An Extensive Study of Keyword Search on Outsourced Encrypted Data in The Cloud

M.KUNDALAKESI[1], K. RESHMA[2]

[1]*Assistant Professor, Department of BCA & M.Sc. SS , Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu ,India*

[2]*Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India*

bstract -- Migration of the local data to the cloud storage has become prominent due to its flexibility and elasticity. Despite of major advantage on outsourcing data, it proportionally increases the challenges on security in terms of data sharing and data confidentiality. To address this issue, many encryption-based security mechanisms has been devoted to cloud. However, the traditional encryption mechanism is not reliable in data sharing paradigms. In this paper, we undergo an extensive study on keyword search on outsourced encrypted data through utilization of many variants in searchable encryption algorithm. Searchable encryption mechanism allows the data user to make searches on the encrypted data by supplying of keywords with decrypting the text for similarity verification towards query. The query keyword will be transformed into the ciphertext. Transformed ciphertext of the keyword will be associated with encrypted index in order to return relevant data files. The particular solution exponentially increases the computation cost and processing memory. In order to combat this issue, we plan to propose a novel framework, in terms of Cryptographic pairing scheme for the mapping the keyword queries towards the encrypted data in the cloud. The pairing scheme works based on the construction of trap doors for the outsourcing document to the cloud. The performance model each mechanism is analyzed on different evaluation scales on various data sizes.

Indexed Terms: Cloud Computing, Secure Data Sharing, Searchable Encryption, Cryptographic Pairing Scheme

I. INTRODUCTION

Outsourcing of local data to cloud has attracted by its appealing features of the cloud towards storage and management [1]. In such environment, privacy preserving of the outsourced data remains questionable in measurable level of security and data confidentiality [2]. In order to protect the data privacy against the untrusted cloud server provider and data user, attribute-based encryption is being applied on basis on public key cryptosystem for key generation [3]. However it leads to high computation cost towards periodic data utilization by the different user. Query Keyword based retrieval system cannot be directly applied to encrypted data. In order to achieve keyword based search to encrypted files, Searchable encryption has to be derived to perform a data search on encrypted data with search trapdoor of keyword provided by a user [4].

The cloud server will return the search results only when the keywords and indexes are matched and the attributes set of user satisfies the access policy in ciphertext. Moreover, data owner and user can generate the keywords index and search trapdoor respectively without relying on trusted third party. Cryptographic pairing scheme will be analysed in depth towards mapping the keyword queries towards the encrypted data in the cloud. The pairing scheme works based on the construction of trap doors for the outsourcing document to the cloud

The rest of the study paper is organized as follows, section 2 describes the review of literature on basis of searchable encryption and attribute-based encryption followed by section 3 to define the proposed methodology as outline and finally section 4 concludes the study of the paper.

II. REVIEW OF LITERATURES

In this section, we describe the existing methods applied to cloud data security in terms of searchable encryption and cryptographic pairing schemes,

A. Searchable Encryption Technique

Searchable encryption technique is analyzed towards examining the retrieval efficiency of the retrieval system towards search keywords on encrypted data is summarized as follows

B. Multi-User Searchable Symmetric Encryption Scheme

In this literature, Searchable encryption scheme show provable security on exposure some query information in terms of search and access patterns to achieve high efficiency. This scheme is exposed to several inferences attacks such leakage principles as query recovery attack can convert opaque query trapdoors to their corresponding keywords based on some prior knowledge and it withstand these attacks. In addition , securely searching on multiple indexes and sharing encrypted data between multiple users through token-adjustment search scheme to preserve the search functionality among multi-indexes, and a key sharing scheme which combines identity-based encryption and public-key encryption[6].

C. Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing

In this literature, the desired flexibility of sharing any group of selected documents with any group of users demands different encryption keys to be used for different documents. It become possible by imposing of key-aggregate searchable encryption and instantiating the concept through a concrete KASE scheme, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents[7].

D. Attribute Based Encryption

Attribute-based encryption (ABE) technique has been used to design fine-grained access control system, which provides one good method to solve the security issues in cloud setting on the outsourced data

E. Outsourced Attribute-Based Encryption with Keyword Search Function

In this literature, Outsourced ABE (OABE) with fine-grained access control provides access encrypted data stored in cloud with outsourcing key-issuing and outsourcing decryption. It efficiently carries out query processing which can implement keyword search function. It performs partial decryption task delegated by data user without knowing anything about the plaintext [8].

F. Attribute-Based Access Control with Constant-Size Ciphertext

In this literature, hierarchical attribute-based access control scheme with constant-size ciphertext has been analysed. The proposed scheme is efficient because the length of ciphertext and the number of bilinear pairing evaluations to a constant are fixed. The hierarchical authorization structure of our scheme reduces the burden and risk of a single authority scenario. The scheme is of CCA2 security under the decisional q-Bilinear Diffie-Hellman Exponent assumption [9].

G. Fully Anonymous Attribute-Based Encryption

In this literature, a revolutionary computing paradigm named as Fully Anonymous attribute-based encryption has been applied to address identity privacy and data privacy. The model decentralizes the central authority to limit the identity leakage and thus achieves semianonymity [10].

H. Tabular View Of The Review Of Literatures

SI. No	Problem	Title	Objective	Advantages
1	Query recovery attack can convert opaque query trapdoors to their corresponding keywords	Multi-User Searchable Symmetric Encryption Scheme	It uses token-adjustment search scheme to preserve the search functionality among multi-indexes	It achieves high efficiency and proven to high isolation to inference attacks
2	Efficient management of key is major challenge of the work	Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing	Data owner distribute a single key and a single trapdoor to the cloud for querying the shared documents in the cloud using KASE scheme	It is proved to be efficient and highly security
3	The computation cost and ciphertext size grow with the complexity of the access policy	Outsourced Attribute-Based Encryption with Keyword Search Function	Encrypted data stored in cloud with outsourcing key-issuing and outsourcing decryption and implements keyword search function	It process queries efficiently with less computational time
4	Data encryption to the outsourced data enforces heavy burden to data owners	Attribute-Based Access Control with Constant-Size Ciphertext	Hierarchical attribute based access control scheme with constant-size ciphertext	Computation cost in encryption and decryption algorithms is low
5	Various privacy concerns emerge in terms of data and user	Fully Anonymous Attribute-Based Encryption.	It incorporates bilinear Diffie-Hellman assumption	It enables flexible on-demand and low-cost usage of computing resources.

III. OUTLINE OF PROPOSED MODEL

The proposed model is defined based on the analysis of the existing model towards achieving the searchable encryption on the encrypted data. From implication of this extensive study, it provides functional aspects to build a novel framework to search the keyword on the encrypted file using cryptographic pairing model with trapdoor and build index. The Similarity between the encrypted data and search keyword is computed using Euclidean search. This model provides high data confidentiality on query search with misspelled keyword to the cloud system.

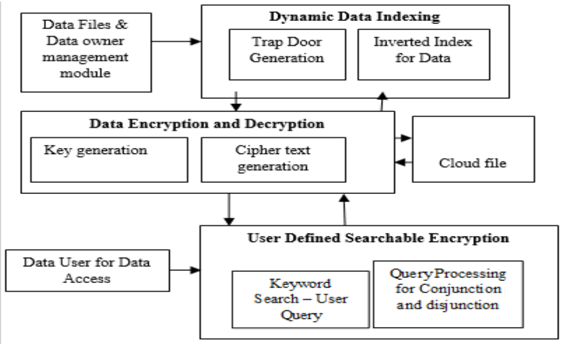
Data Files & Data owner management module
Dynamic Data Indexing
Trap Door Generation
Inverted Index for Data
Data Encryption and Decryption
Key generation
Cipher text generation
Cloud file
Data User for Data Access
User Defined Searchable Encryption
Keyword Search – User Query
Query Processing for Conjunction and disjunction

Figure1 : Architecture Diagram

IV. CONCLUSION

The extensive study of keyword search on outsourced encrypted data in the cloud is presented and analyzed against different data sizes and security parameters. The proposed study analyzed various ABE scheme towards achieving identity and data security. In addition, searchable encryption model provides an encrypted search on the encrypted data with search efficiency. Finally, study includes the data updating in the outsourced data in addition to the search process with encrypted index structure, query generation and keyword index for the data to be retrieved.

REFERENCES

[1] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, “Over-encryption: management of access control evolution on outsourced data,” in *VLDB ’07*, 2007, pp. 123–134.

[2] C. Dong, G. Russello, and N. Dulay, “Shared and searchable encrypted data for untrusted servers,” in *Journal of Computer Security*, 2010.

[3] Y. Wu, Z. Wei, and R. H. Deng, “Attribute-based access to scalable media in cloud-assisted content sharing networks,” IEEE Trans. Multimedia, vol. 15, no. 4, pp. 778–788, 2013.

[4] B. Waters, “Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions,” in CRYPTO, 2009, pp. 619–636.

[5] Y. Zheng, X. Yuan, X. Wang, J. Jiang, C. Wang, and X. Gui, “Toward encrypted cloud media center with secure deduplication,” IEEE Trans. Multimedia, vol. 19, no. 2, pp. 251–265, 2017.

[6] Guofeng Wang, Chuanyi Liu, Yingfei Dong Peiyi, Hezhong Pan, Binxing Fang"IDCrypt: A Multi-User Searchable Symmetric Encryption Scheme for Cloud Applications “in IEEE Access, Volume: 6, 2017.

[7] Baojiang Cui, Zheli Liu, Lingyu Wang "Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage “in IEEE Transactions on Computers, Volume: 65, Issue: 8, Aug. 1 2016

[8] Jiguo Li, Xiaonan Lin, Yichen Zhang, Jinguang Han "KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage" in IEEE Transactions on Services Computing, Volume: 10, Issue: 5, Sept.-Oct. 1 2017.

[9] Wei Teng, Geng Yang, Yang Xiang, Ting Zhang, Dongyang Wang "Attribute-Based Access Control with Constant-Size Ciphertext in Cloud Computing" in IEEE Transactions on Cloud Computing , Volume: 5, Issue: 4, Oct.-Dec. 1 2017

[10] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, Meng Wan "Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption" IEEE Transactions on Information Forensics and Security, Volume: 10, Issue: 1, Jan. 2015