A Lightweight Searchable Encryption and Delegation Mechanism with Forward Privacy for Improving the Security of Industrial Internet of Things-Cloud Systems

S. VENKATESAN (✉ venkatesan708@gmail.com)

Madurai Kamaraj University

K. RAJA RAJESHWARI

Madurai Kamaraj University

M. RAMAKRISHNAN

Madurai Kamaraj University

Research Article

Keywords: Lightweight Searchable Encryption and Delegation (LSED), Data Security, Forward Privacy, Confidentiality, Industrial Internet of Things (IIoT), Cryptography Models

Posted Date: February 23rd, 2022

DOI: <https://doi.org/10.21203/rs.3.rs-1384533/v1>

License: © ⓘ This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

A Lightweight Searchable Encryption and Delegation Mechanism with Forward Privacy for Improving the Security of Industrial Internet of Things-Cloud Systems

S. VENKATESAN¹, K. RAJA RAJESHWARI², M. RAMAKRISHNAN³

1. Research Scholar, Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamil Nadu, India. (E-mail: venkatesan708@gmail.com).
2. Research Scholar, Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamil Nadu, India. (E-mail: rajasubulakshmi@gmail.com).
3. Professor and Head, Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamil Nadu, India. (E-mail: ramkrishod@gmail.com).

Abstract— Improving the security and privacy of the industrial data stored in cloud systems is one of the demanding and challenging problem in the recent days, due to the increased utilization rate of IIoT systems. For this purpose, various lightweight cryptographic models are developed in the conventional works, which are mainly focusing on ensuring the data security against the adversaries. However, it limits with the main problems of increased computational complexity, cost complexity, and time consumption, which degrades the performance of entire system. Hence, this paper objects to design an advanced cryptography models, named as Lightweight Searchable Encryption and Delegation (LSED) methodology with forward privacy for enabling the secured data storage and retrieval operations in IIoT-cloud systems. Moreover, the searchable encryption incorporated with the forward privacy property considers that the previously stored trapdoor is invalid for the recently updated cipher data, which efficiently enhances the security of IIoT data against the adversaries. During performance evaluation, there are various evaluation metrics have been utilized for validating the results of both existing and proposed searchable encryption techniques.

Index Terms— Lightweight Searchable Encryption and Delegation (LSED), Data Security, Forward Privacy, Confidentiality, Industrial Internet of Things (IIoT), and Cryptography Models.

I. INTRODUCTION

Industrial Internet of Things (IIoT) [1-3] have gained a significant attention in the present days, due to its rapid development and utilization. This technology [4, 5] includes the advantages of the automation technologies, reliable communication among the machines, increased ability in handling the large dimensional data, and high learning capability. In this environment [6-9], the communication and interfacing devices are mainly used to perform the processes of monitoring, gathering the large dimensional data, and

analyzing the information. Then, this kind of data can be frequently uploaded to the cloud system by using the intermediate devices of servers/gateways that are located in the specified area. But, this type of communication system [10-12] is more susceptible to the security vulnerabilities, because the untrusted cloud may intend to access the large amount of private or confidential data. Hence, it is more essential to provide security to these systems for ensuring the privacy and confidentiality [13, 14] of the industrial data. For this purpose, there are various cryptography mechanisms are developed for improving the security of IIoT platform [15, 16], which are mainly objects to ensure the data security against the unauthenticated or malicious access. When compared to the other cryptographic models, the Searchable Encryption (SE) is considered as one of the most suitable option for guaranteeing the increased security [17-19] of data stored in cloud systems.

Typically, the SE mechanism [20-22] is a kind of encryption standard that comprises the index based searching structures, which are used to find out the encrypted outsourced cipher data in an efficient way. Moreover, this mechanism is categorized into the types of symmetric SE and searchable public key encryption [23, 24], in which the symmetric models require low computational costs and offers an increased security to the data users. Similar to that searchable public key models does not require any key distribution and management processes, hence it is the most suitable option for the IIoT-cloud systems [21, 25, 26]. Conventionally, numerous research works [27, 28] are done in the field of cryptography for ensuring the properties of data security, privacy, and confidentiality against the adversaries. However, it limits with the major problems of increased computational cost, time, and complexity [29-32]. Therefore, this work intends to develop a lightweight cryptography model based on searchable encryption for securely storing and retrieving the IIoT data. The main contributions behind this work are as follows:

- The LSED technique is mainly used to accomplish an increased efficiency in searching, and forward privacy without exclusive key management process.
- Also, it helps to reduce the searching complexity with reduced computation overhead.
- To evaluate the performance of this model, there are various evaluation metrics have been utilized for results analysis and comparison.

The rest of sections present in the paper are structuralized as follows: Section II investigates about some of the existing works related to the secured data storage and retrieval in IIoT-cloud systems with its advantages and disadvantages. The detailed description about the proposed methodology is presented with its clear architecture model and algorithmic illustrations in Section III. The performance results of both existing and proposed security techniques are validated and compared in Section IV. Finally, the overall paper is concluded with its obtainment and future work in Section V.

II. RELATED WORKS

This section examines some of the conventional cryptography approaches used for securely storing and retrieving the IIoT data in a cloud system. Also, it investigates the benefits and demerits of the existing security mechanisms [33] based on its key principles and operating characteristics.

Abuhasel, et al [34] developed a new framework for managing the resources in cloud-IIoT systems, where the Rivest Shamir Adleman (RSA) method was utilized for ensuring the security of each IIoT device. Here, the device authentication [35] was performed based on the processes of registration, login and verification by using the SHA-512 cryptographic model. Moreover, the RSA encryption mechanism was utilized to provide the additional level of security for the data stored in the IIoT systems. For validating the performance of encryption technique, the measures like encryption time, decryption time, and key generation time have been computed with respect to varying key sizes. However, it has the major limitations of increased complexity in algorithm design, and increased error rate, which degrades the performance of overall security system. *Iqbal, et al* [10] recommended a certificateless cryptographic technique for solving the problems of certificate management and key escrow with increased scalability of networks. Here, the fine grained access control policy mechanism [36] was utilized to manage the sensitive information for secured data transmission. *Sai, et al* [14] constructed a graph based security framework for detecting vulnerabilities in IIoT systems, where the security was ensured by using the lightweight authentication mechanism. In this model [33], the device vulnerabilities have been identified by estimating the dependency value using the graph modeling approach.

In Attribute Based Encryption (ABE) [37]: both the data encryption and decryption could be performed, which has the advantages of better security and optimal performance outcomes. Still, it limits with the problems of increased cost consumption for key for key generation and encryption, and reduced scalability. In Key-Policy Attribute Based Encryption (KP-ABE) [38]: the access tree structure has the responsibility

for generating the keys based on the set pre-determined attributes. The user can encrypt and decrypt the data by using the set of pre-determined attributes. It has the advantage of ensured security with the user attributes, and drawbacks of reduced control policies, and high complexity. In Cipher-text Policy Attribute Based Encryption (CP-ABE) [39]: the data owner could define the set of policies for who could decrypt the original data. It has the ability to solve the problem of single authority failure. However, it has the problems of inefficient computations, more energy consumption, and reduced security. The Identity Based Encryption (IBE) [40] is a kind of public key encryption mechanism, where the key has been generated based on the set of distinct identities of user. Here, the trusted authority can generate the secret private key based on the generated public key. It provides the benefits of ensured properties of confidentiality and privacy, and it has the ability to handle large dimensional dataset. Yet, it facing the difficulties related to increased cost consumption, does not offer the non-repudiation property, and inability to solve the key escrow problem.

Zhang, et al [41] implemented a light weight searchable ABE mechanism for enabling the multiple keyword searching in IIoT systems. The key factor of this work [42] was to increase the data privacy of the industrial data stored in cloud with a flexible access controlling mechanism. Also, it intends to accomplish the properties of lightweight encryption, high data confidentiality, decentralized key management, and exact data retrieval appropriate to the user keyword [42]. *Zhou, et al* [43] introduced a file centric multi-key aggregate keyword SE model for efficiently satisfying the security requirements [44] of IIoT systems. The main purpose of this work [45] was to reduce both the computational cost as well storage cost of the security scheme for enhancing the industrial production growth and development. However, this technique facing the difficulties related to the factors of low performance, and inefficient searching, which degrades the performance of entire system.

Wu, et al [46] utilized IIoT platform for enabling the secured data storage and retrieval operations, where the bilinear diffie hellman process is also carried out for strengthening the security property. *Sujatha, et al* [36] developed a hybrid signcryption algorithm for ensuring the secured data transmission in cloud systems. The purpose of this work was to increase the factors of efficiency, security, and reliability while establishing the data transmission. *Ramakrishnan, et al* [33] designed a CF-huffman code based signcryption methodology for enhancing the compression ration with respect to the frequent items exist in the data model. This work highly concentrating on improving the security [32] of data transmission based on the optimal selection of attributes. The key benefits of this paper were reduced running time and memory utilization rate. *Sujatha and Ramakrishnan* [47] intended to utilize the certificateless signcryption model incorporated with the Keccak MD hash algorithm for enhancing the security of data stored in cloud system.

III. PROPOSED METHODOLOGY

This section presents the detailed description about the proposed Lightweight Searchable Encryption and Delegation

(LSED) methodology used for guaranteeing the privacy and searching efficiency of the IIoT outsourced data. Also, this work objects to minimize an expensive key management process with ensured forward privacy [45, 48]. The typical architecture model of IIoT-cloud data storage and retrieval system is shown in Fig 1, where the partially trusted cloud server is considered for data processing activities such as storage and retrieval in IIoT systems. Typically, there are different types of smart devices [24, 48] are interlinked with the sensor devices, which helps to collect the data from the owner and send the data to the cloud server through an active communication. In IIoT systems, the crowdsourced data need to be verified before storing it in the cloud server, because only the authorized persons can able to access those data at various locations. Hence, the privacy and confidentiality of the stored data are highly depends on the cloud server, if it is not fully trusted, it is more essential to ensure the authenticity and confidentiality of the outsourced in prior. Hence, this research work intends to implement a light weight cryptography model for ensuring the security of IIoT data stored in cloud.

In IIoT systems, the sensor devices are mainly used for gathering the large dimensional data from the owner, and transmitting it to the cloud system through servers or gateways. In this environment [49], providing security to the outsourced data is one of the demanding and essential task for guaranteeing the privacy and security of the sensitive data. For this purpose, there are different types of cryptographic mechanisms are developed in the conventional works [23, 50, 51], which includes Symmetric Key Encryption (SKE), Searchable Encryption (SE), Attribute Base Encryption (ABE), Identity Based Encryption (IBE) and policy based encryption. But, these techniques limit with the problems of inefficient searching, increased computational complexity, and computation overhead. In order to solve these problems, the proposed work develops a Lightweight Searchable Encryption and Delegation (LSED) methodology for improving the security and confidentiality of IIoT outsourced data.

Fig 1. Data storage in IIoT-cloud system

The proposed Lightweight Searchable Encryption and Delegation (LSED) comprises the hidden structure for maintaining the keywords that are associated with the searchable texts with the hidden relationships. The sample illustration of the hidden structure with the relationship is depicted in Fig 2. The main benefit of using the hidden structure analysis is to improve the efficiency of searchable encryption operation.

Fig 2. Hidden structure

A. Entities of IIoT Cloud System

The proposed IIoT-cloud framework comprises the following entities: Data Holder (DH), Data Receiver (DR), Certificate Authority (CA), and Cloud Service Provider (CSP). In this scenario, the communication is established between the following entities: asynchronous owner to receiver communication, and communication between CSP and DR using private and public channels. The overall flow of the proposed LSED based IIoT security system is shown in Fig 3, where a ciphertext searchable application has been deployed for enabling the secured data storage and retrieval processes. Then, the roles and responsibilities of each component is described in below:

Data Holder (DH) – The DH has the responsibility for generating both the outsourced data, and encrypted outsourced data in the form of ciphertexts, which comprises the keywords, versio, index, and file texts.

Data Receiver – The DR can search the queries for obtaining the required data by giving the keyword trapdoor, and they can get all relevant files that are relevant to the given keyword.

Certificate Authority (CA) – The CA has the responsibility for issuing the digital certificates to the authenticated users based on their public key. Then, the provided certificate can be further used for proving the authenticity and identity of each user.

Cloud Service Provider – The CSP has unlimited storage capacity and computation capacity for large amount of data storage and retrieval.

Fig 3. Architecture model of the proposed LSED security framework

The novel contribution of the proposed LSED model is, it eliminates the key management problem for reducing the high storage cost consumption. For instance, it is illustrated that the DH can store the encrypted ciphertext in the CSP, and the DR can give request to the CSP by searching keywords and obtains the relevant results from the server. In this scenario, the data authentication is performed only at the data updating phase, hence the DH is not required to stay in online at all time. Also, we assumed that the entities of DH, DR, and CA are fully trusted, and the CSP is considered as the trusted third party entity. It has the responsibility for honestly executing the predefined statements, but is somewhat probing to know about the trapdoors and encrypted data. The proposed scheme comprises the following stages:

- **Setup:** Let, consider the security parameter δ as input, and produced the public parameter P_p as output.
- **KeyGen** (P_p): It generates both the secret key and public key based on the public parameter P_p , and the pair of keys are denoted as (Pub_k, Sec_k) . This procedure can be executed by the DH and DR respectively with the key pairs of (Pub_{kDH}, Sec_{kDH}) and (Pub_{kDR}, Sec_{kDR}) .
- **Data Update** ($P_p, Pub_{kDR}, Sec_{kDH}, D_b(v), v, \Sigma$): Where, P_p indicates the public parameter, Sec_{kDH} defines the secret key of DH, Pub_{kDR} is the public key of DR, $D_b(v)$ represents the set of files with the keyword of v , and Σ is the mapping of information between input and outputs. The output of ciphertext is represented as follows:

$$\omega = (MD_b(v), MH_v) \quad (1)$$

Consequently, the ciphertext data CD_v is obtained and updated with the mapping of Σ . Then, the DH can send the ciphertext data to the CSP for storage, which is represented as shown in equation (1). Then, the CSP can broadcast the CD_v to the DR, which comprises the information related to the keyword

requested by the DR. After that, the receiver can decrypt the cipher data CD_v obtained from the server, and this process can be done offline.

- **Trapdoor** (P_p, Sec_{kDR}, v, D_v): It consider the inputs of public parameter P_p , secret key of DR Sec_{kDR} , keyword v , and cipher data information D_v , then it produced the searchable trapdoor as the output TD_v .
- **Search** (P_p, MD_b, MH, TD_v): This operation considers the input parameters of P_p public parameter, cipher data $(MD_b(v), MH_v)$, trapdoor data with keyword TD_v , and produced the index set as the output with the matching of keywords IS_v .

B. Security Model

In the proposed model, the parameters such as stability and forward privacy have been considered for ensuring the security of IIoT data storage and retrieval system.

Algorithm 1 – Stability of IIoT Data Storage and Retrieval

Step 1: $P_p \leftarrow Setup(\delta)$
Step 2: $(Pub_{kDH}, Sec_{kDH}) \leftarrow KeyGen(P_p)$
Step 3: $(Pub_{kDR}, Sec_{kDR}) \leftarrow KeyGen(P_p)$
Step 4: $(D_b(v), v) \leftarrow Ad_v(P_p, Pub_{kDH}, Pub_{kDR})$ //Where, Ad_v indicates the adversary;
Step 5: Updated data,
 $(MD_b(v), MH(v), CD_v)$
 $\leftarrow Update(P_p, Pub_{kDH}, Sec_{kDR}, D_b(v), v, \Sigma)$
if $v = v^*$
Step 6: $TD_{v^*} \leftarrow Trapdoor(P_p, Sec_{kDR}, v^*, w_{v^*})$
Step 7: $D_b(v) \leftarrow Search(P_p, MD_b(v), MH_v, TD_{v^*})$
else
Step 8: $Null \leftarrow Search(P_p, MD_b(v), MH_v, TD_{v^*})$
//Where, w_{v^*} is attained after decrypting the cipherdata CD_{v^*} .

C. Forward Privacy

The forward privacy is considered as one of the most essential security property need to be addressed for protecting the IIoT-cloud systems against the attacks. Then, this property can be obtained based on the information leakage in the update phase. Particularly, the data that are recently added in to the server could not be obtained by using the previous trapdoor even if it has the same keyword. If the searchable encryption scheme does not has the property of forward privacy, the attacks or malicious users object to access the recently inserted cipher text by using the already selected keywords with the previous trapdoor. Nevertheless, if the encryption scheme has the forward privacy, the adversaries are not able to access the newly inserted cipher data with the help of previously stored trapdoor. Moreover, the searchable encryption incorporated with the forward privacy property considers that the previously stored trapdoor is invalid for the recently updated cipher data. The forward privacy is performed in the update phase and is illustrated as follows:

Algorithm II – Forward privacy

Step 1: $P_p \leftarrow \text{Setup}(\delta)$
Step 2: $(\text{Pub}_{kDH}, \text{Sec}_{kDH}) \leftarrow \text{KeyGen}(P_p)$
Step 3: $(\text{Pub}_{kDR}, \text{Sec}_{kDR}) \leftarrow \text{KeyGen}(P_p)$
Step 4: $(D_b(v), v) \leftarrow \text{Ad}_v(P_p, \text{Pub}_{kDH}, \text{Pub}_{kDR})$
Step 5: $(MD_b(v), MH(v), CD_v) \leftarrow \text{Update}(P_p, \text{Pub}_{kDR}, \text{Sec}_{kDH}, D_b(v), v, \Sigma)$
Step 6: $TD_v \leftarrow \text{Trapdoor}(P_p, \text{Sec}_{kDR}, v, w_v)$
Step 7: $D_b(v) \leftarrow \text{Search}(P_p, MD_b(v), MH(v), CD_v, TD_v)$
Step 8: $(MD_b^*(v), MH_v^*, CD_v^*) \leftarrow \text{Update}(P_p, \text{Pub}_{kDR}, \text{Sec}_{kDH}, D_b^*(v), v, \Sigma^*)$
Step 9: $D_b^*(v) \leftarrow \text{Search}(P_p, MD_b(v), MH_v, CD_v, MD_b^*(v), MH_v^*, CD_v^*, TD_v)$
//Where, Σ^* indicates the updated information map.

In this work, the lightweight encryption model [52] is developed with forward privacy for ensuring the increased security of IIoT-cloud systems. The key benefits of this technique are reduced computation cost, complexity, and time by using an enhanced publickey cryptography technique.

D. Construction of LSED-FP model

The construction model of proposed LSED-FP comprises the following stages:

KeyGen: It considers the system public parameter P_p as the input and generates two random number $(x, y) \xleftarrow{S} \mathbb{R}_q^*$, then its output is produced as the pair of public key and secret key for the DH and DR, as shown in below:

$$\text{PubK}_{DH} = xP, \text{SecK}_{DH} = x$$

$$\text{PubK}_{DR} = yP, \text{SecK}_{DR} = y$$

Update Phase: This module considers the input of $(P_p, (P_p, \text{Pub}_{kDH}, \text{Sec}_{kDR}, MD_b(v), v, \Sigma))$, where the index set of $MD_b(v) = \{in_{v1}, in_{v2} \dots in_{vm}\}$ that contains the keyword of v , and is defined by $v = |MD_b(v)|$. Consequently, the steps involved in this operation are illustrated in below:

Step 1: The state information is represented as follows:
 $(\text{State}_G, G) \leftarrow \Sigma[v]$, which is done by mapping Σ the keyword v with the counter variable G .
Step 2: if $(\text{State}_G, G) = \perp$, in which the state information is randomly selected based on $\text{State}_0 \leftarrow \{0,1\}^\delta$ and $G = 0$;
Step 3: Then, for each index in_{vj} , ($j = 1, 2 \dots m$), the key is selected $key_{G+j} \xleftarrow{S} \{0,1\}^\delta$ and consequently the next state is determined as,
 $\text{State}_{G+j} = F(key_{G+j}, \text{State}_{G+j-1})$
Then, the parameter $BM_{G+j} = (key_{G+j} \parallel \text{State}_{G+j-1} \parallel in_{vj}) \oplus HF_1(\text{State}_{G+j})$ and $U_{G+j} = HF_0(\text{State}_{G+j})$;
Step 4: Set the keyword of, $\Sigma[v] \leftarrow (\text{State}_{G+o}, F + o)$. After that, the version information is selected as $Ver_v \xleftarrow{S} \mathbb{R}_q^*$ and the head information is estimated as follows:
 $BMHF_v =$

$$(0 \parallel \text{State}_{G+o}) \oplus HF_3(\widehat{BM}(\text{Sec}_{kDH}, \text{Pub}_{kDR}, HF_2(v)V)^{Ver_v})$$

and $uHF_v = HF_4(\widehat{key}(\text{Sec}_{kDH}, \text{Pub}_{kDR}, HF_2(v)V)^{Ver_v})$ respectively;

Step 5: The ciphertext is generated and published as shown in below:

$$CD_v = \{CD_{1v}, CD_{2v}\} = \{HF_5(l\text{Pub}_{kDR}) \oplus (0 \parallel v \parallel Ver_v), lU\}$$

is considered as the version information of keyword v of the DR, which is defined by $l \xleftarrow{S} \mathbb{R}_q^*$;

Step 6: Then, the encrypted database is obtained in the form of

$$MD_b(v) = \{(u_{G+1}, keyHF_{G+1}) \dots (u_{G+m}, keyHF_{G+m})\}$$

and the head information $MHead_v = (u_G, keyHF_G)$ to the CSP and is shared in the form of $CD_v = \{CD_{1v}, CD_{2v}\}$ to the DR.

Based on the receiving text of $MD_b(v), MHead_v$, the service provide can set the parameter of $\Theta[u_{G+j}] = [key_{G+j}]$ and $\Theta[uHF_v] = [key_v]$, where $j = 1, 2, \dots m$. Based on the reception of ciphertext $CD_v = \{CD_{1v}, CD_{2v}\}$ by estimating $(0 \parallel v \parallel Ver_v) = CD_{1v} \oplus HF_5(\text{Sec}_{kDR}, CD_{2v})$. At last, the stored is in the form of Ver_v with the keyword of v as $\Gamma[v] = Ver_v$. The main benefits of using the proposed LSED scheme are as follows:

- Reduced computational complexity
- Forward privacy strengthens the security of data
- Optimal performance efficiency
- High security against the adversaries

IV. RESULTS AND DISCUSSION

This section discusses about the performance and evaluation of both existing and proposed searchable encryption models based on the different types of parameters. Fig 4 and Table 1 compares the time cost of both existing and proposed lightweight encryption models with respect to different computational operations such as update, trapdoor, and search. In this analysis, the approximate time for encrypting all files by using the existing and proposed techniques are validated, where it is depicted that the searchable public key encryption model requires increased time consumption for encrypting the data. When compared to the existing encryption standard, the proposed LSED technique consumes reduced time in terms of milliseconds for all operations.

Table 1. Time cost of existing and proposed schemes with different operations

Operations	Searchable Public key Encryption (ms)	LSED (ms)
Update	10494	1312
Trapdoor	419	119
Search	835.6	60

Fig 4. Time cost analysis between existing and proposed security schemes

Figure 6 and Table 2 compares the existing and proposed encryption techniques with respect to the number of matching ciphertexts. Here, the time cost required for searching the ciphertexts are estimated for analyzing the searching complexity of both existing and proposed security mechanisms. From the evaluation, it is identified that the proposed LSED technique requires reduced time cost for matching the ciphertext with respect to the user keyword, which shows the effectiveness of the proposed scheme over the existing scheme.

Table 2. Time cost analysis with respect to varying number of matching ciphertexts

Number of matching ciphertexts	Searchable Public key Encryption	LSED
1000	38	20
2000	58	25
3000	78	30
4000	102	38
5000	122	40
6000	140	45
7000	160	50
8000	190	58
9000	195	60

Fig 5. Time cost Vs Number of matching ciphertexts

Table 3 presents the computational and storage cost analysis of both existing searchable encryption [25] and proposed LSED mechanisms. Here, the computational cost is analyzed in terms of update, trapdoor, and search operations and the storage cost is examined with the forward privacy property. In this analysis, the parameters $\widehat{BP}$ indicates the bilinear pairing operation, H_{PP} is the secured hash to point operation, Sc_M defines the scalar multiplication operation, DB_S denotes the size of database, HF_{Gr2} is the hash function for group 2, M_{Gr2} defines the multiplication operation of group 2, S_{RP} indicates the secured random pseudo number, and Di_{Gr2} is the division operation of group 2. Based on this evaluation, it is analyzed that the computational cost as well as storage cost of the proposed LSED scheme is efficiently reduced, when compared to the existing scheme.

Table 3. Analysis of computational cost and storage cost of existing and proposed schemes

Operations	Existing SE	Proposed LSED
Update	$(1 \cdot (\widehat{BP} + H_{PP} + Sc_M) + DB_S \cdot (HF_{Gr2} + M_{Gr2}))$	$N_{Op} \cdot (\widehat{BP}^* + 2 \cdot Sc_M + 2 \cdot HF_{Gr2}) + DB_S \cdot S_{RP}$
Trapdoor	$1 \cdot (Sc_M + H_{PP})$	$1 \cdot Sc_M$
Search	$1 \cdot \widehat{BP} + (DB_S + 1) \cdot HF_{Gr2} + DB_S \cdot Di_{Gr2}$	$1 \cdot \widehat{BP}^* + HF_{Gr2} + DB_S \cdot Di_{Gr2} \cdot S_{RP}^{-1}$
Storage Cost	$O(Gr_2 X)$	$O(\delta X)$
Security	No Forward Privacy	Supports Forward Privacy

Table 4 depicts the computational cost of the proposed LSED mechanism is evaluated for both IoT and cloud systems with 80bits and 128bits of operation. For this analysis, the operations such as bilinear pairing, hash to point, scalar multiplication, multiplication, division, and hash function have been considered. Based on this analysis, it is evident that the LSED is more effective for 80 bits operations, when compared to the 128 bits of operations.

Table 4. Computational cost analysis of the proposed scheme

Operations	Time cost (ms) for IIoT		Time cost (ms) for Cloud server	
	80 bits	128 bits	80 bits	128 bits
$\widehat{BP}$	277.6	4472.5	13.86	187.96
H_{PP}	301.2	8026	12.56	336.54
Sc_M	117.9	1412	5.125	57.96
Di_{Gr2}	0.20	1.45	0.011	0.059
M_{Gr2}	0.2	1.52	0.009	0.060
HF_{Gr2}	0.85	6.26	0.075	0.37
S_{RP}/S_{RP}^{-1}	0.085	0.092	0.004	0.005

Fig 6 analyzes the encryption time cost analysis of the proposed LSED scheme with respect to varying number of ciphertexts. Similar to that, Fig 7 shows the time cost analysis of existing and proposed security schemes based on the keywords search. From these analysis, it is identified that the proposed LSED technique provides an improved results in terms of reduced time cost complexity with ensured security, and it shows the overall improved performance of the proposed scheme.

Fig 6. Encryption time cost analysis of the proposed LSED mechanism

Fig 7. Time cost analysis based on the keywords search

V. CONCLUSION

This paper proposed a lightweight cryptography model, named as, LSED for enabling the secured data storage and retrieval processes in an IIoT-cloud systems. The main purpose of this technique is to ensure the privacy and searching efficiency of the IIoT outsourced data with reduced expensive key management process. This scheme comprises the hidden structure for maintaining the keywords that are associated with the searchable texts with the hidden relationships, which supports to improve the efficiency of searchable encryption operation. The novel contribution of the proposed LSED model is, it eliminates the key management problem for reducing the high storage cost consumption. Moreover, this scheme utilizes the forward privacy property that operates based on the information leakage in the update phase. Particularly, the data that are recently added in to the server could not be obtained by using the previous trapdoor even if it has the same keyword. The major advantages of using this LSED are as follows: reduced computational complexity, forward privacy strengthens the security of data, optimal performance efficiency, and high security against the adversaries. For analysis, the performance of both existing and proposed searchable encryption models are validated and compared by using various evaluation metrics such as cost complexity, time complexity, and storage complexity. Moreover, the obtained results state that the proposed LSED technique outperforms the other techniques with improved performance results.

In future, this work can be extended by implementing a certificateless signcryption model for guaranteeing the increased security of IIoT data stored in the cloud server.

REFERENCES

- [1] Y. Zhang, X. Liu, X. Lang, Y. Zhang, and C. Wang, "VCLPKES: Verifiable certificateless public key searchable encryption scheme for industrial Internet of Things," *IEEE Access*, vol. 8, pp. 20849-20861, 2020.
- [2] O. O. Olakanmi, and K. O. Odeyemi, "A certificateless keyword searchable encryption scheme in multi-user setting for fog-enhanced Industrial Internet of Things," *Transactions on Emerging Telecommunications Technologies*, pp. e4257, 2021.
- [3] J. Priyanka, and M. Ramakrishnan, "Efficient Gs-IBE for Collusion Resistance on Multi-handler Cloud Environment Using Attribute-Modulator (AM)," *Intelligent Data Communication Technologies and Internet of Things*, pp. 29-39: Springer, 2021.
- [4] S. Rajkumar, and M. Ramakrishnan, "Smcrp: A secure multicast certificateless routing protocol for network security in wban," *Asian Journal of Research in Social Sciences and Humanities*, vol. 6, no. 9, pp. 115-130, 2016.
- [5] J. Raja, and M. Ramakrishnan, "Confidentiality-preserving based on attribute encryption using auditable access during encrypted records in cloud location," *The Journal of Supercomputing*, vol. 76, no. 8, pp. 6026-6039, 2020.
- [6] J. Bader, and A. L. Michala, "Searchable Encryption with Access Control in Industrial Internet of Things (IIoT)," *Wireless Communications and Mobile Computing*, vol. 2021, 2021.
- [7] M. R. Senouci, I. Benkhaddra, A. Senouci, and F. Li, "An efficient and secure certificateless searchable encryption scheme against keyword guessing attacks," *Journal of Systems Architecture*, vol. 119, pp. 102271, 2021.
- [8] N. Pakniat, D. Shiraly, and Z. Eslami, "Certificateless authenticated encryption with keyword search: Enhanced security model and a concrete construction for industrial IoT," *Journal of Information Security and Applications*, vol. 53, pp. 102525, 2020.
- [9] J. Priyanka, K. R. Rajeshwari, and M. Ramakrishnan, "Operative Access Regulator for Attribute Based Generalized Signcryption Using Rough Set Theory." pp. 458-460.
- [10] Y. Lu, J. Li, and Y. Zhang, "Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted IIoT," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2553-2562, 2019.
- [11] P. Liu, K. Liu, T. Fu, Y. Zhang, and J. Hu, "A privacy-preserving resource trading scheme for Cloud Manufacturing with edge-PLCs in IIoT," *Journal of Systems Architecture*, vol. 117, pp. 102104, 2021.
- [12] D. He, M. Ma, S. Zeadally, N. Kumar, and K. Liang, "Certificateless public key authenticated encryption with keyword search for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3618-3627, 2017.
- [13] B. Vanathy, and M. Ramakrishnan, "Signcryption based hyper elliptical curve cryptography framework for key escrow in manet," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 11, no. 3, pp. 91-107, 2020.
- [14] R. J, and R. M, "Attribute string-based data encryption and decryption for privacy preserving through repeated information accessing in cloud environment," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 1, pp. 1-12, 2020.
- [15] Y. Miao, X. Liu, R. H. Deng, H. Wu, H. Li, J. Li, and D. Wu, "Hybrid keyword-field search with efficient key management for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3206-3217, 2018.
- [16] R. S. ME, and M. Ramakrishnan, "LIGHT WEIGHT AUTHENTICATED TWEAKEY FRAMEWORK FOR BODY AREA NETWORK SECURITY."
- [17] Y. Miao, Q. Tong, R. Deng, K.-K. R. Choo, X. Liu, and H. Li, "Verifiable searchable encryption framework against insider keyword-guessing attack in cloud storage," *IEEE Transactions on Cloud Computing*, 2020.
- [18] Sumathi M, Ramakrishnan M, and S. S. M. U., "Survey on data security in cloud environment," *International Journal of Advanced Research in Engineering and Technology*, vol. 11, no. 4, pp. 155-166, 2020.
- [19] T. Sujithra, D. M. Sumathi, M. Ramakrishnan, and S. Sankar, "Id Based Adaptive-Key Signcryption for Data Security in Cloud Environment," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 11, no. 4, 2020.
- [20] E. Zhang, Y. Hou, and G. Li, "A lattice-based searchable encryption scheme with the validity period control of files," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 4655-4672, 2021.
- [21] M. Zamani, M. Safkhani, N. Daneshpour, and A. Abbasian, "A New Searchable Encryption Scheme with Integrity Preservation Property," *Wireless Personal Communications*, vol. 116, no. 4, pp. 3119-3142, 2021.
- [22] H. Li, and T. Jing, "A lightweight fine-grained searchable encryption scheme in fog-based healthcare IoT networks," *Wireless Communications and Mobile Computing*, vol. 2019, 2019.
- [23] B. Sugumar, and M. Ramakrishnan, "Key Escrow with Certificateless Elliptic Curve Segmentation for Grouping of Shared Data in Mobile Networks," *Indian Journal of Public Health Research & Development*, vol. 9, no. 3, 2018.
- [24] B. Sugumar, and M. Ramakrishnan, "Key Escrow with Elliptic Curve Cryptography-Conceptual Framework for Distributed Mobile Networks," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 11, no. 3, pp. 1060-1067, 2018.
- [25] P. Xu, S. He, W. Wang, W. Susilo, and H. Jin, "Lightweight searchable public-key encryption for cloud-assisted wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3712-3723, 2017.

- [26] M. Padhya, and D. C. Jinwala, "CRSQ-KASE: key aggregate searchable encryption supporting conjunctive range and sort query on multi-owner encrypted data," *Arabian Journal for Science and Engineering*, vol. 45, no. 4, pp. 3133-3155, 2020.
- [27] R. Rajesh, M. Ramakrishnan, and B. Sugumar, "A modest approach on MANET using certificateless cryptography." pp. 1197-1204.
- [28] B. Sugumar, and M. Ramakrishnan, "Key escrow with certificateless elliptic curve division for the gathering of shared information in versatile systems," 2018.
- [29] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567-3569, 2018.
- [30] R. Chaudhary, G. S. Aujla, S. Garg, N. Kumar, and J. J. Rodrigues, "SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2629-2640, 2018.
- [31] S. Li, F. Wang, T. Shi, and J. Kuang, "Probably secure multi-user multi-keyword searchable encryption scheme in cloud storage." pp. 1368-1372.
- [32] A. Sivasundari, and M. Ramakrishnan, "Hybrid aggregated signcryption scheme using multi-constraints differential evolution algorithm for security," *Cluster Computing*, vol. 22, no. 2, pp. 3201-3211, 2019.
- [33] M. Ramakrishnan, and S. Rajkumar, "Cf-Huffman code based hybrid signcryption technique for secure data transmission in medical sensor network," *International Journal of Applied Engineering Research*, vol. 10, no. 4, pp. 11455-11474, 2015.
- [34] K. A. Abuhasel, and M. A. Khan, "A secure industrial internet of things (IIoT) framework for resource management in smart manufacturing," *IEEE Access*, vol. 8, pp. 117354-117364, 2020.
- [35] J. Raja, and M. Ramakrishnan, "Public key based third party auditing system using random masking and bilinear total signature for privacy in public cloud environment." pp. 1200-1205.
- [36] R. Sujatha, M. Ramakrishnan, N. Duraipandian, and B. Ramakrishnan, "Optimal adaptive genetic algorithm based hybrid signcryption algorithm for information security," *CMES-Computer Modeling in Engineering and Sciences*, vol. 105, no. 1, pp. 47-68, 2015.
- [37] D. Ziegler, A. Marsalek, B. Prünster, and J. Sabongui, "Efficient Access-control in the IIoT through Attribute-Based Encryption with Outsourced Decryption." pp. 547-552.
- [38] M. La Manna, P. Perazzo, M. Rasori, and G. Dini, "fABELous: An attribute-based scheme for industrial internet of things." pp. 33-38.
- [39] W. Li, J. Si, J. Xing, Y. Zhang, D. Liu, and Z. Sui, "Unified Attribute-Based Encryption Scheme for Industrial Internet of Things." pp. 12-16.
- [40] D. S. Gupta, S. H. Islam, M. S. Obaidat, P. Vijayakumar, N. Kumar, and Y. Park, "A provably secure and lightweight identity-based two-party authenticated key agreement protocol for IIoT environments," *IEEE Systems Journal*, vol. 15, no. 2, pp. 1732-1741, 2020.
- [41] K. Zhang, J. Long, X. Wang, H.-N. Dai, K. Liang, and M. Imran, "Lightweight searchable encryption protocol for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4248-4259, 2020.
- [42] Ramakrishnan M, and a. A. A. S., "Auditing the cloud based banking systems for ensuring storage security," *European Journal of Scientific Research*, vol. 79, no. 2, pp. 310-316, 2012.
- [43] R. Zhou, X. Zhang, X. Du, X. Wang, G. Yang, and M. Guizani, "File-centric multi-key aggregate keyword searchable encryption for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3648-3658, 2018.
- [44] A. A. S, and a. R. M, "Privacy and Integrity Preserving Trusted Third Party Auditing for Outsourced data in the Cloud by using Security Tags," *International Journal of Control Theory and Application*, vol. 10, no. 29, pp. 1-11, 2017.
- [45] S. A. Ali, and M. Ramakrishnan, "Secure provable data possession scheme with replication support in the cloud using Tweaks," *Cluster Computing*, vol. 22, no. 1, pp. 1113-1123, 2019.
- [46] T.-Y. Wu, C.-M. Chen, K.-H. Wang, and J. M.-T. Wu, "Security analysis and enhancement of a certificateless searchable public key encryption scheme for IIoT environments," *IEEE Access*, vol. 7, pp. 49232-49239, 2019.
- [47] R. Sujatha, and M. Ramakrishnan, "Keccak MD hash algorithm based Tag Kem for certificateless hybrid signcryption," *Middle-East J. Sci. Res.*, vol. 22, no. 12, pp. 1746-1752, 2015.
- [48] S. Ahamed Ali, M. Ramakrishnan, and N. Duraipandian, "A Comprehensive Analysis of Key Management Models in the Cloud: Design, Challenges, and Future Directions." pp. 53-61.
- [49] Ramakrishnan M, and a. S. A, "An Efficient And Highly Secured Key Management Signcryption Scheme For Dynamic Hierarchical Access Control," *Journal of Web Engineering*, vol. 17, no. 6, 2018.
- [50] J. Raja, and M. Ramakrishnan, "An enhanced study on cloud data services using security technologies." pp. 1-5.
- [51] S. D. J, and a. R. M, "Fast and Secure Association Rule Mining on Distributed Databases Using FDM and RSA Algorithms," *Journal of Engineering and Applied Sciences* vol. 13, no. 7, pp. 7187-7191, 2018.
- [52] A. Sivasundari, and M. Ramakrishnan, "Hybrid PRNS Version of Elliptic Curve Cryptography with Signcryption Based Security Enhancement Technique for Dynamic Key Management System," *Journal of Computational and Theoretical Nanoscience*, vol. 15, no. 1, pp. 299-310, 2018.

Author's Profile

S. Venkatesan is a Research Scholar in Madurai Kamaraj University, Madurai, Tamil Nadu, India. His main research area includes Network Security, Cryptography and Cloud IOT.

K. Raja Rajeshwari is a Research Scholar in Madurai Kamaraj University, Madurai, Tamil Nadu, India. His main research area includes Cryptography and IOT.

M. Ramakrishnan is working as the Professor and Head of the Department of Computer Applications, Madurai Kamaraj University, Madurai. His main research area includes Network Security, Cloud Computing, Machine Learning and Big Data Analytics. He has published more than 200 International Journals in various topics.