ISSN 2278-3091

Volume 9, No.4, July – August 2020

Pl

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse104942020.pdf

https://doi.org/10.30534/ijatcse/2020/104942020

A Multi Keyword Searchable Attribute-based Encryption Technique for Data Access Control in Cloud Storage

Prashant Mininath Mane[1], Dr. Manna Sheela Rani Chetty[2]

[1]Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. prashant.mane091318@gmail.com

[2]Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. sheelarani_cse@kluniversity.in

ABSTRACT

Multi Authority Cipher-text-policy Attribute-Based Encryption (MA-C-ABE) scheme is a modern form of basic cryptographic and data encryption, which is useful for data cloud storage for fine-grained access control. Multi-Keyword searchable encryption process allows legitimate users to quickly identify useful data stored in a cloud server without disclosing the searched keywords relevant data. Nonetheless, most of the preceding multi-authority attribute-based models are just considered to be true in poor design or lack of user revocation performance. In this study, it includes a multi-keyword searchable attribute-based encryption technique with a cloud-based attribute update, which is a hybrid of the attribute-based encryption algorithm and multi-keyword searchable encryption technique. It provide a Multi - Keyword Searchable Cipher-text - Attribute-based Encryption (MK-C-ABE) with user revocation to solve the existing issues in cloud services, where access mechanisms are partially hidden so that recipients may never extract confidential data from the ciphertext. However, based on the idea of Bi-Linear (BL) and Bi-Linear Diffie -Hellman (BDH), our framework is proven to be safe toward specifically selected keyword attacks and selectively identified ciphertext attacks, and other ensuring privacy protection.

Key words: Multi- Keyword Search; Cipher-text; Attribute-Based Encryption; Bi-Linear; Bi-Linear Diffie-Hellman

1. INTRODUCTION

Cloud storage is now playing a most important role [1] in our everyday lives with the rapid growth of information technology. The confidential information transferred to the cloud server should be kept secret to maintain data protection that allows data users to encrypt confidential folders while transferring [2][38]. In the meantime, keyword searching from a huge quantity of encrypted data often involves rapidly finding the appropriate files for data users. Consequently, establishing the file keyword list is important for allowing a safe keyword search and protecting data search engine security. This indicates that since the cloud server offers a search engine, it's doesn't learn some keyword search information from data users. Similarly, analyzing stable and functional attribute-based encryption systems, which support attribute revocation and multi-keyword search, has significant average values and main characteristics.

Multi-Authority Attribute-Based Encryption is an evolving basic cryptographic to implement fine-grained, attribute-based access control over external provider data stored in the cloud [3]. Attribute-based encryption is mostly categorized into 2 kinds of key policy attribute-based encryption [4] (KP-ABE) and attribute-based encryption [5] (CP-ABE) cipher-text-policy. The KP-ABE system corresponds to the association of the cipher-text with an attribute collection, and access policy is correlated with the private key of a consumer [6]. Some other form is a cipher - text-policy attribute-based encryption (CP-ABE), initially pushed forth by Bethencourt et al. in [7] which turned secure under the basic traditional approach. In a CP-ABE system, the cryptographic keys of the cloud provider are connected to the collection of attributes, and cipher-text is linked to the policy of access.

In the paper, [8] introduced a CP-ABE system in 2008 it was protected under the presumption of Decisional bilinear Diffie- Hellman (DBH). In 2012, cheng et al. [9] proposed a huge-universe CP-ABE system that implemented attribute association and the storage and workload computing of previous CP-ABE systems. The author [10][39] included a testing step in their system to prevent excessive service, and the plan was experimentally demonstrated under the presumption by Decisional Diffie-Hellman (DDH).

The multi-keyword based searchable is a data retrieval tool. An authorized user initially creates an encrypted data depends on retrieved keywords from data storage and then distributes both encrypted data and index form to the cloud server to facilitate successful searches across encrypted data. The cloud server combines the keywords searched with the attribute data to search the encrypted data and recovers the target files to legitimate data users [11]. Multi-Keyword searchable encryption is an efficient way of finding the required files easily from a large volume of encrypted data maintained in cloud storage.

Given that so many existing CP-ABE systems could not allow revoking attributes and multi-keyword searches. A few data access control systems based on multi-authority attributes were proposed to analyze this issue. However, such systems are either proved secure in the selectively protected framework or lack of an effective revocation method. Revocation is also an important factor for implementing access control systems based on attributes in cloud storage. Attributes of the user change dynamically and his access ability may also modify. The vast number of users makes it impossible to revoke access control of the users in a fast and effective manner to ensure data protection.

The proposed system is a hybrid of Multi-keyword searchable encryption system and Multi-Authority ABE system. Thus the system not only resolves the data confidentiality issue with fine-grained access control but also solves the Multi- Keyword searchable issues. Also, the design in the specific bilinear model is known to be semantic protection against selected cipher-text attack. Thus every legitimate user only has to estimate the operation of the exponent once. Therefore the overhead decryption for users can be greatly protected. The proposed algorithm supports multi keywords searchable as well as the actual user can fit the keyword index stored in cloud servers. Also, our multi-keyword search system under the bilinear Diffie-Hellman (BDH) presumption is proven to be a linguistic defense against selected keyword attacks. The multi-keyword searching is near to the real application than a single keyword search. Our approach supports multi-keyword searching to solve this issue.

The remaining part of this work is structured accordingly. Section 2 describes the related works on Attribute-based Encryption and Multi-Keyword Searchable Encryption System. Section 3 discusses the definition and preliminaries of Bilinear Diffie-Hellman (BDH). Section 4 proposes a brief explanation of Multi-Keyword Search with Multi-Authority Attribute-Based Encryption System. In Section 5 analysis the proposed work for performance evaluation and Security. Finally, concludes the work in Section 6.

2. LITERATURE SURVEY

The literature on keyword searchable Attribute-based encryption systems is investigated in this section. Related research is introduced into two types, namely single and multi-keyword searches based on data access control. The main objective of the paper is multi-keyword searchable encryption and therefore the goal is more on these main categories research studies.

2.1 Multi-Keyword Searchable Attribute-Based Encryption

Multi-keyword searchable encryption allows legitimate users to produce several keywords over encrypted data in a search query. The multi-keyword searchable attribute-based encryption was commonly studied as basic cryptography. The author's Buyrukbilen and Bakiras [12] developed a system to help the ranked results searches use multi-keywords. Their implementation uses a basic indexing system, homo-morphic encryption, and a private protocol for the recovery of information to process searches. For the first time in searching multi-keywords, Yu et al. [13][40] found the anonymity that maintains similarity significance. They used a framework of subspace to include precision of the search and homo-morphic encryption for k-top extraction. In the paper [14] suggested a cloud storage CP-ABE system that knows the access control tree and offers a primary revocation method using proxy re-encryption methodology. A variety of systems have shown how to create an ABE system with revocation efficiently and simply [15, 16]. Their implementation uses a basic indexing system, homo-morphic encryption, and a private protocol for the recovery of data to perform searches. Han et al. [17] suggested a searchable ABE technique, in which keywords would search for cipher-text, to resolve the issue. In the cloud storage system, the use of homo-morphic encryption often receives the scope.

In [18], Zhang et al. suggested a method for dealing in a multi-owner system with a stable multi-keyword ranked search. Various data users use different hidden keys in this program to encrypt their records and keywords while authorized users may ask without knowing the keys of these multiple data users. The research introduced an exponential pattern preserving approach to achieve the essential searching queries. Such works will not help complex tasks. The author [19] proposed an approved and multi-keyword searching system over encrypted cloud data by using cipher-text encryption depends on attributes and searchable symmetric data encryption. The system maintains report privacy, as well as resistance to collusion. Sun et al. [20] suggested a verifiable search system with multi-keyword search and adjustment of file collection through large encrypted dynamic files. In this system, the user can create, remove, or modify data without compromising the search functionality of the conjunctive keyword. In the paper [21] suggested a multi-keyword search system classified to support safe and efficient searching through encrypted wireless cloud data. They developed a multi-keyword search using the appropriate score and k-nearest neighbor methods. Jung et al. [22] suggested a CP-ABE privacy-protecting framework for multi-authority clouds. In the revocation process, the user with the benefit of re-encrypting will retrieve the plaintext notification and restore access policy without re-encrypting. Such a method could threaten privacy protection.

In the paper [23] implemented a request for keywords based on the attributes with consumer revocation and request authorization. Various data holders outsource their encrypted data in this process so that users' search features are separate from an attribute authority. The semi-trusted cloud server is essential in the user revocation process for modifying processes. The author Miao et al. [24] suggested a legitimate multi-keyword searchable system for distributed database user configuration where data user could request search queries and assign search privileges to anyone else. The author [25] implemented a testable multi-keyword system based on the attributes. For encrypted data, an authentication attribute is placed in this system, and the user may check the accuracy obtained from the webserver. In the paper [26] proposed a verifiable searchable system focused on the multi-user setting of homo-morphic encryption. Cloud providers can build an encrypted inverse encoding system within their framework without a request. Also, they proposed an authenticated data structure based on an inverted index to test the accuracy of the search queries.

2.2 Multi-Keyword Search based on Data access Control

The author [27] created a current paradigm of fine-grained data access control and applied it to build a multi-user system of searchable encryption in a distributed cloud. Both systems are used in their designs like a transmitted encryption access control system and a searchable encryption system is protected towards collusion between an untrusted server and an intruder. The author [28] suggested access control by integrating key-policy attribute-based encryption with a searchable encryption method to search for encrypted keys. Therefore, a user can get cipher-texts they are allowed to use. Li and Zhang [29] proposed a cloud storage search for keywords and access control systems. This system is based on the encryption searchable by the public key and the encryption dependent on attributes. A cloud provider manages the access policy and involves a certain consumer that needs to extract the encrypted information to be able to search. Some keyword search schemes focused on attributes neglect the emphasis on effectively decrypting retrieved data.

Zhou et al. [30]'s framework enables both online and offline decryption, making it more convenient for users to identify their search criteria in such a way that they can more reliably scan the relevant encrypted data. Li et al. [31] discussed the importance of searchable encryption over cloud data on medical products. They hybrid the secure k-nearest neighbor and attribute-based encryption methods and implemented a complex searchable symmetric encryption system that can be decrypted by doctors who satisfy the access policy of the patient's encrypted files. Also, a searchable system for multi-user access control is proposed in [32].

The author [32] introduced the bi-linear pairing graph as a cryptography basis and compiled a multiuser access control scheme. They then used a proxy server to create the key and the encrypted data was pre-decrypted. The author [33] addressed the security issues of protecting privacy in the Internet of Things (IoT) evaluating. Then, they introduced an IoT thing-fog-cloud framework trained to accomplish a standard SQL query. Data user exchanges the secret key in this framework with the approved users to create query signatures. Because users may retrieve the entire list through legal requests, and access control framework is designed, and the secret key is changed regularly by the data user.

He et al. [34] established searchable basic encryption with attribute-based access control over encrypted data for multi-keyword searching. Data owners may assign search limits to their outsourced encrypted data within the system. The authorized users can search for Boolean keyword expression and any user may create a delegated user key that has a more limited set of attributes. The author [35] have used secure neighborhood computing, polynomial fitting method, and order-preserving encryption to propose a variety of query systems that allow searching and access control of encrypted spatial information.

3. PRELIMINARIES

The security in our proposal is based on the principle of Bilinear (BL) [36] and the principle of Bilinear Diffie-Hellman (BDH) [37]. The definition is specifically for:

3.1 Bilinear (BL)

Let the B_1 and B_2 be two prime ranks (p), multiplicative cyclic bilinear groups. Let 'b' become a B_1 generator. A bilinear graph is an f: $B_1 * B_1 \rightarrow B_2$ includes various characteristics:

Bi-linearity: We have f (b^x,b^y) = f $(\mathrm{b},\mathrm{b})^{xy}$ for both b ∈ B_1 and x; y∈ C_q.
Non-degeneracy: f (b, b)≠ 1.
Computability: There's an appropriate function for calculating f (m, n) for m; n∈ B_1.

3.2 Bilinear Diffie-Hellman (BDH)

The BDH problem in B_1 is described as follows: (b, b^x, b^y, b^z) ∈ B_1 as input, calculate f $(\mathrm{b},\mathrm{b})^{xyz}$ ∈ B_1 as input. They say the opponent O has ε benefit over B_1 in solving BDH problems if

$$\text{p} =| \{O\,(\text{b}, b^x, b^y, b^z) = \text{f}\,(\text{b},\text{b})^{xyz}\ \}| \geq \ \varepsilon$$

It says the assumption of BDH holds in B_1 if no probability polynomial opponent O has non-negligible benefit in resolving the issue of BDH in B_1.

3.3 Linear secret sharing systems

A linear secret sharing system ∑ is also called linear (over C_q) across several components Q if

i. The shares forming a vector over C_q for every group.

ii. A matrix S with m rows and n columns is available, called the share-generating matrix for ∑. For all z = 1,2,…,n, the function δ defines the party labeling n^{th} row of S as $\delta(z)$.

It consider the column vector c= (e, v_1,..., v_n) ∈ C_q^z, where e $C\ C_q$ is the privacy to be shared, and $v_1, \ldots,\ v_n$ ∈ C_q^z are randomly selected. Then S_v is the vector of one share of the privacy e according to∑. The share $(S_v)_n$ belongs to party$\delta(z)$. Assume that ∑ is an LSSS for access control structure C. let P ∈ J be any authorized set, and U ∈ {0,…, n}. Then, there exist constants $\{x_n\ \in\ C_q\}_{n\in 1}$such that, if $\{\alpha_n\}$ are valid shares of any secret p according to∑, then $\sum_{n\in 1}\ x_n$ = p. Similarly, in time polynomial these coefficient $\{x_n\}$ could be identified in the size of the share-generating vector V.

3.4 System and Security Model

In this section, it describes our Multi Authority Access Control system concept, system description, and security standards.

3.4.1 System Model

Figure 1 shows the system architecture of our proposal which comprises the following main entities.

Central Authority (CA): The CA determines the criteria in general. It is responsible for providing the consumer with a gid-related key. It does not take part in any actions relevant to the attributes.

Attribute Authorities (AAs): Every AA is responsible for managing a specific attribute system, which would be a subset of the universe attribute system. Every attribute is regulated by a specific AA in our system, and then each AA can control an arbitrary scale of the domain attribute. When processing a user's private key request it responds to the key associated with the attribute. However, if one or more attributes are removed from one or more users, the main updating procedure is also executed for unrevoked users.

Cloud Storage (CS). The CS is essential for data management and for allowing legitimate users access to data. If a search secret is issued, it is also essential for the keyword search of a customer. And it also changes the user's partial secret key linked to the modified attribute and allows legitimate users to partially decrypt the user's cipher-text using a partial secret key.

Data Owners (DO): A data provider must encrypt it under a DEK (Data Encryption Key) when the data file is sent to the cloud storage. It then establishes an access policy and implements the DEK system. It may also request for deletion of the data file from the cloud storage server.

Data Users (DU): Every legitimate user will search the data from the system for their benefit. The user creates a search trapdoor to maintain search keyword confidentiality. The consumer then sends his identity to CS and looks for a trapdoor. Without disclosing any keyword search data, the CS can locate the encrypted data including the keywords and do a lot of selective decryption tasks to which the user's decryption load. The user eventually gets the partially decrypted files and then decrypts the partially decrypted files using the partial secret key of his owner.

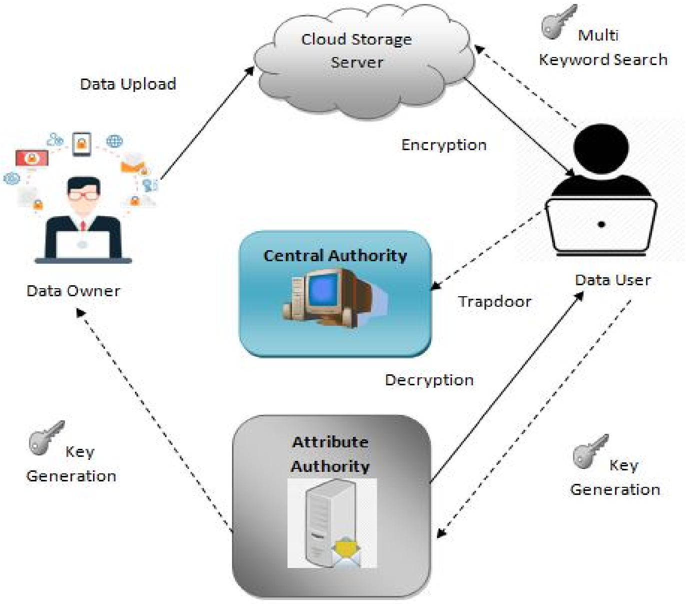

Figure 1: Architecture of the System and Security Model

3.4.2 Security Model

The selective security model for our scheme: Initialization: Opponent O assigns to challenger C a challenged access structure O^* randomly.

Setup: The challenger C executes the setup algorithm and sends the public variables PV to the opponent O and holds the master key (MSK) to itself.

Step 1: Opponent O adaptively provides repeated secret keys belonging to attribute sets(a_1, a_2,.., a_i) where none of these sets match the access framework O^* set.

Challenge: Opponent O transmits two s_1 and s_2 signals of equal duration to C. The challenger C randomly chooses a bit y ∈ {0, 1} and encrypts the message E_y for the access controlO^*. The challenger C sends the cipher-text to the opponent O.

4. PROPOSED SYSTEM

This section discusses the proposed Multi-Keyword Searching Attribute-Based Encryption System. AAs execute the initialization process and with a generator g, extracts a bilinear group B of prime rank p. It chooses two different exponents α, β ∈ C_q, and a hash value H: {0, 1} → B randomly selected as part B. Therefore, AAs calculate the following for a master secret key MSK and a public vector PV:

$$MSK = \{\beta, b^{\alpha}\},\ PV = \{B, b, h= b^{\beta}, x = f\,(b, b)^{\alpha})$$

In this step, AA modifies the retriever R_i with a private key P_i and the data owner with an anonymous keyA_k. Through a secured channel, a data owner with identity I_0 chooses a random attribute $S_0 \in C_q$ and sends I_0 and S_0 to AA. Then AA performs the MK_0 algorithm and returns A_0 = H(I_0)$^{\beta}$ to the data owner and stores S_0. For an I_i identity retriever, AA chooses a random $R_i \in C_q$ and also $R_j \in C_q$ for every attribute $\pi_i \in A_i$ in which A_i represents the set of attributes belonging to S_i. Then AA implements the MK_i algorithm and computes the private key

P_i = {K = $b^{(\alpha + R_i/\beta)}$, { ${R_j}^{i}$ = b^{R_i}H (R_i)^{R_j}, ${R'_j}^{i}$= b^{R_i} } $R_i \in$ I_i }.

The data owner with identity I_0 uses its hidden attribute S_0 for outsourcing a file and outsources its encryption key after such steps of index creation and file encryption. The data owner creates a database encrypted with the keyword. It searches the set of files F and collects the keywords X={ x_a,…, x_n } from F. for every keyword x_a ∈ X, the data provider creates the index by computing I_{x_a} = f (H (x_a), A_0)^{S_0}. Finally, the data provider creates the index for the keyword set X by running the Create Index (F, X) algorithm.

4.1 File Encryption

The files are encrypted by the Data Owner (D_O). The D_O encrypts file F with a symmetric key n using the symmetric encryption algorithm to get ciphertext E_n (F). Therefore D_O encrypts the symmetric key n using the corresponding algorithm for encryption.

Data Owner- Encrypt: {PP, n, (X, β)} → Ciphertext. Let, X be a matrix (a * b), and X_n be the vector that corresponds to the n^{th} row of matrix X. Matrix X rows are associated with attributes by the featureβ. The encryption technique only selects a vector at random; e= (r, $b_1, \dots, b_n$)∈ C_q^z. Such vector 'e' entities can be used to transmit the vector β of the randomized encryption. For n= 1 to j, it evaluates ω_n = $X_n E^S$. Then select random numbers $b_1, \dots, b_n \in C_q$., and cipher-text output:

$$CP = \{(X, \beta),\ E = n.\ f\,(b, b)^{xy},\ E = b^{x},$$

$$X_n = (b^{C_q(n)})^{\omega_n}\ H(\beta(i)^{C_q(n) y_n},\ n=1,2,\dots,n\}$$

Where $C_q(n)$ corresponds to the master key related to the π(n) ∈ M value.

4.2 Trapdoor Generation

If an R_n retriever with the A_n attribute set requires a Trapdoor Gen{TG_n, DO_i} method to retrieve the graded k-top data via multi-keyword search over outsourced files by a data owner with DO_i identity. He encrypts and sendsDO_i to AA by its secret key TG_n. So the AA retrieves the corresponding S_0 and returns to the retriever R_{TG_n}(H $(DO_i)^{\beta\, S_0}$). The retriever R_n then generates trapdoor TG_n = r (H, (y_n), H $(DO_i)^{\beta\, S_0}$), or each keywords y_n. After that, he encrypts the trapdoor with the cloud server 's key C_k and sends R_{C_k} (TG_n, g) regardless of it.

4.3 File Decryption

The retriever $R_n$sends the ciphertext C_p and $({DO_i}^{n}, ({DO'_i}^{n})$ values from secret key TG_n to the proxy server for decryption of a file. The decryption model is implemented by the proxy server. The decryption algorithm (C_p , TG_n, n) uses a ciphertext C_p = (A_t , C', C, { C_d , C'_d }$_{d \in D}$) to decode it from the access tree A_t . It assumes that the attribute set S is used by a data owner to encrypt files. If the node j is a leaf node with q = att_j and q∈ S, the proxy server will calculate:

$$\frac{\mathrm{r}\,\{(DO_i{}^{n}, C_d\}}{\mathrm{r}\,\{(DO_i{}^{n}, C_d\}} = \frac{\mathrm{r}\{b^{R_n}\,\mathrm{H}(n)^{R_n}, b^{y_i(1)}\}}{\mathrm{r}\,\{b^{r_n}, \mathrm{H}(n)^{y_i(1)}\}} = \mathrm{r}\,(\mathrm{b},\mathrm{b})^{R_n y_i(1)}$$

If node j is a non-leaf node, then for all children of n such as node q, the decryption algorithm is retrieved, and the output is stored as Z_q . Let K_n be a set of C_n children of node n. The n-rooted sub-tree is achieved if and only if it satisfies Z_n sub-trees that are rooted at the x-node. The proxy server is calculating as follows, where log, there is a coefficient of Lagrange:

$Z_c = \sum_{q\in Z_n} (K_n{}^{log_{y}.\, Z'_{n(1)}}$, where Z'_n index (n): $q \in Z_n$, y $= index_n$

$$= \sum_{q\in Z_n} (\mathrm{r}\,(\mathrm{b},\mathrm{b})^{R_n.y_i(1)})^{log_{y}.\, Z'_{n(1)}}$$

$$=\sum_{q\in Z_n} (\mathrm{r}\,(\mathrm{b},\mathrm{b})^{R_n.parent_{(i)}{}^{(index(n))}})^{log_{y}.\, Z'_{n(1)}}$$

$$= \sum_{q\in Z_n} (\mathrm{r}\,(\mathrm{b},\mathrm{b})^{R_n.y_i(1)}{}^{log_{y}.\, Z'_{n(1)}} = \mathrm{r}\,(\mathrm{b},\mathrm{b})^{R_n.y_i(1)}$$

The proxy server determines the mixing function required to decrypt the ciphertext from this recursive algorithm by calling Decrypt (C_p , TG_n, n) = $\mathrm{r}\,(\mathrm{b},\mathrm{b})^{R_n.y_i(1)}$= $\mathrm{r}\,(\mathrm{b},\mathrm{b})^{R_n.z}$ algorithm and sending A = $\mathrm{r}\,(\mathrm{b},\mathrm{b})^{R_n.z}$ to the retriever. The retriever would then create a stable file by calculating:

$$\frac{C'_p}{\{\mathrm{f}(C_p, DO_i/A)\}} = \frac{\mathrm{Z}q^{n}}{\{\frac{\mathrm{r}\,(h^{n}, b^{(\sigma+R_n)/\beta})}{\mathrm{r}\,(\mathrm{b,b})^{R_n.z}}\}}$$

$$= \frac{\mathrm{Z}\, r\,(b,b)^{\sigma n}}{\{\mathrm{r}\,(b^{\beta n}, b^{(\sigma+R_n)/\beta} / \mathrm{r}\,(\mathrm{b,b})^{R_n.z})\}} = \mathrm{Z}$$

5. PERFORMANCE ANALYSIS

This chapter specifically discusses comparisons of performance and efficiency between our proposed system and existing work. The performance analyses help to compare the functional differences between the proposed and the other works. In this paper stimulate the key generation time, file encryption, and file decryption by data user with a various set of attributes. Implementation is carried out using the library Pairing Cryptography (LPC). In particular, 'I' refer to the set of attributes, which follow the specification of the access and 'Z' denotes the set of attributes held by the data owner. Some literature supports multi-keyword search and authentication, but it does not support attribute-based encryption and revocation. Furthermore, some other literature does not support proof of security and privacy under the difficult issue. Our proposal supports all the features as compared to other approaches.

Figure 2(a) demonstrates scales of secret key times linearly in the number of secret key attributes in several systems.

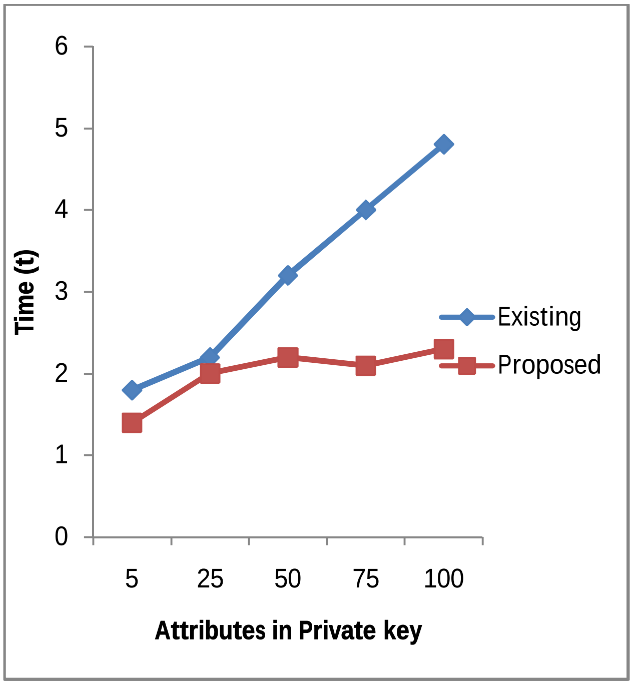

Figure 2 (a): Multi keyword generation time

Figure 2(b) indicates the scales of encryption periods sequentially in the number of ciphertexts attributes in several systems. In our system, it also notes that the setup generation to take more computational cost than the system.

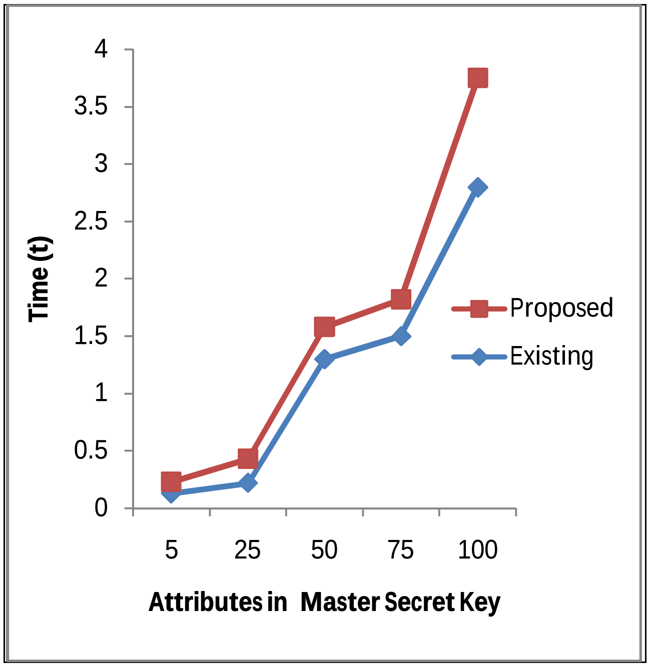

Figure 2(b): Encryption Time

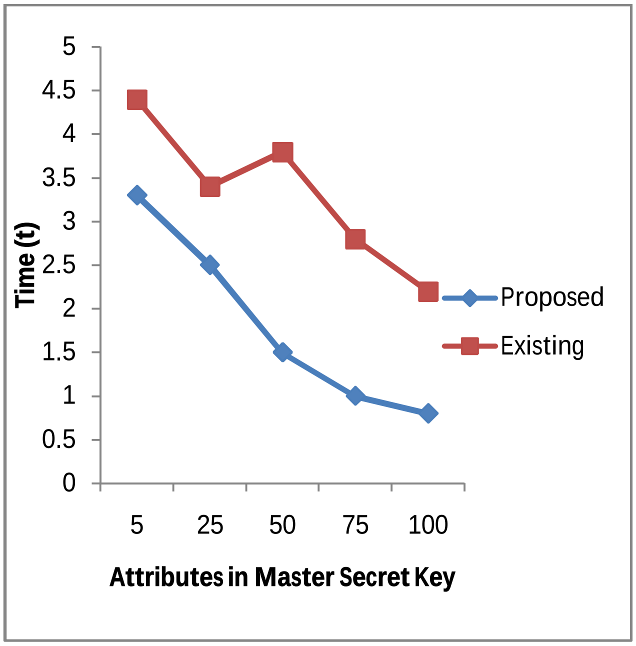

Figure 2 (c): Decryption Time

The system's encryption time and multi-key search generation time naturally takes more computing time than our system. Figure 2(c) illustrates that our scheme user-decryption time takes less computational time than the existing system.

6. CONCLUSION

In this paper, it proposed a Multi- keyword searchable attribute-based encryption system with data access control for cloud storage. It first established a standard method Multi Authority-Ciphertext-Attribute Based Encryption system that allows the data owner to determine and implement the appropriate access policy. They are proving the reliability of our system based on the BDH theory and BL theory. Results of the performance assessment suggest that the proposed work is more effective than other works of attribute-based encryption with data access control. It also outsources the process to the cloud storage with high computing costs to reduce the computing workload on the data user. Our system is also known to be semantic protection against the selected ciphertext-policy and plaintext attack specified in the basic bi-linear design theory.

REFERENCES

1. Wang, S., Yao, L., & Zhang, Y. **Attribute-based encryption scheme with multi-keyword search and supporting attribute revocation in cloud storage**, PloS one, 13(10), e0205675 ,2018. https://doi.org/10.1371/journal.pone.0205675
2. Mell, P., & Grance, T. **The NIST definition of cloud computing**, 2011.
3. Li, Q., Ma, J., Li, R., Liu, X., Xiong, J., & Chen, D.. Secure, **efficient and revocable multi-authority access control system in cloud storage**, Computers & Security, 59, pp. 45-59, 2016.
4. Goyal, V., Pandey, O., Sahai, A., & Waters, B.. **Attribute-based encryption for fine-grained access control of encrypted data**,In Proceedings of the 13th ACM conference on Computer and communications security,pp. 89-98, October 2006.
5. Bethencourt, J., Sahai, A., & Waters, B. **Ciphertext-policy attribute-based encryption**,IEEE symposium on security and privacy, pp. 321-334,May 2007. https://doi.org/10.1109/SP.2007.11
6. Wang, S., Ye, J., & Zhang, Y. **A keyword searchable attribute-based encryption scheme with attribute update for cloud storage**, PloS one, 13(5), e0197318, (2018).
7. Bethencourt, J., Sahai, A., & Waters, B. **Ciphertext-policy attribute-based encryption**, IEEE symposium on security and privacy (SP'07), pp. 321-334, May 2007.
8. Goyal, V., Jain, A., Pandey, O., & Sahai, A. **Bounded ciphertext policy attribute based encryption**, In International Colloquium on Automata, Languages, and Programming, pp. 579-591 Springer, Berlin, Heidelberg, July 2008.
9. Goyal, V., Jain, A., Pandey, O., & Sahai, A. **Bounded ciphertext policy attribute based encryption**, In International Colloquium on Automata, Languages, and Programming, pp. 579-591.Springer,Berlin,Heidelberg, July 2008.
10. Li, J., Wang, H., Zhang, Y., & Shen, J., **Ciphertext-Policy Attribute-Based Encryption with Hidden Access Policy and Testing**, Ksii Transactions on Internet & Information Systems, 10(7), 2016. https://doi.org/10.3837/tiis.2016.07.026
11. Zarezadeh, M., Mala, H., & Ashouri-Talouki, M., **Multi-keyword ranked searchable encryption scheme with access control for cloud storage**. Peer-to-Peer Networking and Applications, 13(1), pp. 207-218, 2020.
12. Buyrukbilen, S., & Bakiras, S., **Privacy-preserving ranked search on public-key encrypted data**, In 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing , pp. 165-174, November 2013.
13. Yu, J., Lu, P., Zhu, Y., Xue, G., & Li, M. **Toward secure multi keyword top-k retrieval over encrypted cloud data**. IEEE transactions on dependable and secure computing, 10(4), 239-250, 2013.
14. Yu, S., Wang, C., Ren,K., & Lou,W. **Attribute based data sharing with attribute revocation**.In Proceedings of the 5th ACM symposium on information, computer and communications security, pp. 261-270, April 2010.
15. Hur, J., & Noh, D. K. **Attribute-based access control with efficient revocation in data outsourcing systems**, IEEE Transactions on Parallel and Distributed Systems, 22(7), pp. 1214-1221, 2010.

16. Xie, X., Ma, H., Li, J., & Chen, X. **New ciphertext-policy attribute-based access control with efficient revocation**. In Information and Communication Technology-EurAsia Conference Springer, Berlin, Heidelberg, pp. 373-382, March 2013.
17. Han, F., Qin, J., Zhao, H., & Hu, J. **A general transformation from KP-ABE to searchable encryption**, Future Generation Computer Systems, 30, 107-115, 2014.
18. Zhang, W., Xiao, S., Lin, Y., Zhou, T., & Zhou, S. **Secure ranked multi-keyword search for multiple data owners in cloud computing**, In 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 276-286, June 2014.
19. Li, H., Liu, D., Jia, K., & Lin, X. **Achieving authorized and ranked multi-keyword search over encrypted cloud data,** In 2015 IEEE International Conference on Communications (ICC) (pp. 7450-7455) , June 2015. https://doi.org/10.1109/ICC.2015.7249517
20. Sun, W., Liu, X., Lou, W., Hou, Y. T., & Li, H. **Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data,**In 2015 IEEE Conference on Computer Communications (INFOCOM), pp. 2110-2118, April 2015.
21. Li, H., Liu, D., Dai, Y., Luan, T. H., & Shen, X. S. **Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage**. IEEE Transactions on Emerging Topics in Computing, 3(1), pp. 127-138,2014.
22. Jung T, Li XY,Wan Z,Wan M. **Privacy preserving cloud data access with multi-authorities**, In: INFOCOM, 2013 proceedings IEEE,doi:10.1109/ INFCOM.2013.6567070,pp. 2625–33,2013.
23. Sun, W., Yu, S., Lou, W., Hou, Y. T., & Li, H. **Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud**, IEEE Transactions on Parallel and Distributed Systems, 27(4),pp. 1187-1198, 2014.
24. Miao, Y., Ma, J., Liu, X., Liu, Z., Shen, L., & Wei, F. **VMKDO: Verifiable multi-keyword search over encrypted cloud data for dynamic data-owner**. Peer-to-Peer Networking and Applications, 11(2), pp. 287-297, (2018).
25. Fan, Y., & Liu, Z. **Verifiable attribute-based multi-keyword search over encrypted cloud data in multi-owner setting**. In 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC) (pp. 441-449), June 2017.
26. Wu, D. N., Gan, Q. Q., & Wang, X. M. **Verifiable public key encryption with keyword search based on homomorphic encryption in multi-user setting**, IEEE Access, 6, pp. 42445-42453, 2018.
27. Liu Z,Wang Z, Cheng X, Jia C, Yuan K. **Multi-user searchable encryption with coarser-grained access control in hybrid cloud**, In: Fourth International conference on emerging intelligent data and web technologies (EIDWT). IEEE, pp. 249–255, 2013 https://doi.org/10.1109/EIDWT.2013.48
28. Kaci, A., & Bouabana-Tebibel, T. **Access control reinforcement over searchable encryption**. In Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014), pp. 130-137, August 2014.
29. Li, J., & Zhang, L. **Attribute-based keyword search and data access control in cloud**, In 2014 Tenth International Conference on Computational Intelligence and Security, pp. 382-386, November 2014.
30. Zhou, P., Liu, Z., & Duan, S. **Flexible attribute-based keyword search via two access policies**. In International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 815-822). Springer, Cham, November 2016.
31. Li, H., Yang, Y., Dai, Y., Bai, J., Yu, S., & Xiang, Y. **Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data**, IEEE Transactions on Cloud Computing, 2017.
32. Cao, L., Wang, Y., Dong, X., Liu, Y., Zhang, Y., Guo, X., & Feng, T. **Multiuser access control searchable privacy-preserving scheme in cloud storage**, International Journal of Communication Systems, 31(9), e3548, 2018.
33. Ren, H., Li, H., Dai, Y., Yang, K., & Lin, X. (2018). **Querying in internet of things with privacy preserving: Challenges, solutions and opportunities**. IEEE Network, 32(6), 144-151. https://doi.org/10.1109/MNET.2018.1700374
34. He, K., Guo, J., Weng, J., Weng, J., Liu, J. K., & Yi, X. **Attribute-based hybrid Boolean keyword search over outsourced encrypted data**, IEEE Transactions on Dependable and Secure Computing, 2018.
35. Xu, G., Li, H., Dai, Y., Yang, K., & Lin, X. **Enabling efficient and geometric range query with access control over encrypted spatial data**, IEEE Transactions on Information Forensics and Security, 14(4), 870-885, 2018.
36. Zu, L., Liu, Z., & Li, J. **New ciphertext-policy attribute-based encryption with efficient revocation**, In 2014 IEEE International Conference on Computer and Information Technology (pp. 281-287, September 2014. https://doi.org/10.1109/CIT.2014.97
37. Rhee, H. S., Park, J. H., Susilo, W., & Lee, D. H. **Trapdoor security in a searchable public-key encryption scheme with a designated tester**. Journal of Systems and Software, 83(5), 763-771, 2010.
38. Syed.Karimunnisa, Dr.Vijaya Sri Kompalli, **Cloud Computing: Review on Recent Research Progress and Issues**, International Journal of Advanced Trends in Computer Science and Engineering, Vol. 8, April 2019 https://doi.org/10.30534/ijatcse/2019/18822019
39. Dhananjaya. V, 2Dr. Balasubramani. R, **Design and Analysis of high security ECC based Cryptography by Holomorphic and data storage in Cloud** , International Journal of Advanced Trends in Computer Science and Engineering, Vol. 9, Pp. 1720-1728, April 2020. https://doi.org/10.30534/ijatcse/2020/124922020

40. Bholanath Mukhopadhyay, Dr. Rajesh Bose and Dr. Sandip Roy, **A Novel Approach to Load Balancing and Cloud Computing Security using SSL in IaaS Environment**, International Journal of Advanced Trends in Computer Science and Engineering, Vol. 9, Pp. 2362-2370, April 2020. https://doi.org/10.30534/ijatcse/2020/221922020