID_i$ ||$KD_i$ ||$R_D$) and $Message_3$ = ($A_1$, $R_D$, $T_{d1}$, $PID_i$ )
17) Device $D_i$ Send ($Message_3 \oplus ID_G$ ) to gateway
18) Gateway Check if ($|T_{g1} - T_{d1}| < \blacktriangle T$)
19) Compute $A_2$ = hash ($ID_G$ || $K_G$ || $R_g$) and $Message_4$ = $A_2$, $A_2$, $PID_i$, $T_{g1}$
20) Gateway send ($Message_4 \oplus PID_G$ ) to IAS
21) IAS check if ($|T_S - T_{g1}| < \blacktriangle T$)
22) Compute $A_1$' = hash ($ID_i$ ||$KD_i$ ||$R_D$)
23) Compare if ($A_1$ == $A_1$')
24) Device is legitimate
25) Compute A2' = hash ($ID_G$ || $K_G$ || $R_g$)
26) Compare if ($A_2$ == $A_2$')
27) Gateway is legitimate
28) IAS Compute $K_{S1}$←hash ($ID_G$||$K_G$||$R_g$||$PID_G$||$T_S$)
29) Gateway check if ( $|T_S - T_{g2}| < \blacktriangle T$)
30) Compute $PID_G$ = hash ($ID_G$||$K_G$||$R_g$||$T_{g1}$||$T_S$) and $K_{S2}$ ← hash ($PID_i$ || $ID_G$||$R_D$||$R_g$
31) Compute $A_6$ ← h($K_G$||A3) and $Message_6$ = {$A_5$, $A_5$, $T_S$, $T_{g2}$}
32) Device $D_i$ check if ($|T_{d2} - T_{g2}| < \blacktriangle T$ )
33) Compute $PID_i$ new= hash ($ID_i$||$KD_i$|$R_D$||$T_{d1}$||$T_S$)
34) Check if ($PID_i$ New = = hash ($KD_i$ || A5 ))
35) Message is from authentic Gateway
36) Device compute $K_{S3}$ = hash ($PID_G$||$ID_i$||$R_D$||$R_g$) and A'$_6$= hash ($PID_i$||$ID_G$||$R_D$||$R_g$||$A_3$)
37) Device $D_i$ Checks if ($A_6$ == A'$_6$)
38) $K_{S3}$ is valid
39) Device $D_i$ start communication with Gateway

The proposed ESIA scheme uses a three-step procedure to make a secure connection. These steps are given below:

### 3.2.2 Initialization

The IAS conducts the following actions during the initialization phase: The IAS sends and saves data $KD_i$ and $PID_i$ for a specific device $D_i$ in its database as ($KD_i$, $PID_i$). There is a tuple ($ID_i$,$KD_i$, $PID_i$) for each Di. It also assigns and saves data $K_G$ and $PID_G$ for the gateway in its database as ($K_G$, $PID_G$). The information about gateway is stored in the form of a tuple ($ID_G$,$K_G$, $PID_G$).

### 3.2.3 Pairing

Each device has to register itself with the IAS to start secure communication in the network. As indicated in Equation 1, device $D_i$ chooses a random number $r_D$, selects the present time stamp td1, and computes the hash H1 by joining $PID_i$, $r_D$ and $KD_i$. At this instance, a message $Message_1$ = ($ID_i$, $r_D$, $t_{d1}$ ,$H_1$) is produced, XORed with $PID_i$, i.e. $Message_1 \oplus PID_i$, and transmitted to IAS.

$$H_1 = hash(PID_i \| r_D \| KD_i) \quad (1)$$

After receiving Message1, the IAS selects its present timestamp $t_S$ and determines whether $| t_S - t_{d1} | < \Delta T$. The pair-up attempt fails and Message1 is dropped if the time period exceeds the given acceptable ΔT; otherwise, further processing is carried out [8]. After $Message_1$ has been time-validated, the IAS utilises $PID_i$ to decrypt it in order to retrieve $ID_i$. The IAS verifies $ID_i$ in its record after

retrieval of $ID_i$. If it is discovered, it confirms that $D_i$ is a valid device. Further, the IAS looks for a tuple ($PID_i$,$KD_i$) in its own records and computes a hash function. The IAS compares the computed hash function to the $H_1$ obtained from $KD_i$. If the computed hash function by IAS and $H_1$ is same then it indicates that a valid device sent the registration or pairing request. At this stage, IAS generates the hash of $ID_i$, $r_D$, $t_{d1}$ and $t_S$ for $D_i$ and derives a new identity $D_{new}ID_i$ for Di as given in Equation 2. In this case, $D_{new}ID_i$ acts as a fresh identity for $D_i$. The IAS creates a hash $H_2$ by encrypting $D_{new}ID_i$ with IDG as shown in Equation 3. Afterwards, IAS sends a message to $D_i$ with the format ($Message_2 = H_2, t_S$).

$$D_{new}ID_i = hash(ID_i \parallel r_D \parallel t_{d1} \parallel t_S) \quad (2)$$

$$H_2 = hash(D_{new}ID_i \oplus ID_G) \quad (3)$$

After receiving $Message_2$, $D_i$ retrieves its latest timestamp $t_{d2}$ and determines whether $| t_{d2} - t_S | < \Delta T$. The $Message_2$ is rejected if the time period exceeds the set acceptable $\Delta T$; else, additional processing is carried out. As demonstrated in Equation 4, when $Message_2$ has been validated, $D_i$ determines its new identity $D_{new}ID_i$ by creating a hash of $ID_i$, $r_D$, $t_{d1}$ , and $t_S$. At this time, $D_{new}ID_i$ acts as device $D_i$ new identity. It is important to note that the IAS had already created an identical new identity for $D_i$. Then, using Equation 5, device $D_i$ determines $ID_G$ from $H_2$, calculates $H'_2$ , and determines if $H'_2$ matches $H_2$. The current session request for joining is approved if a legitimate hash function is determined, and $D_i$ changes its new identity, i.e., $D_{new}ID_i$ gets the new $PID_i$. Figure 2 depicts the whole process of the pairing phase.

$$PID_i = D_{new}ID_i = hash(ID_i \parallel r_D \parallel t_{d1} \parallel t_S) \quad (4)$$

$$ID_G = (H_2) \oplus (hash(D_{new}ID_i \parallel t_S)) \quad (5)$$

**3.2.4 Authentication**

The device $D_i$, IAS and gateway take part in authentication process. A key to the session is produced for device and gateway to continue conversing with one another throughout this procedure, which involves mutual authentication. For the authentication process, subsequent procedures are carried out as follows

1. $D_i$ generates a random integer $R_D$, selects the present timestamp $T_{d1}$ , and creates a hash $A_1$ by combining $ID_i$, $KD_i$, and $R_D$ as indicated in Equation 6.

$$A_1 = hash(ID_i \parallel KD_i \parallel R_D) \quad (6)$$

This is followed by the creation of a message $Message_3 = A_1, R_D, T_{d1}$, and $PID_i$, followed by its XOR with $ID_G$, i.e., $Message_3 \oplus ID_G$, and its transmission to IAS as an identification request.

2.When gateway receives $Message_3$, gateway retrieves its present timestamp $T_{g1}$ and determines whether $|T_{g1} - T_{d1}| < \Delta T$. The Message3 is eliminated if this time period exceeds the stated acceptable $\Delta T$; else, execution continues. During this phase, gateway produces an arbitrary number $R_g$ and creates a hash $A_2$ by combining $ID_G$,$K_G$,$R_g$ as indicated in Equation 7. In order to send a message to IAS, that is encrypted as an identification inquiry, a message $Message_4 = A_1, A_2, PID_i, T_{g1}$ is produced. The content of this message is then XOR with $PID_G$, resulting in $Message_4 \oplus PID_G$.

$$A_2 = hash(ID_G \parallel K_G \parallel R_g) \quad (7)$$

3.After getting $Message_4$, IAS retrieves its latest timestamp TS and determines whether $| T_S - T_{g1} | < \Delta T$. $Message_4$ is eliminated if this time period exceeds the stated acceptable $\Delta T$, else additional processing is performed. Following the time validation of $Message_4$, IAS then verifies the accuracy of device and gateway in its record. The device and gateway have already been linked if it discovers the pair of tuples ($PID_i$, $KD_i$) for device $D_i$ and ($PID_G$, $K_G$) for gateway in its record set. The IAS regenerates the hash $A'_1$ and compares it to the hash $A_1$ that it obtained from the device. If IAS computed the identical hash, then $D_i$ is a verified device and permitted to continue the process. Likewise, IAS regenerates the hash $A'_2$ and compares it to the hash $A_2$ that it obtained from gateway. When both hash values are same, gateway is legitimate, and the procedure continues. In any case, the difference indicates that the request for information is sent through an unauthorized channel and can be dismissed.

4.The IAS determines a new-identity $New_{IDi}$ for $D_i$ by creating the hash of $ID_i$, $KD_i$, $R_D$, $T_{d1}$, and $T_S$ as indicated in Equation 8. This is done after device $D_i$ and gateway have been validated. $New_{IDi}$, also known as $PID_i$, acts as a new identity in this scenario.

$$PID_i = New_{IDi} = hash(ID_i \parallel KD_i \parallel R_D \parallel T_{d1} \parallel T_S) \quad (8)$$

5.As demonstrated in Equation 9, IAS additionally creates a new identity $New_{IDG}$ for gateway by creating the hash of $ID_G$, $K_G$, $R_g$, $T_{c1}$ and $T_S$. In this case, $New_{IDC}$ acts as a fresh identity for gateway.

$$PID_i = New_{IDi} = hash(ID_G \parallel K_G \parallel R_g \parallel T_{g1} \parallel T_S) \quad (9)$$

6.As indicated in Equation 10 to Equation 13, IAS creates a number of hashing codes and an encrypted session key for gateway called $K_{S1}$. Since gateway is the primary means of transmission for any data transfer across $D_i$ and IAS, $K_{S1}$ already includes safety primates designed for gateway. $ID_i$, $T_{d1}$ , and $T_S$ are concatenated to create the hash $A_3$. The combination of $K_{S1}$ ,$A_3$, and $PID_G$ results in the creation of the hash $A_4$. Finally, $A_3$ and $R_D$ are combined to create the hash $A_5$.

$$A_3 = hash(ID_i \parallel T_{d1} \parallel T_S) \quad (10)$$

$$K_{S1} = hash(ID_G \parallel K_G \parallel R_g \parallel PID_G \parallel T_S) \quad (11)$$

$$A4 = \text{hash}(K_{S1} \parallel A_3 \parallel PID_G) \quad (12)$$

$$A_5 = \text{hash}(A_3 \parallel R_D) \quad (13)$$

7.The IAS produces $\text{Message}_5 = T_S, A_3, A_4$ and $A_5$, and broadcasts it to the gateway. Since Equation 10 generates a variety of hashing codes, $\text{Message}_5$ is challenging for opponents to decrypt. Furthermore, such hash codes create $K_{S1}$ and the prediction of $K_{S1}$ in $\text{Message}_5$ is a challenging task. When gateway receives $\text{Message}_5$, gateway retrieves its most recent time stamp, $T_{g2}$ , and determines whether $|T_S - T_{g2}| < \Delta T$.

The $\text{Message}_5$ is eliminated if the time period exceeds the stated acceptable $\Delta T$; else, more computation is performed. As stated in Equation 14 to Equation 16, gateway determines its new identity $PID_G$ once $\text{Message}_5$ has been validated by creating a hash of $ID_G$, $K_G$, $R_g$, $T_{g1}$, and $T_S$. In this situation, $PID_G$ acts as gateway's new identity, much like the one created by IAS.

$$PID_G = \text{hash}(ID_G \parallel K_G \parallel R_g \parallel T_{g1} \parallel T_S) \quad (14)$$

$$K_{S2} = \text{hash}(PID_i \parallel ID_G \parallel R_D \parallel R_g) \quad (15)$$

$$A_6 = \text{hash}(K_{S2} \parallel A_3) \quad (16)$$

8.The gateway creates an encrypted session key $K_{S2}$ by concatenating $PID_i$, $ID_G$ ,$R_D$, and $R_g$ as shown in Equation 15. Finally, as illustrated in Equation 16, a hash $A_6$ is created by joining $K_{S2}$ and $A_3$. The gateway now produces the message $\text{Message}_6 = A_5, A_6, T_S, T_{g2}$ and XOR it with $PID_G$, making it $\text{Message}_6 \oplus PID_G$. The data is encrypted and transmitted to device $D_i$.

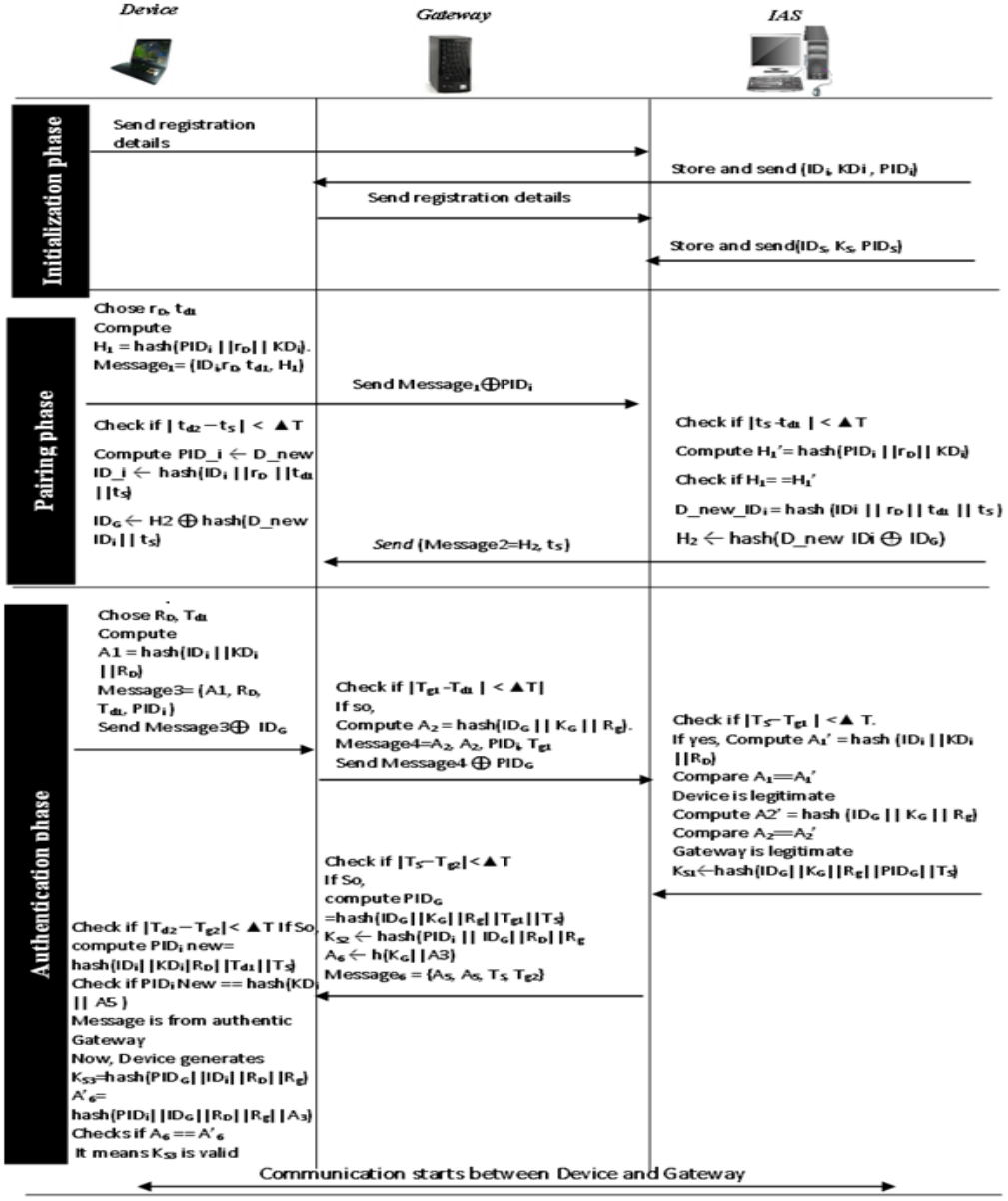


**Fig. 3:** The complete (initialization, pairing and authentication phases) communication procedure.

9.In order to determine whether $| T_{d2} - T_{g2} | < \Delta T$ after receiving $Message_6$, $D_i$ first selects its current time stamp $T_{d2}$. The $Message_6$ is eliminated if the time span exceeds the stated acceptable $\Delta T$; else, the procedure continues. Using the hash of $ID_i$, $KD_i$, $R_D$, $T_{d1}$ , and $T_S$, as indicated in Equation 17, $D_i$ determines its new identity $P_{New}ID_i$ after $Message_6$ has been validated. $P_{New}ID_i$ in this instance acts as a fresh identity for $D_i$. It is important to note that IAS previously produced an identical new identity for $D_i$.

$$P_{New}ID_i = hash(ID_i \| KD_i \| R_D \| T_{d1} \| T_S) \quad (17)$$

$$K_{S3} = hash(PID_G \| ID_i \| R_D \| R_g) \quad (18)$$

The hash $A_5$ is updated. The validity of $P_{New}ID_i$, i.e., $P_{New}ID_i = hash(KD_i \| A_5)$, indicates that gateway identification has been properly confirmed. At this point, $D_i$ constructs a session key $K_{S3}$ by concatenating $PID_G$, $ID_i$, $R_D$, and $R_g$ using a hash function, as depicted in Equation 18. $D_i$ reconstructs $A'_6$ which is determined as $hash(PID_i \| ID_G \| R_D \| R_g \| A_3)$ to verify the accuracy of $K_{S3}$ . $hash(K_{S2} \| A_3)$ can also be used to compute $A'_6$. If $A'_6$ is identical to $A_6$ obtained by gateway i.e., $A_6 = hash(K_{S3} \| T_{d1})$, which means $K_{S3}$ is valid. After completing this process, device $D_i$ and gateway are qualified to send the data to each other after successfully establishing their mutual authentication. Figure 3 depicts the whole communication procedure of initialization, pairing and authentication.

## 4. Performance analysis against various attacks

A preliminary study is done to verify the accuracy of the ESIA scheme, and the results reveal that ESIA is robust against a variety of hostile attacks. Identities and random numbers used in ESIA are 112 bits long, while timestamps are 28 bits long. The SHA3-224 hash function is applied to create a 224-bit long hash digest.

### 4.1 Replay attack

Device $D_i$, IAS and gateway include a timestamp in each communication to guard against replay attacks on the information being transmitted. The accuracy of each message can be verified using a timestamp. A message is rejected if it is sent outside of the permitted time frame. As shown in Step 2 and 3 in authentication phase the usage of unique timestamps by individual devices and gateway avoids the chances of replay attack. When gateway receives a message from device, gateway retrieves its present timestamp Tg1 and determines whether $|Tg1 - Td1| < \Delta T$. The Message is eliminated if this time period exceeds the stated acceptable $\Delta T$. Therefore, the usage of unique timestamp by devices and gateway refrain from replay attacks by ensuring that each communication is unique and cannot be reused by an attacker. During verification of gateway the IAS retrieves its latest timestamp TS and determines whether $| TS - Tg1 | < \Delta T$. The recent Message is eliminated if this time period exceeds the stated acceptable $\Delta T$. Therefore, the proposed system is resistant to replay attacks.

### 4.2 Forgery attack

A malicious party may deploy a forgery attack on every network object (clients, servers, and gateways). Following are the potential outcomes during a forgery attack on IAS and device.

• When an attacker attempts to produce a fake identity for IAS, the IAS must seize and control $Message_1$ and $Message_4$. The opponent provides IAS a valid $A_1$,$A_2$, $PID_i$ for $Message_4$. The attacker begins by employing $PID_G$ to retrieve the information ($A_1$,$A_2$, $PID_i$) as the $Message_4$ is protected by encryption ($Message_4 \oplus PID_G$). The attacker still needs $KD_i$ to break $A_1$ and $ID_G$ to unlock $A_2$ even if the attacker obtains $PID_G$. An attacker might even try to listen in and control $Message_1$ to harm the server with a counterfeit. Despite this, the attacker requires $PID_i$ to decrypt the data as the $Message_1 \oplus PID_i$ is secured. The opponent would still want $KD_i$ and $r_D$ to reproduce a legitimate $H_1$ regardless of whether it is already hacked. forgery attacks is quite challenging to conduct against IAS due to the usage of hashing techniques and encrypted keys.

• An attacker needs to seize and control $Message_2$ and $Message_6$ in order to prepare an attack on device $D_i$. A legitimate $H_2$ must be supplied to $D_i$ in order to create the $Message_2$. The opponent would need $PID_i$ of $D_i$ and the $ID_G$ of a gateway to access the network. The $Message_6$ and $PID_G$ are necessary to unlock the encrypted message even if an opponent cracks $Message_6$, the other party needs to first crack $A_5$ and $A_6$ in order to start an imitation attack on $D_i$. The hash codes $A_5$ and $A_6$ in the proposed method are the most durable and reliable as they combine encrypted keys with pseudorandom values. An opponent can not retrieve the keys on a variety of the latest and most advanced computing platforms as they are hashed. An opponent needs to be aware of these hash values, encrypted keys, and pseudo-random numbers in order to counterfeit $D_i$.

Table 1. Symbols and description.

| Symbol | Description |
|---|---|
| $D_i$ | IoT Device |
| *IAS* | Identity authentication server |
| *G* | IoT gateway |
| $ID_i$ | Identity of device |
| $PID_i$ | Pseudo-identity of device |
| $KD_i$ | Secret key of device |
| *IDG* | Identity of gateway |
| *PIDG* | Pseudo-identity of gateway |
| *KG* | Secret key of gateway |
| $t_{d1}$, $t_{d2}$ | Time stamps of device for pairing |
| $T_g$ | Time stamp of gateway for pairing |
| $r_D$ | Random number generated by device for pairing |

| | |
|---|---|
| $T_{d1}$ , $T_{d2}$ | Time stamps of device for authentication |
| $T_s$, $T_S$ | Time stamps of IAS for authentication |
| $\Delta T$ | Legal delay time interval |
| $R_D$ | Random number generated by Di for authentication |
| $R_g$ | Random number generated by gateway for authentication |
| $Message_1$,.. $Message_6$ | Encrypted messages |

### 4.3 Key compromise during mutual authentication and key agreement

Authentication between parties is ensured since no identity of any process can be falsified. To protect the data transferred during an entire session, everything is controlled by a special encrypted session key. For pairing, verification and authentication, many existing methods start with permanent keys and keep them throughout. Meanwhile, $D_i$ and gateway do not have permanent keys

in the proposed method. Since they are prohibited from knowing anything about one another prior to their first communication, the pairing phase is required for every fresh device $D_i$ and gateway.

### 4.4 De-synchronization attack

In the presence of latency within the network or attacker blocking, gateway carries on its activities using the recently acquired values. For the subsequent pairing if $Message_2$ is not obtained by $D_i$ within the pairing process due to network latency or delay by an opponent, then gateway might fail to get $Message_5$ during the authentication stage. In this case, gateway may even carry on with its activities using the most recent information for a subsequent session. The gateway can utilize the most recent $PID_i$ to finish the operation if $Message_6$ is not obtained by $D_i$ during the authentication step because of the communications latency or delay by an opponent. In Table 2, we have compared the proposed ESIA scheme with the CPK-based scheme [2] and LightIoT [8] in terms of their ability to resist various attacks.

As the number of devices increases, the communication traffic increases proportionally. The proposed ESIA scheme employs XOR operations and hash functions to complete all stages of encryption and authentication. To establish secure communication and data transfer between devices and the gateway, multiple messages are exchanged. Consequently, as the number of devices grows, the total number of messages exchanged among devices, the gateway, and the IAS also increases. Similarly, the overhead on the IAS rises because it must manage all devices in the network to initiate communication. Over time, with a large number of devices, a potential bottleneck may arise in the IAS due to the increased frequency of device registration and verification for the gateway. Therefore, the proposed scheme is best suited for small networks.

## 5. Implementation and results

In this section, we assess and validate our proposed ESIA scheme using experimental findings in a simulated environment.

### 5.1 Simulation model

The Contiki-based Cooja simulator is used for simulation to evaluate the implementation of proposed ESIA scheme. Contiki Operating System 3.0 is used to run the Cooja simulator. The memory requirement for Contiki 3.0 is 2 GB, with a 2.5 GHz processor. The simulator provided an option to choose the appropriate sort of mote. The proposed method is implemented over the RPL protocol. All the IoT devices are Tmote sky. IEEE 802.15.4 is used as a MAC layer protocol for the IoT network.

We have deployed 1 gateway, 1 IAS (remote server) and multiple devices (sensor nodes). At first, the network architecture is built by the scattered placement of sensors, gateway, and remote server. Figure 4 shows the simulation environment with total 40 nodes. Nodes 1 to 38 are the sensor nodes or IoT devices, node 39 represents the gateway, and node 40 represents the remote server or IAS. The performance of the proposed scheme is analysed in the presence of various attacks and the attacker nodes are represented by node 41 to node 44. To assess the effectiveness of the ESIA scheme, we raised the number of sensor devices, gateway, and a remote server in the operated region. As the number of devices increases, in the same ratio the communication traffic also increases. All the devices are distributed in a 400m× 400m region in in the simulation environment. The total simulation time is considered as 1800 seconds. In Table 3, all the desired settings and complete configuration of the cooja simulator are given for the proposed scheme.

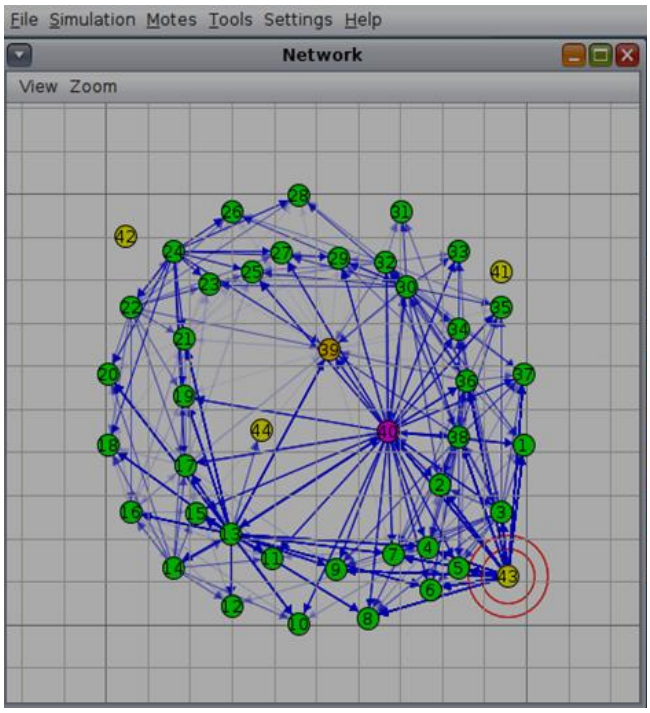


**Fig. 4:** Simulation environment with total 40 nodes: node 1 to 38 (sensor nodes or IoT devices), node 39 (gateway), node 40 (remote server or IAS), node 41 to 44 (attackers).

### 5.2 Performance matrix and result analysis

The performance of the proposed ESIA scheme is analyzed by considering six performance matrices: communication cost, computational overhead, energy consumption, packet loss rate, throughput and network latency. The results are compared with the Combined Public Key (CPK) based scheme[2)] and LightIoT[8)] to validate the performance of the proposed ESIA scheme.

In the proposed ESIA scheme the random numbers are generated using linear congruence method[32)]. The use of random numbers is beneficial to avoid many adverse conditions, as following

Table 2. Features comparison of proposed scheme with existing schemes.

| **Key Points** | **CPK-based scheme [2]** | **LightIoT [8]** | **Proposed ESIA** |
|---|---|---|---|
| Key generation | Generated consistently by the key management center depending on identity | Key is generated for the ongoing session after the clients and gateways mutually authenticate each other via the server | Generated consistently by the IAS using the identity of devices and gateway |
| Key storage | Takes up minimal space to store, kept centrally or distributed | The key is kept in an online database, it needs a lot of management and memory | Takes smaller space then both schemes and can be kept centrally or decentrally |
| Key distribution and management | Static distribution via a secure route, dynamic administration | Dynamic management combined with static distribution | Dynamic distribution via a secure route and dynamic control |
| Authentication method | Lightweight cryptography and physical unclonable function | Hash functions and Exclusive OR (XOR) operations | Lightweight hash codes and XOR computations |

- Since each session's login request is unique due to the random number's freshness, ESIA scheme ensures the legitimate user identity cannot be obtained.
- Every session has a unique set of random numbers that are used in the session key. Thus, the revealing of some session keys will not compromise the privacy of other session keys.
- It is evident from ESIA scheme that the session key only applies to the random numbers. The random numbers used in each session key are distinct from one another, even in the case that the secret keys are compromised.

The use of bitwise XOR operations and hash functions make the proposed approach significantly lightweight for the resource-constrained devices. The use of SHA3-224 hash function provide high security with low overhead. The key size is 224 bits, which is smaller than other SHA algorithms. Therefore, our proposed system provides the same level of security with smaller key size which reduces the computation overhead in resource constraints applications.

#### 5.2.1. Communication cost

The message with encryption ($Message_1 \oplus PID_i$) is sent by $D_i$ in ESIA. The length of $Message_1$ is 476 bits. The communication overhead incurred when IAS

transmits the message as $Message_2 = H_2$, $t_g$ is 288 bits. The information in the $Message_3$ has a length of 476 bits and is sent by $D_i$ as $Message_3 = (A_1, R_D, T_{d1}, PID_i)$ . On gateway, the secured ($Message_4 \oplus PID_G$) results in a 644 bit transmission cost. The highly complicated and efficient $Message_5 = (T_C, A_3, A_4, A_5)$ uses multiple hashing operations and has a 784 bit communication cost on IAS.

Table 3. Configuration of the Contiki Cooja simulator for the proposed ESIA scheme energy consumption during experiments.

| Parameters | Value |
|---|---|
| Operating System | Contiki Operating System 3.0 |
| Mote Type | Tmote Sky |
| Area | 400m × 400m |
| Nodes Layout | Random |
| Number of devices | 10 to 40 |
| Radio medium | Model Unit Disk Graph Medium(UDGM):Distance Loss |
| Communication range of IoT devices | 50m |
| Communication range of gateway | 200m |
| Number of gateway | 1 |
| MAC Layer | IEEE 802.15.4 |
| Duty Cycle | null RDC |
| Routing Protocol | Routing Protocol for Low-Power and Lossy Networks (RPL) |
| Objective Function | Minimum Rank with Hysteresis Objective Function |
| Host System | i3@2.53GHz 4GB Memory |
| Simulation time | 1800 seconds |

The secured ($Message_6 \oplus PID_G$) also adds 532 bits of transmission cost to gateway. In proposed ESIA scheme, network components will have a total communication cost of 3164 bits. Table 4 displays the communication costs endured by network components when transferring messages with their peers.

Table 4. Comparison of Communication cost

| Scheme name | No. of messages | Communication cost (in bits) |
|---|---|---|
| Proposed ESIA | 6 | 3164 |
| CPK-based scheme [2] | 5 | 3808 |
| LightIoT [8] | 6 | 3424 |

### 5.2.2. Computational overhead

The ESIA scheme utilizes robust hash functions with minimal computational overhead. The computational time required to complete

the hash and XOR operations at the device, gateway, and server is denoted by $C_h$ and $C_{XOR}$, respectively as denoted in Table 5.

In the CPK-based scheme, no computation is performed by the gateway; instead, the gateway immediately forwards the data to the server. Therefore, there is no computational overhead at the gateway in the CPK-based scheme, which is indicated as blank in the table. The computational overhead of the ESIA scheme is lower than that of LightIoT [8] because resource-constrained devices impose a relatively low computational burden, making the proposed ESIA a viable choice for implementation in various resource-constrained applications.

For the performance comparison Table 6 is used that represents the average value of energy consumption, PLR, throughput and network latency in the presence and absence of attacks. Here we have considered replay attack, forgery attack, key-compromise and de-synchronization attack while measuring the performance of proposed scheme with comparison to other schemes.

Table 5. Comparison of computational overhead.

| Schemes | Device | Gateway | Server | Total computational time |
|---|---|---|---|---|
| **CPK-based scheme [2]** | 10 $C_h$+ 2 $C_{XOR}$ | -- | 10 $C_h$+ 2 $C_{XOR}$ | 20 $C_h$ + 4 $C_{XOR}$ |
| **LightIoT [8]** | 5 $C_h$ + 2 $C_{XOR}$ | 4 $C_h$ + 2 $C_{XOR}$ | 8 $C_h$ + 1 $C_{XOR}$ | 17 $C_h$ + 5 $C_{XOR}$ |
| **Proposed ESIA** | 7 $C_h$ + 1 $C_{XOR}$ | 3 $C_h$ + 2 $C_{XOR}$ | 6 $C_h$ + 1 $C_{XOR}$ | 16 $C_h$ + 4 $C_{XOR}$ |

### 5.2.3. Energy consumption

The total energy consumption in proposed scheme is calculated using Equation 19 as given below

$$E = E_D + E_{IAS} + E_G \quad (19)$$

$E_{IAS}$ and $E_G$ indicate the energy needed by the IAS and gateway respectively, while $E_D$ reflects the total energy utilized by all devices. Milliwatts (mW) are used for calculating the network's total consumption of energy. We

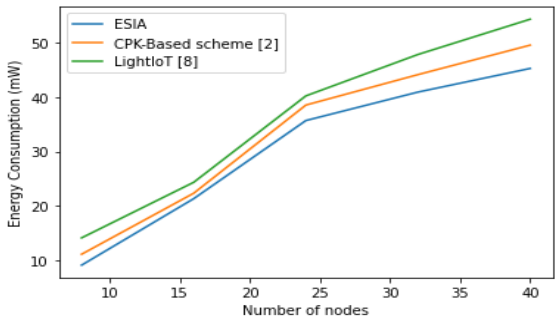


**Fig. 5:** Energy consumption with attack.

Table 6. Comparison of performance matrices of proposed ESIA with other schemes in the presence and absence of attacks.

| | With attack | | | | Without attack | | | |
|---|---|---|---|---|---|---|---|---|
| | **Average Energy Consumption** | **Average PLR** | **Average Throughput** | **Average Network Latency** | **Average Energy Consumption** | **Average PLR** | **Average Throughput** | **Average Network Latency** |
| **Proposed ESIA** | 30.4732 | .00175 | 24.983 | 0.42 | 28.4732 | .00164 | 25.76 | 0.4038 |
| **CPK-based scheme[2]** | 30.9537 | .00185 | 23.458 | 0.48 | 29.5348 | .00180 | 25.124 | 0.452 |
| **LightIoT [8]** | 38.1588 | .00195 | 21.730 | 0.45 | 32.9588 | .00179 | 24.06 | 0.416 |

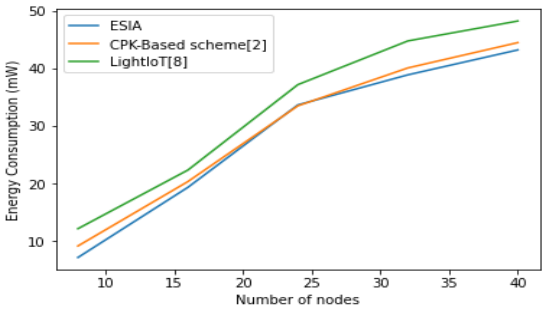


**Fig. 6:** Energy consumption without attack.

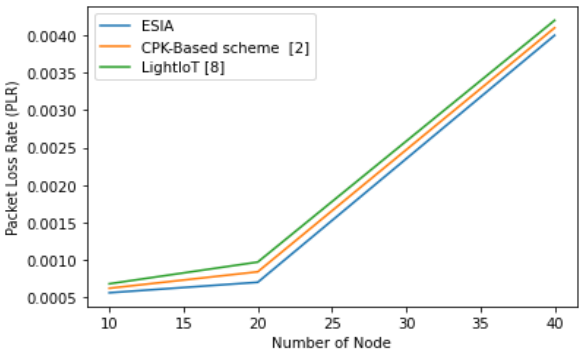


**Fig. 7:** Packet loss rate with attack.

considered that if a network node gets compromised by any adversary, the compromised node will use a greater amount of energy than usual for communication. Minimum usage of energy indicates the lack of or a small impact of a security breach or attack, whereas excessive usage of energy indicates a greater impact of an attack or a breach in security. Whenever a device gets targeted by an attacker, its energy usage rises. The authentication procedure of the ESIA scheme minimizes the consumption of energy during the initial interaction between the connected devices by using the smallest amount of data processing and communication. The ESIA scheme demonstrated improved outcomes of all participating device's. Figure 5 shows the outcomes of the ESIA scheme accompanied by current innovative approaches for overall energy consumption in the presence of attack. Figure 6 shows the energy consumption in the absence of attack. The proposed scheme indicates that energy consumption slightly increases in the presence of all considered attacks (replay attack, forgery attack, key-compromise and de-synchronization attack) compared to when there is no attack. This demonstrates that the attack's impact is minimal while using ESIA scheme.

### 5.2.4. Packet Loss Rate (PLR)

PLR is characterized as the depletion of packets during communication as a result of attacks. Attacks prevent some sent messages from being received, which makes it difficult to measure productivity.

For certain sources, the amount of data transferred is impacted by the packet loss rate. Since some networks view packet loss as a sign of bottleneck and adjust the communication rate to avoid jamming, therefore packet loss indirectly reduces efficiency. The PLR is calculated using Equation 20.

$$PLR = PKT_{loss}/T \quad (20)$$

Here PLR stands for packet loss rate, $PKT_{loss}$ indicates the total amount of lost packets, and T stands for the total time needed. As shown in Fig. 7, the PLR of ESIA is lower than the CPK-based scheme[2)] and LightIoT[8)]. For 10, 20 and 40 nodes, the PLR values of ESIA are 0.00056, 0.0007 and 0.0040 respectively. The value of PLR increases in the network as the number of IoT devices. It also increases the traffic rate which increases the value of PLR. The PLR of the proposed ESIA scheme is lower than the CPK-based scheme and LightIoT as here we have used lightweight hash codes and XOR computations. The PLR results in Figure 8 indicate that in the absence of the attack the value of PLR is a little bit smaller as compare to the presence of attack. Therefore, the impact of attack is minimal when using the ESIA scheme. Although the PLR value slightly increases in the presence of an attack with the ESIA

scheme, other schemes experience a greater impact, showing a more significant rise in PLR.

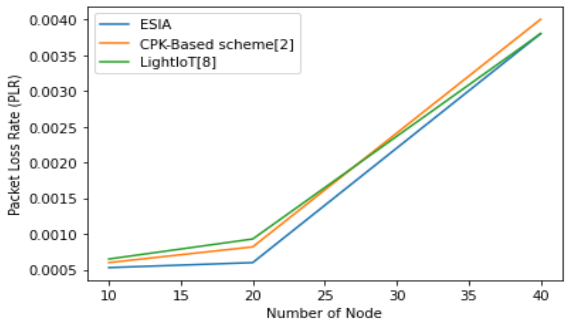


**Fig. 8:** Packet loss rate without attack.

### 5.2.5. Throughput

The system's throughput is the amount of data it can effectively access and process in a particular period of time. In most cases, throughput is computed in bits per second (bps) using Equation 21 as follows

$$\text{Throughput(bits/sec)} = P_{rcvd} * P_{length}/T \quad (21)$$

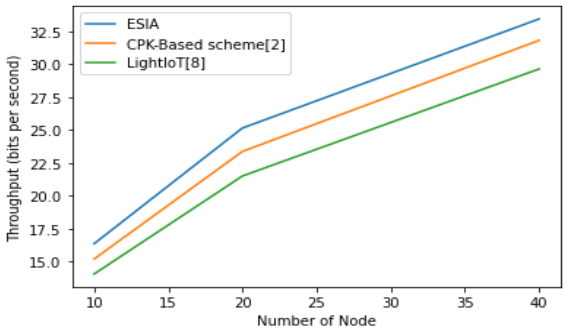


**Fig. 9:** Throughput with attack

Here $P_{rcvd}$ is the aggregate quantity of successfully received packets, $P_{length}$ denotes the length of each packet in bits, and T denotes the total amount of time needed to transfer the data. The implementation result in Fig. 9

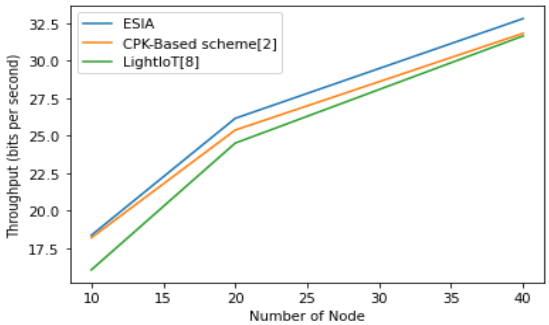


**Fig. 10:** Throughput without attack

represents the performance of the proposed ESIA scheme against the CPK-based scheme[2)] and LightIoT[8)] in terms of network throughput. Figure 9 depicts the throughput of ESIA and CPK-based scheme and LightIoT. The results show that the throughput of the ESIA scheme is better than the CPK-based scheme and LightIoT. The throughput for the different number of devices 10, 20 and 40 are 16.35, 25.15 and 33.45bps respectively. As the number of devices increases, the throughput also improves. Figure 10 illustrates the throughput in the absence of an attack, and the difference between the results suggests that the attack's impact is low when using the ESIA scheme compared to other schemes.

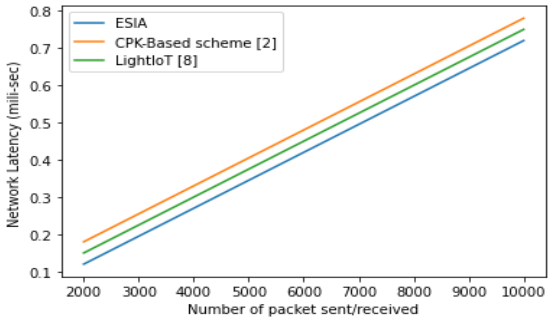


**Fig. 11:** Network latency with attack

### 5.2.6. Network latency

The delay caused during communication over networks is referred to as network latency. The effectiveness of any method in delay-sensitive IoT network applications relies on delay as greater delay in the connected network impairs its efficiency. The delay displays the duration of data transmitted via the network transmissions. Typically, low-latency networks are ones that respond quickly, whereas high-latency networks have a greater wait or latency. The network latency NL is defined using Equation 22 as the sum of propagation delay and serialization delay.

$$NL = P.D. + S.D. \quad (22)$$

$$P.D. = Distance/Speed \quad (23)$$

$$S.D. = P_{length} / T_{rates} \quad (24)$$

Here P.D. and S. D. are the propagation delay and serialization delay which are computed using Equation 23 and Equation 24 respectively. Here $P_{length}$ denotes the length of each packet in bits and $T_{rates}$ denotes the transmission rates in bits per second (bps).

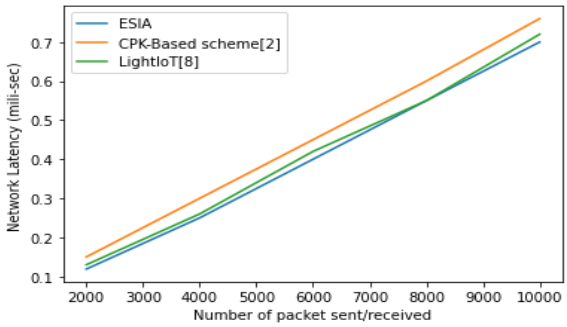


**Fig. 12:** Network latency without attack

The ESIA is efficient in terms of network latency because of its simple design and straightforward authentication method, and transmission. Figure 11 depicts the comparative analysis of network latency of the ESIA scheme with CPK-based scheme[2] and LightIoT[8]. For the various ratios of the number of packets sent over received, the latency values are 0.120, 0.27, 0.42, 0.57 and 0.72. By increasing the number of devices in the simulation scenario, we also saw a rise in traffic through the network. A consistent time period is visible across the whole interaction process for both sent messages and received messages. Figure 11 and 12, indicates that the difference in the presence and absence of attack is very less. Therefore, ESIA scheme approximately resolve the problem of attacks as compare to the CPK-based scheme and LightIoT.

## 6. Conclusion

This paper presents an energy-efficient and secure system designed for sustainable networking. The ESIA scheme, with its three-step process, facilitates basic identification and authentication for IoT devices with limited resources, enabling communication with a portable gateway and a distant server. The devices register with the server using a pair of messages, and the authentication process involves multiple messages to establish a secure session for data transmission. The ESIA scheme ensures timely transmission of delay-sensitive data by utilizing lightweight hash codes and XOR computations. Simulation results demonstrate the scheme's superior performance in terms of throughput, energy consumption, packet loss rate (PLR), and network latency, while maintaining robustness against various potential attacks.

### References


1) S. Sathyadevan, K. Achuthan, R. Doss & L. Pan, "Protean Authentication Scheme – A Time-Bound Dynamic KeyGen Authentication Technique for IoT Edge Nodes in Outdoor Deployments", *IEEE Access*, 7, 92419-92435 (2019). https://doi.org/ 10.1109/ACCESS.2019.2927818.
2) M. Zhang, J. Mao, Y. Ma, L. Xu & C.Wang , "A cpk-based identity authentication scheme for IoT", *Computer Systems Scienc e and Engineering*, 40(3), 1217-1231, (2020). https://doi.org/10.32604/csse.2022.017657.
3) Y. Yao, Z. Zhu, S. Huang, X. Yue, C. Pan & X. Li, "Energy Efficiency Characterization in Heterogeneous IoT System With UAV Swarms Based on Wireless Power Transfer", *IEEE Access*, 8, 967-979, (2020). https://doi.org/10.1109/ACCESS.2019.2961977.
4) J. A. Ansere, G. Han, L. Liu, Y. Peng & M. Kamal, "Optimal Resource Allocation in Energy-Efficient Internet-of-Things Networks With Imperfect CSI", *IEEE Internet of Things Journal,* 7(6), 5401-5411, (2020). https://doi.org/10.1109/JIOT.2020.2979169.
5) V.K. Kaliappan, A.B. Lalpet Ranganathan, S. Periasamy, P. Thirumalai, T.A. Nguyen, S. Jeon, D. Min & E. Choi, "Energy-Efficient Offloading Based on Efficient Cognitive Energy Management Scheme in Edge Computing Device with Energy Optimization", *Energies 15*, 8273, (2022). https://doi.org/10.3390/en15218273.
6) M. Yi, X. Xu & L. Xu, "An Intelligent Communication Warning Vulnerability Detection Algorithm Based on IoT Technology", *IEEE Access*, 7, 164803-164814, (2019). https://doi.org/10.1109/ACCESS.2019.2953075.
7) A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad & Z. Mushtaq, "An Energy-Efficient Data Aggregation Mechanism for IoT Secured by Blockchain", *IEEE Access*, 10, 11404-11419, (2022). https://doi.org/10.1109/ACCESS.2022.3146295.
8) M. A. Jan, F. Khan, S. Mastorakis, M. Adil, A. Akbar & N. Stergiou, "LightIoT: Lightweight and Secure Communication for Energy-Efficient IoT in Health Informatics", *IEEE Transactions on Green Communications and Networking*, 5(3), 1202-1211, (2021). https://doi.org/10.1109/tgcn.2021.3077318.
9) S. Han, "Energy Efficient Secure Computation Offloading in NOMA-Based mMTC Networks for IoT", *IEEE Internet of Things Journal*, 6(3), 5674-5690, (2019). https://doi.org/10.1155/2022/5230594
10) M. G. Samaila, J. B. F. Sequeiros, T. Sim˜oes, M. M. Freire & P. R. M. Inacio, "IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space", *IEEE Access*, 8, 16462-16494, (2020). r https://doi.org/10.1109/ACCESS.2020.2965925.
11) D. Chen, W. Yang, J. Hu, Y. Cai & X. Tang, "Energy-Efficient Secure Transmission Design for the Internet of Things With an Untrusted Relay", *IEEE Access*, 6, 11862-11870, (2018). https://doi.org/10.1109/ACCESS.2018.2805818.
12) Z. Kahleifeh & H. Thapliyal, "2-Phase Energy-Efficient Secure Positive Feedback Adiabatic Logic for CPAResistant IoT Devices", *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, *New Orleans, LA, USA*, 1-5, (2020). https://doi.org/10.1109/WF-IoT48130.2020.9221065.
13) N. V. Abiramy, G. Smilarubavathy, R. Nidhya & D. A. Kumar, "A Secure and Energy Efficient Resource Allocation Scheme for Wireless Body Area Network", *2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), India*, 729-732, (2018). https://doi.org/10.1109/I-SMAC.2018.8653789.
14) Y.Wang,W. Yang, X. Shang, J. Hu, Y. Huang & Y. Cai, "Energy-Efficient Secure Transmission forWireless Powered Internet of Things With Multiple Power Beacons", *IEEE Access*, 6, 75086-75098, (2019).

https://doi.org/10.1109/ACCESS.2018.2883143
15) R. Yadav & V. Passricha, "Energy Efficient Content Based Routing with Cluster Based Scheduling Mechanism", *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India*, 432-436, (2019). https://doi.org/10.1109/COMITCon.2019.8862223
16) A. Gouissem, K. Abualsaud, E. Yaacoub, T. Khattab & M. Guizani, "A Secure Energy Efficient Scheme for Cooperative IoT Networks", *IEEE Transactions on Communications*, 70(6), 3962-3976, (2022). https://doi.org/10.1109/tcomm.2022.3165887.
17) Y. Zhang, Q. Ren, K. Song, Y. Liu, T. Zhang & Y. Qian, "An Energy-Efficient Multilevel Secure Routing Protocol in IoT Networks", *IEEE Internet of Things Journal*, 9(13), 10539-10553, (2022). https://doi.org/10.1109/JIOT.2021.3121529.
18) X. Li, J. Peng, M. S. Obaidat, F. Wu, M. K. Khan, & C. Chen, "A Secure Three-Factor User Authentication Protocol With Forward Secrecy for Wireless Medical Sensor Network Systems", *IEEE Systems Journal,* 14(1), 39-50, (2020). https://doi.org/10.1109/JSYST.2019.2899580.
19) W. Mercy Kiruba, M. Vijayalakshmi, "Implementation and Analysis of Data Security in a Real Time IoT Based Healthcare Application", *2nd International Conference on Trends in Electronics and Informatics*, 1460-1465, (2018). https://doi.org/10.1109/ICOEI.2018.8553908.
20) X. Meng, J. Xu, X. Wu & Z. Wang, "Design of a Mutual Authentication and Key Agreement Protocol for WBANs", *Journal of Information Hiding and Privacy Protection*, 2(03), 107-114, (2020). https://doi.org/10.32604/jihpp.2020.09901.
21) A. Yeole, D.R. Kalbande & A. Sharma, "Security of 6LoWPAN IoT Networks in Hospitals for Medical Data Exchange", *Procedia Computer Science*, 152, 212-22, (2019). https://doi.org/10.1016/j.procs.2019.05.045.
22) R. Darwin ,"Implementation of Advanced IDS in Contiki for Highly Secured Wireless Sensor Network", *International Journal of Applied Engineering Research*, 13(6), 4214-4218, (2018). https://www.ripublication.com/ijaer18/ijaerv13n6_144.pdf (Accessed: March 5, 2025).
23) W. Wang, P. Xu, D. Liu, L. T. Yang & Z. Yan, "Lightweighted Secure Searching Over Public-Key Ciphertexts for Edge-Cloud-Assisted Industrial IoT Devices", *IEEE Transactions on Industrial Informatics*, 16(6), 4221-4230, (2020). https://doi.org/10.1109/TII.2019.2950295.
24) Ramiz Salama, Sinem Al-Turjman, Chadi Altrjman, Fadi M. Al-Turjman, Om Vikash, S. Yadav, Satvik Vats, "The Main Threat to Computer Network Security in Smart Cities," 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), 419-425, (2023).
25) Rani, P., Verma, S., Yadav, S. P., Rai, B. K., Naruka, M. S., & Kumar, "Simulation of the Lightweight Blockchain Technique Based on Privacy and Security for Healthcare Data for the Cloud System", IGI Global. https://doi.org/10.4018/IJEHMC.309436.
26) M. S. Sumathi, V. Jain, G. K. Kumar, & Z. Z. Khan, "Using Artificial Intelligence (AI) and Internet of Things (IoT) for Improving Network Security by Hybrid Cryptography Approach", Evergreen, 10 (2), 1133-1139 (2023). https://doi.org/10.5109/6793674.
27) I. Alam, & M. Kumar, "A novel protocol for efficient authentication in cloud-based IoT devices", Multimedia Tools and Applications, 81(10), 13823-1384, (2022). https://doi.org/10.1007/s11042-022-11927-y.
28) P. Singh, M. Khari, & S. Vimal, "EESSMT: an energy efficient hybrid scheme for securing mobile ad hoc networks using IoT", Wireless Personal Communications, 126(3), 2149-2173, (2022). https://doi.org/10.1007/s11277-021-08764-x.
29) A. Razaque, Y. Jararweh, B. Alotaibi, M. Alotaibi, & M. Almiani, "Hybrid energy-efficient algorithm for efficient internet of things deployment. Sustainable Computing: Informatics and Systems", 35, 100715, (2022). https://doi.org/10.1145/3386723.338788.
30) R. Kumar, S. Singh, & P. K. Singh, "A secure and efficient computation based multifactor authentication scheme for Intelligent IoT-enabled WSNs", Computers and Electrical Engineering, 105, 108495, (2023). https://doi.org/10.1016/j.compeleceng.2022.108495
31) S. Ramamoorthi, & A. Appathurai, "Energy aware Clustered blockchain data for IoT: An end-to-end lightweight secure & Enroute filtering approach", Computer communications, 202, 166-182, (2023). https://doi.org/ 10.1016/j.comcom.2023.02.010.
32) A. Idaman, & R. Rosnelly, "Implementation of Linear Congruent Methods and Multiplication Random Numbers for Academic Potential Tests", International Journal of Research in Vocational Studies (IJRVOCAS), 2(4), 32-41, (2023). https://doi.org/10.53893/ijrvocas.v2i4.160.