Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.047117

ARTICLE

Enabling Efficient Data Transmission in Wireless Sensor Networks-Based IoT Applications

Ibraheem Al-Hejri[1], Farag Azzedin[1,*], Sultan Almuhammadi[1] and Naeem Firdous Syed[2]

[1]Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Dhahran, 31261, Saudi Arabia

[2]Center for Cyber Resilience and Trust (CREST), Deakin University, Geelong, 3220, Australia

*Corresponding Author: Farag Azzedin. Email: fazzedin@kfupm.edu.sa

Received: 25 October 2023 Accepted: 06 December 2023 Published: 20 June 2024

ABSTRACT

The use of the Internet of Things (IoT) is expanding at an unprecedented scale in many critical applications due to the ability to interconnect and utilize a plethora of wide range of devices. In critical infrastructure domains like oil and gas supply, intelligent transportation, power grids, and autonomous agriculture, it is essential to guarantee the confidentiality, integrity, and authenticity of data collected and exchanged. However, the limited resources coupled with the heterogeneity of IoT devices make it inefficient or sometimes infeasible to achieve secure data transmission using traditional cryptographic techniques. Consequently, designing a lightweight secure data transmission scheme is becoming essential. In this article, we propose lightweight secure data transmission (LSDT) scheme for IoT environments. LSDT consists of three phases and utilizes an effective combination of symmetric keys and the Elliptic Curve Menezes-Qu-Vanstone asymmetric key agreement protocol. We design the simulation environment and experiments to evaluate the performance of the LSDT scheme in terms of communication and computation costs. Security and performance analysis indicates that the LSDT scheme is secure, suitable for IoT applications, and performs better in comparison to other related security schemes.

KEYWORDS

IoT; lightweight; computation complexity; communication overhead; cybersecurity threats; threat prevention; secure data transmission; Wireless Sensor Networks (WSNs); elliptic curve cryptography

1 Introduction

Critical infrastructures such as oil and gas supply, transportation networks, healthcare systems, and power grids face significant security challenges in today's interconnected world. One of the major concerns is the increasing sophistication and frequency of cyber attacks. These infrastructures heavily rely on computerized systems and interconnected networks, making them vulnerable to malicious actors seeking to disrupt operations, steal sensitive data, or cause physical damage [1,2]. In the oil and gas industry, for example, cyber attacks can disrupt the production and distribution of energy resources, leading to significant economic and environmental consequences [3,4]. Similarly, transportation networks are susceptible to cyber attacks that can compromise the safety and efficiency of public transportation systems or disrupt the flow of goods and services [5].

Meeting the resilience and reliability security requirements for these critical infrastructures is of paramount importance. A resilient and reliable infrastructure ensures the continuous operation of essential services, safeguards public safety and protects economic stability. It requires a multi-faceted approach that includes robust cybersecurity measures, regular vulnerability assessments, and proactive incident response strategies. By implementing stringent security protocols, such as access controls, encryption, and intrusion detection systems, critical infrastructures can strengthen their defenses against cyber threats [6].

Reducing the overhead and complexity of security defenses for critical infrastructures is crucial in effectively mitigating cyber threats. Simplifying security measures helps to streamline operations, improve efficiency, and enhance the overall effectiveness of defensive strategies. Complex security defenses can introduce unnecessary overhead, making it challenging to manage and maintain the infrastructure's security posture. This complexity often leads to an increased risk of misconfigurations, vulnerabilities, and human errors, which can be exploited by cyber attackers [7]. Moreover, reducing overhead and complexity allows for quicker response times in the event of a security incident [8,9]. Simplified security measures enable security teams to identify and respond to threats more efficiently, reducing the time required for analysis, investigation, and remediation. This agility is crucial in critical infrastructures where any delay in addressing a cyber threat can have severe consequences, such as prolonged downtime, financial losses, or compromised public safety [10]. Overall, by streamlining security defenses, critical infrastructures can enhance their resilience, reduce operational costs, and enable rapid response to cyber threats. A simplified and efficient security framework empowers organizations to focus on proactive threat intelligence, continuous monitoring, and timely incident response, thereby bolstering their ability to protect essential services and maintain the reliability and security of critical infrastructures [11].

The current trend in Internet of Things (IoT) security is towards providing lightweight and efficient schemes to secure data transmission. Ensuring the security of IoT applications is a challenge due to the incapability of a considerable proportion of resource-limited IoT devices to implement proper security schemes [12,13]. IoT devices encounter several distinct challenges that impact their overall security. These challenges include the limited computational power, memory, and energy resources of IoT devices, making it difficult to implement robust security measures on the devices themselves. Even though tremendous security defenses and countermeasures have been developed, these solutions cannot be applied directly to IoT infrastructures due to the major difference in computation and storage capabilities between conventional computing and IoT devices [14].

Data transmission schemes can play a crucial role in overcoming or mitigating these challenges faced by IoT devices [15]. By employing our proposed lightweight secure data transmission (LSDT) scheme, the confidentiality and integrity of data exchanged between IoT devices and other components can be ensured. LSDT scheme encrypts the data during transit, mitigating the risk of unauthorized access or tampering. Additionally, LSDT employs message authentication codes (MACs) which can be utilized to verify the integrity of transmitted data. Furthermore, due to its low communication and computation costs, the LSDT scheme reduces the energy expenditure of the network. This can alleviate the strain on limited network bandwidth and reduce transmission costs. By addressing these critical challenges and providing a lightweight and efficient solution, LSDT makes a significant contribution to the field of secure data transmission in IoT environments.

This paper focuses on securing data in transit, which is notably more susceptible to attacks when compared to other stages within the data life cycle [16]. Consequently, data must be kept protected from unauthorized access and other threats [17]. The transmitted data should not only be authentic

but also free from unauthorized modifications [13,18,19]. Without achieving confidentiality, integrity, and authentication; the transmitted data will be suspicious and may even bring undesired consequences [20]. Another challenge to protect data transmission is the diversity of communication channels, protocols, and techniques that may hinder the implementation of security solutions [21]. There has been growing attention on IoT data transmission security [12,13,19] and various schemes have been proposed to ensure data transmission secrecy [22–25]. Most of these schemes have focused on securing sensitive data transmission between IoT entities [26], by implementing countermeasures such as: (a) ensuring message integrity [23] and applying mutual authentication [23,24] and (b) mitigating attacks such as Man-In-The-Middle (MITM) [23–25], replay, and brute force [22,24,25]. Although a large proportion of the proposed schemes achieved most of the security requirements, the main drawback of these schemes is high computational and communication overhead [22–25]. This motivated us to propose a lightweight secure scheme that addresses these critical challenges related to secure data transmission in IoT environments. The contributions of this paper are as follows:

- Introducing a novel LSDT scheme. LSDT utilizes an efficient combination of symmetric keys and Elliptic Curve Menezes-Qu-Vanstone asymmetric key agreement protocol [27]. LSDT is lightweight (in terms of communication and computation costs) and provides secure data transmission that achieves confidentiality, integrity, and end-to-end mutual authentication. In addition, LSDT resists MITM, brute force, and replay attacks.
- Analyzing and adding communication and computation costs for LSDT and related security schemes.
- Demonstrating that LSDT excels in terms of security and outperforms other existing schemes in terms of communication and computation costs through comprehensive analysis and simulation experiments.

Our proposed LSDT scheme is versatile and can be applied across various industries within the IoT domains including e-healthcare systems, smart cities, and critical infrastructure systems like oil and gas supply, and power grids. The LSDT scheme addresses the crucial aspects of data security and authentication, which are integral to the seamless integration between IoT devices. Ensuring the security and integrity of data transmitted between IoT devices is of paramount importance in industries relying on IoT technology. By implementing the LSDT scheme, organizations across diverse sectors can enhance the protection of sensitive data, establish secure communication channels, and authenticate the devices connected to the IoT network. This scheme offers a robust and adaptable solution that can be tailored to meet the specific security requirements of different IoT industries, facilitating their successful integration and operation.

The rest of the article is organized as follows. For clarity and completeness purposes, Section 2 presents related work. The proposed scheme architecture and phases are described in Section 3. Section 4 discusses the performance and security analyses of the proposed scheme. Comparative analysis is presented in Section 5 while Section 7 concludes the article and envisions future directions.

2 Related Work

In recent years, there has been a growing interest in the development of secure authentication schemes for the IoT. This is because IoT devices are often connected to the internet and can be vulnerable to a variety of attacks. Dang et al. [28] proposed one of the recent secure authentication protocols which offers efficient energy consumption and direct communications between devices. This ECC-based scheme involves three phases: Registration, authentication between servers and IoT nodes, and authentication between two IoT nodes. Another recent authentication scheme for IoT is the one

proposed by Panda et al. [29]. This scheme consists of two phases: Registration and authentication, and it uses ECC to provide secure mutual authentication between IoT devices and cloud servers. The scheme is easy to implement and it can be used in a variety of IoT applications. Sowjanya et al. [30] introduced a lightweight protocol for end-to-end authentication based on ECC. This protocol is designed to overcome the security weaknesses (i.e., forward secrecy, key control) of an earlier scheme proposed by Li et al. [31]. The Sowjanya et al.'s protocol achieves much higher security standards in three well-defined phases, namely, initialization, registration, and authentication. The first phase entails the definition of the system's parameters. In the next phase, each user needs to register with the network manager to receive authentication parameters for the system. In the third phase, the user's credentials are verified by the application server before being granted access to medical services. Sowjanya et al.'s protocol focused on securing the communication between users and the application server using ECC. This advanced technique is employed to protect data transmission against cyber threats. The use of this technology coupled with the three-phase authentication process provides a robust framework for securing sensitive medical data.

In the realm of RFID security, Das et al. [32] developed a protocol for authentication that upholds the privacy of tags and enables mutual authentication of reader and tag. The approach involves using the public key of both components as their ID while keeping their private key concealed. The protocol is carried out in two phases. Firstly, during the setup phase, a one-time computation is carried out and stored for future use when tags are added or removed from the RFID system. Secondly, in the authentication phase, the reader and tag engage in on-demand communication. In a similar vein, Kalra et al. [25] developed an authentication scheme based on ECC and HTTP cookies to ensure the secrecy of IoT systems. However, it was discovered by Chang et al. [33] that there were two major issues with this method: Achieving mutual authentication and session key generation was considered impossible. In response, Chang et al. [33] proposed an improved technique that aimed to overcome the defects of Kalra et al.'s strategy [25]. Nevertheless, it was later revealed by Wang et al. [34] that the Chang et al.'s technique still lacked security, as an attacker could impersonate the server and establish a connection with a known device. Wang et al. [34] proposed a new method that addresses security risks in the IoT network, allowing for secure communication between known devices and a server. This approach enables devices to communicate with a server without compromising their privacy, ensuring that the IoT ecosystem remains secure. By utilizing these methods, security protocols can be enhanced to prevent malicious actors from compromising the security and privacy of the IoT environment.

To secure communication in IoT environments, several lightweight schemes have been proposed. One such scheme is the Secure Data Transmission Scheme (SDTS), proposed in [22]. This scheme consists of a base station, cluster heads, and members. SDTS is composed of four phases, including initialization, key generation, encryption, and decryption, and utilizes ECC to encrypt data transmitted between IoT nodes. It is resistant to brute force and replay attacks, although it has been identified as vulnerable to MITM attacks [35]. Additionally, it does not ensure authentication and integrity between cluster heads and cluster members [35]. The authors in [23] proposed another authentication scheme based on ECC and hash functions for IoT systems. In this scheme, users and sensors need first to authenticate themselves to the gateway before exchanging data with each other. This scheme is susceptible to brute force and replay attacks, and its high computation and communication costs make it inefficient for IoT environments [22].

Furthermore, a secure authentication scheme for cloud servers and IoT environments was presented in [24]. This scheme consists of initialization, registration, login, and authentication phases, with system parameters set by the cloud server and each device required to provide its ID and password for registration. The scheme is based on ECC and is designed to address security flaws in a previous

scheme [25]. However, major limitations include a lack of data integrity and high communication and computation costs [22]. A new key management scheme for IoT-enabled Wireless Sensor Networks (WSNs) was proposed in [36]. This scheme is designed to overcome the main security weakness of a previous scheme [37], which lacked mutual authentication and session key agreement. However, identity authentication requires a significant amount of energy [38]. In [39], authors introduced a novel hierarchical key management method designed to enhance the security and privacy of heterogeneous wireless sensor networks. This method addresses key generation, distribution, and maintenance while providing services such as message confidentiality, integrity, and authenticity. To bolster the confidentiality and security of the method, a main key is supplemented with three auxiliary keys, which collectively encrypt network information across three distinct levels. The proposed approach partitions the network into multiple areas overseen by area managers, which are nodes possessing greater processing power and memory capabilities. Additionally, a lightweight authentication process is implemented by these area managers. By adopting a hierarchical key management strategy, the proposed method offered notable advantages in terms of power consumption, efficiency, flexibility, and scalability.

The authors in [13] presented an enhanced security mechanism tailored specifically for WSNs. The proposed approach took into consideration factors such as the desired security level, application requirements, and the bit error rate of the network. To provide flexibility to the user, this approach utilized the reserved bits of the frame control field in the Zigbee MAC header, allowing them to choose between insecure or secure modes based on their specific needs. Furthermore, this study introduced a cross-layered interaction technique that enables the network to dynamically switch to alternative algorithms under specific circumstances, such as when the bit error rate reaches a certain threshold. This adaptive approach ensures that the network can employ the most suitable security measures based on real-time conditions and special criteria. In [40], authors proposed a three-phase method to address privacy and information security concerns in IoT systems. In the first phase, a unique key is shared between child and parent nodes to encrypt subsequent communications. The second phase involves the encryption of data with different keys during intra-cluster communications, with updating the keys at each connection to ensure security. The third phase incorporates an authentication protocol for inter-cluster communications to prevent malicious nodes from joining the network. This helps to protect the network from unauthorized access and data tampering. The authors showed that the proposed method significantly improved the performance of the network.

The authors in [2] introduced the innovative architecture called Blockchain Internet of Medical Things (BIoMT) to ensure secure data fusion processing for lung cancer workflows in fog cloud networks. The BIoMT architecture incorporates the Blockchain Data Fusion Secure scheme, comprising blockchain validation strategies and task scheduling. The primary objective of this study was to optimize the makespan of lung workflow tasks while adhering to stringent security and deadline constraints within cloud and fog networks. Notably, the authors had taken security measures to an advanced level by addressing runtime ransomware attacks that may occur in cloud and fog networks. By focusing on the advancement of digital healthcare systems in a pervasive environment, this study significantly contributed to the enhancement of healthcare services. Table 1 shows a summary of the existing works discussed in this section.

Several schemes have been proposed to ensure the secrecy of data transmission in IoT [22–25,28–32,40] as shown in Table 2. However, they suffer from various security weaknesses such as MITM [22,31,32], brute force [23,29–32,36,40] and lack of integrity [22,24,25] and mutual authentication [22,25]. Although some of the proposed schemes achieved various security requirements, their main drawback is high communication and computation costs [22,28–31,36,40]. This motivated us to

propose a scheme to fill these gaps. As such, our proposed scheme will have the following properties: (a) ensures confidentiality, integrity, and end-to-end mutual authentication, (b) resists MITM, brute force, and replay attacks, and (c) is lightweight in terms of communication and computation costs.

Table 1: Summary of related works

Ref.	Math. model	Simulation	Performance metrics
[22]	✓	×	Communication, computation costs
[23]	✓	×	Communication, computation, storage costs
[24]	✓	×	Communication, computation, storage costs
[25]	✓	×	Communication, computation, storage costs
[28]	✓	✓	Computation, storage costs
[29]	✓	✓	Communication, computation, storage costs
[30]	✓	×	Communication, computation, storage costs
[31]	✓	×	Computation cost
[32]	✓	✓	Communication, computation costs
[33]	×	×	–
[34]	✓	×	–
[36]	✓	×	Communication, computation, storage costs
[40]	×	✓	Computation cost

Table 2: Limitations of exiting lightweight schemes

Ref.	Limitations
[22]	Data integrity and mutual authentication are not achieved [35]. Subject to MITM attack [35].
[23]	Vulnerable to brute force and replay attacks [22]. High communication cost [22].
[24]	Data integrity is not achieved [22]. High communication and computation costs [22].
[25]	Data integrity and mutual authentication are not achieved [24]. High communication and computation costs [22].
[28]	High communication and computation costs [28].
[29]	High communication and computation costs [29].
[30]	High communication and computation costs [30].
[31]	Subject to MITM attack [31]. High communication cost [31].
[32]	Subject to MITM attack [32].
[36]	Performing identity authentication needs a significant amount of energy [38]. High computation cost [38,41].
[40]	High communication and computation costs [40].

3 Proposed Lightweight Secure Data Transmission Scheme

3.1 LSDT Architecture

WSNs are at the heart of IoT architectural implementation [42,43]. WSNs have played a pivotal role in the development of IoT technology which is proven to have a significant influence on the twenty-first century [44]. Because of their extensive usage in many vital and essential applications, WSNs have been regarded as one of the most important topics of study [36,45]. Despite WSN-based IoT applications having significant use cases in intelligent environments, their adoption is difficult due to energy constraints in sensor nodes. WSNs' principal design goal is to maximize energy efficiency which can be achieved by reducing the computation and communication costs [43,46]. The constrained resources available in WSNs also make implementing security solutions challenging, making them vulnerable to cybersecurity threats [47].

Due to these reasons, we are proposing an LSDT scheme for WSNs. The network architecture of the proposed LSDT scheme shown in Fig. 1 is composed of the base station (B) and the number of sensors. The B is assumed to be a reliable, secure, and powerful computing device. The sensors are grouped into clusters to reduce the total power consumption of the network. Each cluster is represented by a cluster head (H) and each sensor is referred to as a cluster member (M). The Ms gather sensed data and transmit it to Hs using one-hope communication. The Hs gather the sensed data collected by Ms and forward it to the B.

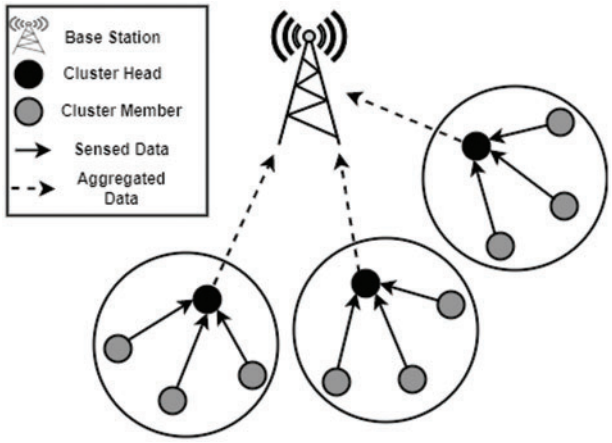

Figure 1: Network architecture

Each entity x in our architecture has a static public key, namely K_x^{su} and static private key, namely K_x^{sr}. Similarly, x has an ephemeral key pair, namely, (K_x^{eu}, K_x^{er}). In addition, two entities x and y can share a key represented as K_{xy}^{r}. The architecture uses $C(m)$ to represent the ciphered message m while $V(z)$ is the MAC function output. Table 3 lists the notations used in the proposed scheme.

Table 3: Proposed scheme notations

Notation	Description
p	Large prime number
$\mathbb{F}_p$	Prime field

(Continued)

Table 3 (continued)

Notation	Description
G, q	Basepoint G of prime order q
K_x^{su}	Node x static public key
K_x^{sr}	Node x static private key
K_x^{eu}	Node x ephemeral public key
K_x^{er}	Node x ephemeral private key
s_A	Implicit signature
K_{xy}^{r}	Shared key between node x and node y
K_{xy}^{p}	Pre-shared key between node x and node y
CK_{xy}^{r}	Ciphered shared key between node x and node y
C(m)	Ciphered exchanged messages m
V(z)	MAC function output
E(K, m)	Symmetric encryption of message m using key K
D(K, m)	Symmetric decryption of message m using key K

3.2 LSDT Overview

In our proposed LSDT scheme, we combine both symmetric and asymmetric protocols into one scheme to enhance performance and security as well as reduce the network's energy cost. We use symmetric key-based protocol to ensure authentication between B and Hs because of the following reasons: (a) symmetric key protocol consumes less energy [48,49], (b) although the communication cost is high in large networks [48,49], this communication cost is minimized since the number of Hs are much smaller than Ms, and (c) processing time is minimal in symmetric key protocols since there is no need to perform any complex computations [48,49]. This relieves Hs already overloaded with other tasks such as gathering and forwarding messages.

In addition, we use ECMQV, which is an asymmetric key protocol, to guarantee authentication between Hs and Ms for the following reasons. First, the ECMQV protocol is appropriate for a large number of sensors or when there is more than one-hope communication between Ms and B [48,49]. Second, the total amount of communication messages required for ECMQV is small [48,49]. Specifically, authors in [50,51] reported that ECMQV takes only two communication messages. Therefore, this improves the power consumption of the scheme. Finally, since ECMQV is lightweight [48,49], Ms are capable of performing ECMQV computation operations.

3.3 LSDT Phases

The proposed LSDT scheme consists of three phases: Initialization phase, key establishment phase, and data transmission phase as illustrated in Fig. 2.

3.3.1 Initialization Phase

In this phase, we assume that a pre-shared key K_{BH}^{p} is established securely. In addition, the B generates the scheme parameters including the elliptic curve $\mathbb{E}$ over $\mathbb{F}_p$, G, q, and publishes these parameters to Hs and Ms. The B also publishes the static private and public keys for both Ms and Hs as shown in Fig. 2. The public key, either static or ephemeral, is derived from its corresponding

private key as shown in Eq. (1).

$$K_x^{su} = K_x^{sr} * G. \tag{1}$$

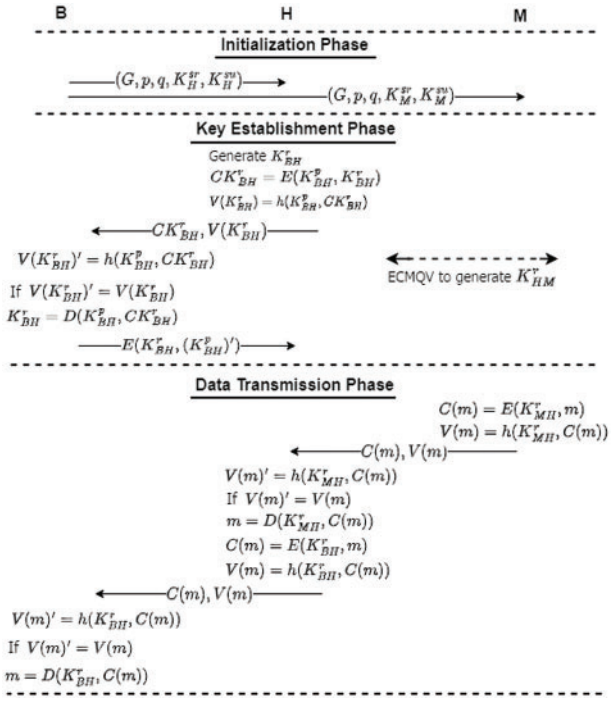

Figure 2: The operational flow diagram of LSDT

Each M and its H also exchange their static public keys. This is needed for generating the shared key between M and H using ECMQV protocol during the next phase as described in Section 3.3.2. It should be noted that the initialization phase is only done once which aims just to generate and set the scheme parameters. Hence, this phase is not included in the performance analysis of the scheme [22–24].

3.3.2 Key Establishment Phase between M and H

Three steps are established in this phase. In the first step, the M generates K_M^{er} and then calculates K_M^{eu}. Similarly, the H generate K_H^{er} and calculates K_H^{eu}. In the second step, both M and H exchange their ephemeral public keys. Finally, the M and H need to generate the implicit signature to calculate the shared key as shown in Algorithm 1.

Algorithm 1: ECMQV Key Derivation for CM

Input: $\mathbb{E}$, p, G, q. Private keys: K_M^{sr}, K_M^{er}. Public keys: K_H^{su}, K_H^{eu}
Output: Shared key $K_{MH}^r \in \mathbb{E}$ $(\mathbb{F}_p)$

1: $m \leftarrow \left\lceil \frac{(\log_2 q)}{2} \right\rceil$ ▷ [m is the half-bit length of q]
2: $u_A \leftarrow (u_x \bmod 2^m) + 2^m$ ▷ [u_x is the x-coordinate of K_M^{eu}]
3: $sA \leftarrow (K_M^{er} + uA \cdot K_M^{sr}) \bmod q$ ▷ [Implicit Signature]

(Continued)

Algorithm 1 (continued)

4: $v_A \leftarrow (v_x \bmod 2^m) + 2^m$ ▷ [v_x is the x-coordinate of K_H^{eu}]
5: $z_A \leftarrow s_A \cdot v_B \bmod q$
6: $K_{MH}^{r} \leftarrow MPM(sA \cdot K_H^{eu} + zA \cdot K_H^{su})$

It should be noted that two scalar multiplications and a point addition are needed for a straightforward implementation of the multiple point multiplication (MPM) operation (line 6 in Algorithm 1). However, Shamir's method [52] allows us to compute that with a cost close to one scalar multiplication as shown in Algorithm 2 and hence speeding up the computation process of the ECMQV protocol. This optimization is done by executing the elliptic scalar multiplication operations concurrently, especially with the pre-computed stage (line 1 in Algorithm 2). The identical bits of k and l are scanned from most significant to least significant bit. The intermediate value (line 2 in Algorithm 2), which is initially set to infinity, is doubled for each bit as shown in line 4 in Algorithm 2. If the location of the scanned bit is ($ki = 1, li = 0$), ($ki = 0, li = 1$), or ($ki = 1, li = 1$), then P, Q, or P + Q is added to the intermediate value, respectively, as shown in lines 5−13 in Algorithm 2.

Algorithm 2: Multiple Point Multiplication (MPM)

Input: $P = K_H^{eu}, Q = K_H^{su} \in \mathbb{E}\ (\mathbb{F}_p)$, two scalars: $k = s_A$, $l = z_A$
where $k = \sum_{i=0}^{m-1} 2^i k_i$, $l = \sum_{i=0}^{m-1} 2^i l_i$ and $k_i, l_i \in \{0, 1\}$
Output: $R = k \cdot P + l \cdot Q \in \mathbb{E}\ (\mathbb{F}_p)$
1: $Z \leftarrow P + Q$ ▷ [Pre-computation Stage]
2: $R \leftarrow O$ ▷ [Point Doubling]
3: **for** $i \leftarrow m - 1$ to 0 **do**
4: $R \leftarrow R + R$
5: **if** ($k_i = 1$) and ($l_i = 0$) **then**
6: $R \leftarrow R + P$
7: **end if**
8: **if** ($k_i = 0$) and ($l_i = 1$) **then**
9: $R \leftarrow R + Q$
10: **end if**
11: **if** ($k_i = 1$) and ($l_i = 1$) **then**
12: $R \leftarrow R + Z$
13: **end if**
14: **end for**
15: *return* R

3.3.3 Key Establishment Phase between B and H

The flow chart of this phase is illustrated in Fig. 3. Each H generates K_{BH}^{r} and encrypts it using K_{BH}^{p} which is established securely between the B and Hs during the initialization phase. H sends the encrypted shared key CK_{BH}^{r} along with $V(K_{BH}^{r})$ to B, where $V(K_{BH}^{r})$ is the output of hashing CK_{BH}^{r} with K_{BH}^{p} using the 256 hash function. Finally, H cancels K_{BH}^{p} and a new pre-shared key is generated for the next round of the protocol to enhance the security of the scheme.

When the B receives the data transmitted from H, the B calculates $(V\ (K_{BH}^{r}))'$ and verifies the matching between the recalculated hash function and the received one $V(K_{BH}^{r})$. If there is no matching,

it rejects the message. Otherwise, it decrypts CK^{r}_{BH} using K^{p}_{BH} to get $K^{r}_{BH}$and saves it as a shared key between B and H as shown in Fig. 3.

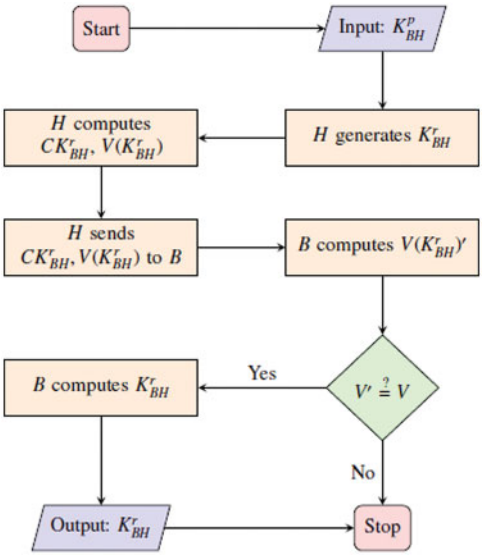

Figure 3: Key establishment (H-B) phase flow chart

Doing these steps guarantees establishing a shared key securely which only H and B have access to K^{r}_{BH} since it is encrypted by the pre-shared key which is known only to H and B. To verify the H, the H generates K^{r}_{BH} (as a nonce), encrypts it using K^{p}_{BH}, and sends the message (encrypted nonce) to the B. The B decrypts the message and hence authenticates H. To authenticate B to H, the B generates a new pre-shared key $(K^{p}_{BH})'$ to be used for the next round. The new pre-shared key is sent to H encrypted using K^{r}_{BH} which is known only to B and H. Therefore, $(K^{p}_{BH})'$ can be accessed only by H.

3.3.4 Data Transmission Phase

The flow chart of this phase is highlighted in Fig. 4. The data m sensed by the M is encrypted using K^{r}_{MH} which is shared between each M and its H. The M then sends the encrypted data $C(m)$ along with the resulting hash output $V(m)$ to the H, where $V(m)$ is the output of hashing $C(m)$ with K^{r}_{MH}. After receiving the encrypted message from its Ms, the H checks if the recalculated hash function $(V(m))'$ matches the received hash function $V(m)$. If there is a match, it decrypts $C(m)$ using K^{r}_{MH} to get m. After gathering the message from all Ms, the H aggregates and encrypts the sensed data using K^{r}_{BH}. Finally, the H sends the encrypted sensed data $C(m)$ along with $V(m)$ to the B. Upon receiving $C(m)$ and $V(m)$, the B verifies $(V(m))'$ and $V(m)$. If no match is found, the communication message is ignored. Otherwise, the B decrypts $C(m)$ using K^{r}_{BH} to get m as shown in Fig. 4.

4 Performance Analysis

In this section, we evaluate the performance of the proposed scheme in terms of communication cost, computation cost, and security services. To compare our work with existing schemes, our performance analysis utilizes 160-bit ECC [22–25,41,53], AES-128, and SHA-256 [13,54–56].

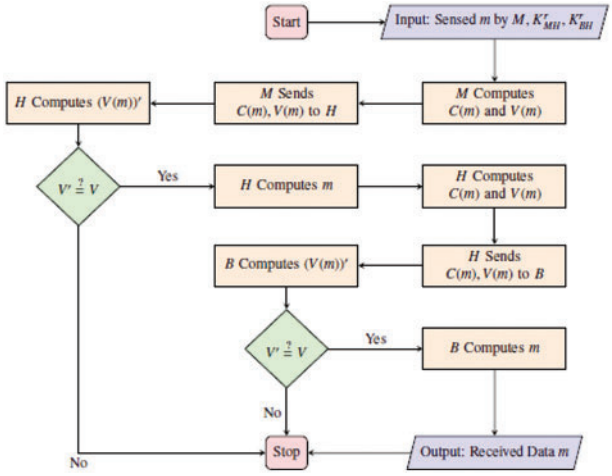

Figure 4: Data transmission phase flow chart

4.1 Communication Cost

The communication cost of the proposed scheme is equivalent to the total size of the scheme messages. To calculate the size of the transmitted messages during the scheme's phases, we use 160-bit ECC, where the ECC point $P = (x_P, y_P) \in E_p(a, b)$ is of size $(160 + 160) = 320$ bits. Furthermore, the sizes of the hash functions, random numbers, and symmetric encryption/decryption operations are also considered to be 160 bits. Therefore, the total communication cost (in bits) of the proposed scheme can be expressed as shown in Eq. (2), where n is the number of transmitted messages. It is worth mentioning that we consider the communication cost for M, H, and B for one data transmission.

$$\sum_{i=1}^{n} \text{Message}(i). \tag{2}$$

During the key establishment phase between M and H, the M sends its ephemeral public key K_M^{eu} which is 160 bits long to the H. The H also sends its ephemeral public key K_H^{eu} which is 160 bits long to the M. During the key establishment phase between H and B, the H sends the encrypted shared key CK_{BH}^{r} along with V (K_{BH}^{r}) to the B (i.e., the message size is $160 + 160 = 320$ bits). The B sends the encrypted new pre-shared key $(K_{BH}^{p})'$ which is 160 bits long to the H.

During the data transmission phase, the M sends the encrypted data $C(m)$ along with the resulting hash output $V(m)$ to the H (i.e., the message size is $160 + 160 = 320$ bits). After gathering the message from all Ms, the H sends its own $C(m)$ and $V(m)$ to B (i.e., the message size is $160 + 160 = 320$ bits). The total communication cost for one message transmission is $320 + 480 + 640 = 1440$ bits as shown in Table 4.

Table 4: LSDT communication cost

Scheme phase	No. of messages	Cost (bits)
Key establishment (M, H)	2	320
Key establishment (B, H)	2	480

(Continued)

Table 4 (continued)

Scheme phase	No. of messages	Cost (bits)
Data transmission	2	640
Total	6	1440

4.2 Computation Cost

Computation cost refers to the cost used to calculate the encryption and authentication operations of the scheme. The calculation method for computation cost involves a number of ECC point multiplications (T_m) and hash function operations (T_h) performed during the scheme's phases. As reported in the literature [22–25,40,41], the computation cost of inexpensive operations (i.e., concatenation, comparison, XOR) is ignored. These studies consider only T_m and T_h to calculate the computation cost. They also demonstrated that $T_m >> T_h$ which is shown by [40,57] to be 7.3529 ms for T_m and 0.0004 ms for T_h. It is noteworthy that the computation cost for M, H, and B is also computed for one data transmission.

During the key establishment phase between M and H, as shown in Algorithm 1, M calculates its ephemeral public key K_M^{eu} which takes one T_m. Then, M takes another T_m to calculate the shared key K_{MH}^{r}. Similarly, H calculates its ephemeral public key K_H^{eu}taking one T_m and another T_m [50] to calculate the shared key K_{MH}^{r}. During the key establishment phase between H and B, as demonstrated in Fig. 3, H calculates $V(K_{BH}^{r})$ taking one T_h. Similarly, B calculates $(V(K_{BH}^{r}))'$ taking also one T_h. During the data transmission phase, M calculates $V(m)$ (i.e., one T_h). After receiving the data from its CMs, the H recalculates $(V(m))'$ taking one T_h. After gathering the data from all CMs, H calculates $V(m)$ taking another T_h. Upon receiving the data, the B recalculates $(V(m))'$ taking one T_h. Therefore, the total computation cost for one data transmission is $4T_m + 6T_h$ as shown in Table 5.

Table 5: LSDT computation cost

Scheme phase	M	H	B	Total
Key estab. (M, H)	$2T_m$	$2T_m$	-	$4T_m$
Key estab. (B, H)	-	T_h	T_h	$2T_h$
Data transmission	T_h	$2T_h$	T_h	$4T_h$
Total	$2T_m + T_h$	$2T_m + 3T_h$	$2T_h$	$4T_m + 6T_h$

4.3 Simulation and Computational Time

The proposed scheme is implemented using Contiki OS version 3.0, and the performance evaluation is performed through the Cooja simulator which is one of the simulation tools targeted for IoT. Cooja is designed to provide a simulation for Contiki motes and permits to simulation of large and small networks [58]. Throughout our experiments, we employ the Cooja simulator to choose a suitable radio medium model, such as a Multi-path Raytracer Medium (MRM), Directed Graph Radio Medium (DGRM), or Unit Disk Graph Model (UDGM). Additionally, we select a specific mote type from the available options, including SKY mote, Wismote, or Z1. We then proceed to select a network topology, such as random positioning or a uniform 2D-Grid, followed by determining the

transmission range for the populated nodes. It should be noted that all Contiki default settings are used unless otherwise specified. To measure the computation cost, the rtimer library of Contiki is used [55].

For our experimental purposes, three clusters are organized, with each cluster consisting of one cluster head and three cluster members. The network topology is shown in Fig. 5 where nodes 1−6 are Ms, nodes 7 and 8 represent Hs and node 9 is B. The Skymote platform is used for our experiments and all Contiki default settings were used unless otherwise specified. To measure the computation cost, we used the rtimer library of Contiki [55].

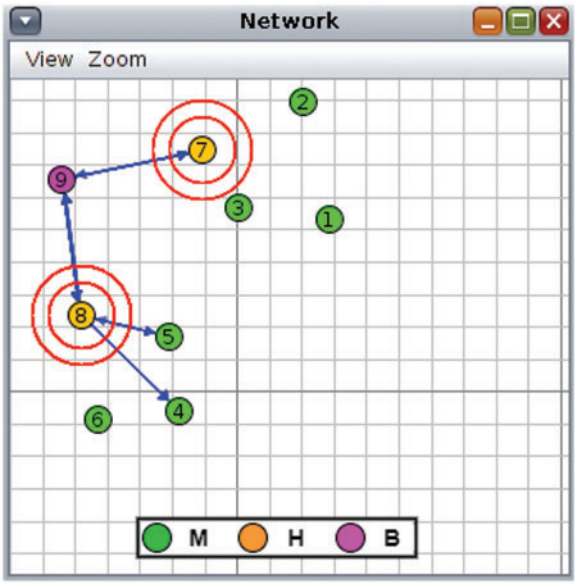

Figure 5: Network topology

In our experiments, the Skymote platform is used to evaluate the performance of the proposed scheme. Each ECC multiplication operation (T_m) takes 2.93 s, and the MAC hash function (T_h) operation takes 0.06 s. The total computation time for one data transmission is $4(2.93) + 6(0.06) = 12.1$ s as shown in Table 6. Please refer to Section 4.2.

Table 6: LSDT computational time

Scheme phase	M	H	B	Total
Key estab. (M, H)	5.86	5.86	–	11.72
Key estab. (B, H)	–	0.06	0.06	0.13
Data transmission	0.06	0.13	0.06	0.26
Total	5.92	6.05	0.13	12.1

4.4 Security Analysis

In this section, we state our security claims that are ensured by the proposed LSDT scheme and provide our justification for each claim.

- **Claim:** LSDT ensures confidentiality.

Justification: The data is encrypted using *160-bit ECC* and *AES-128*. Even if an attacker can crack the secret key and asymmetric key pair in one round, the attacker cannot benefit from those keys since new keys are generated every round.

- **Claim:** LSDT ensures integrity.

Justification: Since nodes send encrypted messages as well as hashed messages, the receiving nodes can check that the message has not been modified or altered by verifying the hashed message. It should be noted that the shared key (i.e., either K^{r}_{BH}, K^{r}_{MH}) is used for encryption and hashing. Please refer to Sections 3.3.3 and 3.3.4.

- **Claim:** LSDT ensures end-to-end mutual authentication.

Justification: As mentioned in Section 3.3.1, both H and B have K^{p}_{BH}. To verify the H, the H generates a nonce (i.e., K^{r}_{BH}), encrypts it using K^{p}_{BH}, and sends the message (encrypted nonce) to the B. The B decrypts the message and hence authenticates H. H can similarly authenticate B. Furthermore, and since LSDT utilizes ECMQV between H and its Ms, mutual authentication between H and its Ms is ensured since it is inherited from ECMQV [59,60].

- **Claim:** LSDT resists the MITM attack.

Justification: Any attempt to launch an MITM attack is thwarted because the LSDT scheme achieves end-to-end mutual authentication as described above.

- **Claim:** LSDT resists replay attacks.

Justification: During the key establishment phase between B and H, each message includes an encrypted nonce to disable any attempt to perform a replay attack. If the attacker re-transmits a message using the same encrypted nonce, the receiving node can detect the replayed message immediately since a new key is generated in each round.

- **Claim:** LSDT resists brute force attacks.

Justification: Since LSDT uses *160-bit ECC* and *AES-128*, LSDT resists brute force attacks. This property is inherited from *160 bits ECC* and *AES-128* [61]. The key spaces for searching for the keys in *160-bit ECC* and *AES-128* using brute force attacks are 2^{160} and 2^{128}, respectively [22]. In addition, the generated keys are used to encrypt/decrypt messages for only one round. As such, compromising the keys of one round does not affect the system security.

5 Comparative Analysis

Table 7 shows the comparison of existing security schemes in terms of security properties and their resistance to different attacks. Although other schemes violate some security properties and are vulnerable to some attacks, it is observed that LSDT ensures security properties and resists different attacks.

Furthermore, we analyze and provide a comprehensive breakdown of communication costs associated with the existing related schemes to investigate the cost distribution among their phases as shown in Table 8. Upon careful observation, we notice that our scheme exhibits comparable or lower communication costs during the key generation phase when compared to [23,29–31,36], and demonstrates competitive value in comparison to other schemes. We also notice that our scheme

incurs lower communication costs during the data transmission phase, which is executed more often compared to the key generation phase, outperforming other schemes in this regard.

Table 7: Security services comparison

Property	LSDT	[22]	[23]	[24]	[25]	[28]	[29]	[30]	[31]	[32]	[36]	[40]
Confidentiality	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Integrity	✓	×	✓	×	×	✓	✓	✓	✓	✓	✓	✓
Mutual authentication	✓	×	✓	✓	×	✓	✓	✓	✓	✓	✓	✓
MITM attack resistance	✓	×	✓	✓	✓	✓	✓	✓	×	×	✓	✓
Brute force attack resistance	✓	✓	×	✓	✓	✓	×	×	×	×	×	×
Replay attack resistance	✓	✓	×	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 8: Communication cost comparison

Scheme	Key gen.		Data trans.		Total	
	# Messages	# Bits	# Messages	# Bits	# Messages	# Bits
[22]	3	480	2	1280	5	1760
[23]	4	2080	4	3680	8	5760
[24]	2	640	3	1760	5	2400
[25]	3	480	2	1760	5	2240
[28]	–	–	–	–	–	–
[29]	2	800	3	1760	5	2560
[30]	2	1120	2	1440	4	2560
[31]	2	1120	2	960	4	2080
[32]	2	640	3	1120	5	1760
[36]	5	2400	3	2400	8	4800
[40]	–	–	–	–	–	–
LSDT	4	800	2	640	6	1440

We also conduct an in-depth investigation and offer a thorough analysis of computation cost associated with the existing related schemes, aiming to explore how costs are distributed across their stages, as illustrated in Table 9. We notice that our scheme demonstrates comparable or lower computation costs during the key generation phase when compared to [28,30,36]. Moreover, it showcases competitive value when compared to other schemes. Additionally, it is observed that our scheme incurs lower computation costs during the data transmission phase, which occurs more frequently than the key generation phase.

The obtained results, as illustrated in Figs. 6 and 7, provide compelling evidence of the superiority of the proposed LSDT scheme over other related schemes in terms of communication and computation costs, respectively. These findings highlight the effectiveness and efficiency of our approach compared to existing security schemes. In-depth analysis reveals that LSDT demonstrates notable advantages

in terms of resource utilization and computational complexity, making it a secure, lightweight, and efficient solution for IoT environments with limited resources.

Table 9: Computation cost comparison

Scheme	Computation cost		
	Key gen.	Data trans.	Total
[22]	$3T_m$	$2T_m + 2T_h$	$5T_m + 2T_h$
[23]	$25T_h$	$4T_m + 31T_h$	$4T_m + 56T_h$
[24]	$2T_m + 5T_h$	$8T_m + 7T_h$	$10T_m + 12T_h$
[25]	$2T_m + 3T_h$	$7T_m + 7T_h$	$9T_m + 10T_h$
[28]	$8T_m + 9T_h$	$7T_m + 9T_h$	$15T_m + 18T_h$
[29]	$3T_m + 4T_h$	$8T_m + 9T_h$	$11T_m + 13T_h$
[30]	$6T_m + 2T_h$	$9T_m + 4T_h$	$15T_m + 6T_h$
[31]	Tm	$5T_m + 5T_h$	$6T_m + 5T_h$
[32]	$2T_m$	$4T_m + 4T_h$	$6T_m + 4T_h$
[36]	$4T_m + 2T_h$	$7T_m$	$11T_m + 2T_h$
[40]	$2T_m + 3T_h$	$15T_m + 13T_h$	$17T_m + 16T_h$
LSDT	$4T_m + 2T_h$	$4T_h$	$4T_m + 6T_h$

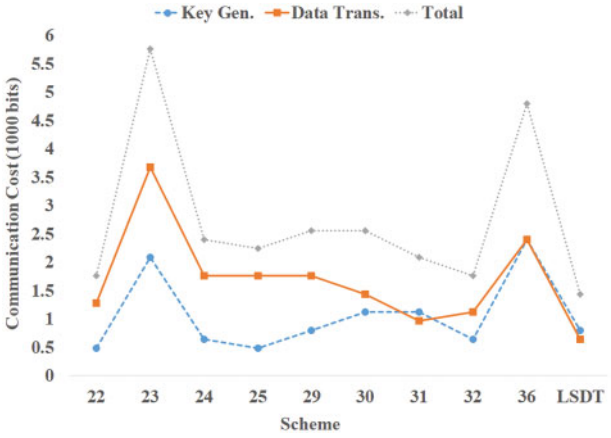

Figure 6: Communication cost comparison

In Fig. 6, the comparison of communication costs demonstrates that LSDT outperforms other related schemes. This achievement can be attributed to the effective combination of symmetric keys and the utilization of the Elliptic Curve MQV asymmetric key agreement protocol. The scheme's ability to minimize overhead and optimize data transmission contributes to its superiority in terms of communication costs. Furthermore, the analysis provided in Section 4.1 offers detailed insights into the optimizations employed by the LSDT scheme to achieve these superior results.

Similarly, Fig. 7 showcases the comparative analysis of computation costs, revealing the superior performance of the LSDT scheme. By leveraging a well-designed combination of symmetric keys and

the Elliptic Curve MQV protocol, the scheme minimizes computational overhead while maintaining a high level of security. This efficient utilization of computational resources makes the LSDT scheme highly suitable for resource-constrained IoT environments. For a comprehensive understanding of the computation costs, please refer to Section 4.2, where a detailed breakdown and analysis are provided.

Figure 7: Computation cost comparison

In conclusion, the results of the comparison demonstrate that the LSDT scheme excels in terms of both communication and computation costs when compared to other related security schemes. The scheme's lightweight nature, combined with its robust security measures, positions it as a suitable choice for IoT environments with limited resources. The findings presented in this study contribute to the advancement of secure data transmission in IoT applications and highlight the potential of the LSDT scheme in addressing the challenges faced in such environments.

6 Research Limitations

While the proposed LSDT scheme appears promising, there are some limitations to consider. Firstly, the evaluation of the scheme's performance is conducted within a simulation environment, which may not accurately reflect real-world conditions. Additionally, the scheme's scalability requires further investigation to determine its feasibility. Scalability is a crucial aspect to consider in IoT environments, as the number of connected devices and the volume of transmitted data continue to grow rapidly. It is essential to evaluate whether the LSDT scheme can accommodate a large-scale deployment without compromising its performance and efficiency. Furthermore, it is important to study the potential impact of network latency and packet loss on the effectiveness of the LSDT scheme, as these factors hold significant importance in IoT environments [15]. By conducting a comprehensive study on how these issues can affect the scheme's performance, we can better understand the practical implications and optimize the scheme accordingly. This analysis should encompass scenarios where network connectivity is unstable or prone to disruptions, as well as situations where packets may be lost or delayed during transmission. Such insights will allow us to develop robust strategies to mitigate the impact of these challenges and ensure reliable and secure data transmission in IoT environments.

7 Conclusion and Future Directions

IoT has a significant impact across many fields, from small wearable devices to substantial industrial systems. However, secure data transmission is considered one of the major challenges in

IoT environments. In this article, we proposed LSDT as a lightweight (in terms of communication and computation costs) security scheme that addresses this challenge by providing confidentiality, integrity, and end-to-end authentication in IoT environments. LSDT achieves this by effectively combining symmetric keys and ECMQV protocols.

We analyzed LSDT and compared it to existing secure data transmission schemes. Obtained results indicate that LSDT is resistant to a variety of cybersecurity attacks while ensuring confidentiality, integrity, and end-to-end mutual authentication. Furthermore, our comparative analysis shows that LSDT is efficient and suitable for IoT applications as it performs better compared to other relevant schemes in terms of communication and computation costs.

Although the proposed LSDT scheme shows promise, there are some limitations to consider. Firstly, the evaluation of the scheme's performance is conducted within a simulation environment, which may not accurately reflect real-world conditions. The scheme's scalability also requires further investigation. Furthermore, it is important to study the potential impact of network latency and packet loss on the LSDT scheme, which are crucial considerations for IoT environments. Therefore, a comprehensive assessment of these limitations is necessary before implementing the LSDT scheme in practical IoT applications.

As for future work, we are implementing a prototype to validate the proposed scheme that can be applied in IoT environments. Furthermore, our work could be expanded to include heterogeneous WSNs with numerous base stations. Another way to extend this work is by exploring the application of innovative techniques such as blockchain to establish end-to-end authentication across all scheme components and conducting a comprehensive performance evaluation in comparison to other relevant schemes.

Acknowledgement: None.

Funding Statement: The authors would like to acknowledge the support of the Interdisciplinary Research Center for Intelligent Secure Systems (IRC-ISS) Internal Fund Grant #INSS2202.

Author Contributions: The authors confirm contribution to the paper as follows: Study conception and design: Farag Azzedin, Ibraheem Al-Hejri; analysis and interpretation of results: Ibraheem Al-Hejri, Farag Azzedin, Sultan Almuhammadi; draft manuscript preparation: Ibraheem Al-Hejri, Farag Azzedin, Sultan Almuhammadi. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. E. Barka *et al.*, "Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure," *Trans. Emerg. Telecomm. Technol.*, vol. 33, no. 8, pp. e3706, 2022. doi: 10.1002/ett.3706.

[2] A. Lakhan *et al.*, "Secure blockchain assisted internet of medical things architecture for data fusion enabled cancer workflow," *Internet Things*, vol. 24, no. 1, pp. 100928, 2023. doi: 10.1016/j.iot.2023.100928.

[3] S. H. Al Zaabi and R. Zamri, "Managing security threats through touchless security technologies: An overview of the integration of facial recognition technology in the UAE oil and gas industry," *Sustainability*, vol. 14, no. 22, pp. 14915, 2022. doi: 10.3390/su142214915.
[4] F. Azzedin, H. Suwad, and Z. Alyafeai, "Countermeasureing zero day attacks: Asset-based approach," in *2017 Int. Conf. High Perform. Comput. Simul. (HPCS)*, Genoa, Italy, IEEE, 2017, pp. 854–857.
[5] M. Lehto, "Cyber-attacks against critical infrastructure," in *Cyber Secur.: Crit. Infrastruct. Protect.*, Springer, 2022, pp. 3–42.
[6] Z. Yang *et al.*, "Indicator-based resilience assessment for critical infrastructures–A review," *Saf. Sci.*, vol. 160, no. 4, pp. 106049, 2023. doi: 10.1016/j.ssci.2022.106049.
[7] N. A. Jalali and H. Chen, "Federated learning security and privacy-preserving algorithm and experiments research under internet of things critical infrastructure," *Tsinghua Sci. Technol.*, vol. 29, no. 2, pp. 400–414, 2023. doi: 10.26599/TST.2023.9010007.
[8] V. Khaustova, M. R. Tirlea, L. Dandara, N. Trushkina, and I. Birca, "Development of critical infrastructure from the point of view of information security," *Univers Strateg.*, vol. 53, no. 1, pp. 2023, 2023.
[9] S. Alyami, R. Alharbi, and F. Azzedin, "Fragmentation attacks and countermeasures on 6LoWPAN internet of things networks: Survey and simulation," *Sensors*, vol. 22, no. 24, pp. 9825, Dec. 14, 2022. doi: 10.3390/s22249825.
[10] P. Nayak and G. Swapna, "Security issues in IoT applications using certificateless aggregate signcryption schemes: An overview," *Internet of Things*, vol. 21, pp. 100641, Apr. 1, 2023.
[11] F. Stolz, M. Fyrbiak, P. Sasdrich, and T. Güneysu, "Recommendation for a holistic secure embedded ISA extension," in *Int. Conf. Appl. Cryptogr. Netw. Secur.*, Kyoto, Japan, Springer, 2023, pp. 62–84.
[12] F. Azzedin and T. Alhazmi, "Secure data distribution architecture in IoT using MQTT," *Appl. Sci.*, vol. 13, no. 4, pp. 2515, 2023. doi: 10.3390/app13042515.
[13] U. Panahi and C. Bayılmıs, "Enabling secure data transmission for wireless sensor networks based IoT applications," *Ain Shams Eng. J.*, vol. 14, no. 2, pp. 101866, 2023. doi: 10.1016/j.asej.2022.101866.
[14] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," *Internet Things*, vol. 15, no. 11, pp. 100420, 2021. doi: 10.1016/j.iot.2021.100420.
[15] F. Azzedin and I. Alhejri, "A layered taxonomy of internet of things attacks," in *Proc. 6th Int. Conf. Future Netw. Distr. Syst.*, Tashkent, Uzbekistan, 2022, pp. 631–636.
[16] F. Varghese and P. Sasikala, "A detailed review based on secure data transmission using cryptography and steganography," in *Wirel. Pers. Commun.*, 2023, pp. 1–28.
[17] F. Li *et al.*, "Privacy-aware secure anonymous communication protocol in CPSS cloud computing," *IEEE Access*, vol. 8, pp. 62660–62669, 2020. doi: 10.1109/ACCESS.2020.2982961.
[18] L. Li, S. Li, H. Peng, and J. Bi, "An efficient secure data transmission and node authentication scheme for wireless sensing networks," *J. Syst. Archit.*, vol. 133, no. 4, pp. 102760, 2022. doi: 10.1016/j.sysarc.2022.102760.
[19] N. Mahlake, T. E. Mathonsi, D. Du Plessis, and T. Muchenje, "A lightweight encryption algorithm to enhance wireless sensor network security on the internet of things," *J. Commun.*, vol. 18, pp. 47–57, 2023. doi: 10.12720/jcm.18.1.47-57.
[20] T. Alam, "Efficient and secure data transmission approach in cloud-MANET-IoT integrated framework," *J. Telecommun., Electr. Comput. Eng.*, vol. 12, no. 1, 2020. doi: 10.2139/ssrn.3639058.
[21] X. Luo *et al.*, "A lightweight privacy-preserving communication protocol for heterogeneous IoT environment," *IEEE Access*, vol. 8, pp. 67192–67204, 2020. doi: 10.1109/ACCESS.2020.2978525.
[22] Y. Harbi, Z. Aliouat, S. Harous, and A. Bentaleb, "Secure data transmission scheme based on elliptic curve cryptography for internet of things," in *Int. Symp. Model. Implemen. Complex Syst.*, Springer, 2019, pp. 34–46.
[23] F. Wu, L. Xu, S. Kumari, and X. Li, "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on internet of things security," *J. Ambient Intell. Humaniz. Comput.*, vol. 8, no. 1, pp. 101–116, 2017. doi: 10.1007/s12652-016-0345-8.

[24] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu and N. Kumar, "A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers," *J. Supercomput.*, vol. 74, no. 12, pp. 6428–6453, 2018. doi: 10.1007/s11227-017-2048-0.
[25] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive Mob. Comput.*, vol. 24, no. 1, pp. 210–223, 2015. doi: 10.1016/j.pmcj.2015.08.001.
[26] R. Sharma and R. Arya, "Secure transmission technique for data in IoT edge computing infrastructure," *Complex Intell. Syst.*, vol. 8, no. 5, pp. 3817–3832, 2022. doi: 10.1007/s40747-021-00576-7.
[27] H. Li, "Pseudo-random scalar multiplication based on group isomorphism," *J. Inf. Secur. Appl.*, vol. 53, no. 177, pp. 102534, 2020. doi: 10.1016/j.jisa.2020.102534.
[28] T. K. Dang, C. D. Pham, and T. L. Nguyen, "A pragmatic elliptic curve cryptography-based extension for energy-efficient device-to-device communications in smart cities," *Sustain. Cities Soc.*, vol. 56, no. 7, pp. 102097, 2020. doi: 10.1016/j.scs.2020.102097.
[29] P. K. Panda and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment," *J. Reliab. Intell. Environ.*, vol. 6, no. 2, pp. 79–94, 2020. doi: 10.1007/s40860-020-00098-y.
[30] K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," *Int. J. Inf. Secur.*, vol. 19, no. 1, pp. 129–146, 2020. doi: 10.1007/s10207-019-00464-9.
[31] X. Li, J. Peng, S. Kumari, F. Wu, M. Karuppiah and K. K. Raymond Choo, "An enhanced 1-round authentication protocol for wireless body area networks with user anonymity," *Comput. Electr. Eng.*, vol. 61, pp. 238–249, 2017. doi: 10.1016/j.compeleceng.2017.02.011.
[32] M. L. Das, P. Kumar, and A. Martin, "Secure and privacy-preserving rfid authentication scheme for internet of things applications," *Wirel. Pers. Commun.*, vol. 110, no. 1, pp. 339–353, 2020. doi: 10.1007/s11277-019-06731-1.
[33] C. C. Chang, H. L. Wu, and C. Y. Sun, "Notes on "secure authentication scheme for IoT and cloud servers"," *Pervasive Mob. Comput.*, vol. 38, no. 15, pp. 275–278, 2017. doi: 10.1016/j.pmcj.2015.12.003.
[34] K. H. Wang, C. M. Chen, W. Fang, and T. Y. Wu, "A secure authentication scheme for internet of things," *Pervasive Mob. Comput.*, vol. 42, no. 15, pp. 15–26, 2017. doi: 10.1016/j.pmcj.2017.09.004.
[35] C. Zhang *et al.*, "Achieving fuzzy matching data sharing for secure cloud-edge communication," *China Commun.*, vol. 19, no. 7, pp. 257–276, 2022. doi: 10.23919/JCC.2022.07.020.
[36] Y. Harbi, Z. Aliouat, A. Refoufi, S. Harous, and A. Bentaleb, "Enhanced authentication and key management scheme for securing data transmission in the internet of things," *Ad Hoc Netw.*, vol. 94, no. 2, pp. 101948, 2019. doi: 10.1016/j.adhoc.2019.101948.
[37] A. Mehmood, M. M. Umar, and H. Song, "ICMDS: Secure inter-cluster multiple-key distribution scheme for wireless sensor networks," *Ad Hoc Netw.*, vol. 55, no. 9, pp. 97–106, 2017. doi: 10.1016/j.adhoc.2016.10.007.
[38] E. Yuan, L. Wang, S. Cheng, N. Ao, and Q. Guo, "A key management scheme based on pairing-free identity based digital signature algorithm for heterogeneous wireless sensor networks," *Sensors*, vol. 20, no. 6, pp. 1543, 2020. doi: 10.3390/s20061543.
[39] H. Barati *et al.*, "A hierarchical key management method for wireless sensor networks," *Microprocess. Microsyst.*, vol. 90, no. 1, pp. 104489, 2022. doi: 10.1016/j.micpro.2022.104489.
[40] M. Ataei Nezhad, H. Barati, and A. Barati, "An authentication-based secure data aggregation method in internet of things," *J. Grid Comput.*, vol. 20, no. 3, pp. 29, 2022. doi: 10.1007/s10723-022-09619-w.
[41] D. Fang, Y. Qian, and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3474–3484, 2020. doi: 10.1109/JIOT.2020.2970974.
[42] F. Afroz and R. Braun, "Empirical analysis of extended QX-MAC for IoT-based WSNS," *Electronics*, vol. 11, no. 16, pp. 2543, 2022. doi: 10.3390/electronics11162543.
[43] A. Seyyedabbasi, F. Kiani, T. Allahviranloo, U. Fernandez-Gamiz, and S. Noeiaghdam, "Optimal data transmission and pathfinding for WSN and decentralized IoT systems using I-GWO and Ex-GWO algorithms," *Alex. Eng. J.*, vol. 63, no. 12, pp. 339–357, 2023. doi: 10.1016/j.aej.2022.08.009.

[44] T. Palanisamy, D. Alghazzawi, S. Bhatia, A. Abbas Malibari, P. Dadheech and S. Sengan, "Improved energy based multi-sensor object detection in wireless sensor networks," *Intell. Autom. Soft Comput.*, vol. 33, no. 1, pp. 227–244, 2022. doi: 10.32604/iasc.2022.023692.
[45] G. Halidoddi and R. Pandu, "Secured data transmission using multi-objective trust based Bat optimization algorithm and enhanced homomorphic cryptosystem for WSN," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 1, pp. 214–224, 2022.
[46] V. Sivasankarareddy, G. Sundari, C. Rami Reddy, F. Aymen, and E. C. Bortoni, "Grid-based routing model for energy efficient and secure data transmission in WSN for smart building applications," *Appl. Sci.*, vol. 11, no. 22, pp. 10517, 2021. doi: 10.3390/app112210517.
[47] A. Johnson, J. Molloy, J. Yunes, J. Puthuparampil, and A. Elleithy, "Security in wireless sensors networks," in *2019 IEEE Long Island Syst., Appl. Tech. Conf. (LISAT)*, Farmingdale, NY, USA, IEEE, 2019, pp. 1–3.
[48] N. Fayed, E. Daydamoni, and A. Atwan, "Efficient combined security system for wireless sensor network," *Egypt. Inform. J.*, vol. 13, no. 3, pp. 185–190, 2012. doi: 10.1016/j.eij.2012.09.001.
[49] N. N. Anandakumar, M. P. L. Das, S. K. Sanadhya, and M. S. Hashmi, "Reconfigurable hardware architecture for authenticated key agreement protocol over binary edwards curve," *ACM Trans. Reconfig. Tech. Syst.*, vol. 11, no. 2, pp. 1–19, 2018. doi: 10.1145/3231743.
[50] J. Großschädl, A. Szekely, and S. Tillich, "The energy cost of cryptographic key establishment in wireless sensor networks," in *Proc. 2nd ACM Symp. Inf., Comput. Commun. Secur.*, Singapore, 2007, pp. 380–382.
[51] H. Krawczyk, "HMQV: A high-performance secure diffie-hellman protocol," in *Annu. Int. Cryptol. Conf.*, Springer, 2005, pp. 546–566.
[52] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in *2008 Int. Conf. Inf. Process. Sens. Netw. (IPSN 2008)*, St. Louis, Missouri, USA, IEEE, 2008, pp. 245–256.
[53] S. Jebri, A. B. Amor, M. Abid, and A. Bouallegue, "Enhanced lightweight algorithm to secure data transmission in IoT systems," *Wirel. Pers. Commun.*, vol. 116, no. 3, pp. 2321–2344, 2021.
[54] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Gener. Comput. Syst.*, vol. 129, no. 5, pp. 77–89, 2022. doi: 10.1016/j.future.2021.11.011.
[55] K. T. Nguyen, "Lightweight security protocols for IP-based wireless sensor networks and the internet of things," Ph.D. dissertation, Institut National des Télécommunications, France, 2016.
[56] S. S. Hameedi and O. Bayat, "Improving IoT data security and integrity using lightweight blockchain dynamic table," *Appl. Sci.*, vol. 12, no. 18, pp. 9377, 2022. doi: 10.3390/app12189377.
[57] L. Xu and F. Wu, "Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care," *J. Med. Syst.*, vol. 39, no. 2, pp. 1–9, 2015. doi: 10.1007/s10916-014-0179-x.
[58] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with cooja," in *Proc. 2006 31st IEEE Conf. Local Comput. Netw.*, Tampa, FL, USA, IEEE, 2006, pp. 641–648.
[59] W. B. Hsieh and J. S. Leu, "Implementing a secure VoIP communication over SIP-based networks," *Wirel. Netw.*, vol. 24, no. 8, pp. 2915–2926, 2018. doi: 10.1007/s11276-017-1512-3.
[60] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, "Key management protocol with implicit certificates for IoT systems," in *Proc. 2015 Workshop on IoT Chall. Mob. Indus. Syst.*, New York, NY, USA, 2015, pp. 37–42.
[61] K. Sarmila and S. Manisekaran, "Honey encryption and AES based data protection against brute force attack," in *2022 Sixth Int. Conf. I-SMAC (IoT in Soc., Mob., Anal. Cloud)(I-SMAC)*, Dharan, Nepal, IEEE, 2022, pp. 187–190.